1) Классическое определение вероятности

Теория вероятности изучает неслучайные закономерности массовых случайных явлений. Причем, рассматривает те явления, которые могут быть неоднократно повторены в одинаковых условиях.

Набор условий называется **случайным экспериментом.**

Результаты случайного эксперимента называют **случайным событием или событием** (обозн.: A, B, C).

Случайное событие – это то что может произойти или не произойти в результате ряда экспериментов.

Множество всевозможных итогов случайного эксперимента называется **вероятностным пространством** (+ $\Omega=\{ \omega_1 ,\omega_2 ,\ldots\omega_n\}$)

Элементарное событие называется благоприятствующим событию A, если его появление влечет за собой появление события A.

Классическое определение вероятности

$$P(A)=\frac{m}{n}.$$

Вероятностью P(A) случайного события A называется отношение числа m благоприятствующих ему элементарных событий к их общему числу n.

Основные свойства вероятности

1. Вероятность случайного события A есть неотрицательное число, заключенное между нулем и единицей, т. е. $0 \le P(A) \le 1$.

2. Вероятность достоверного события равна единице $P(\Omega) =1$.

Случайное событие называется **достоверным** если оно обязательно происходит при данном случайном эксперименте.

3. Вероятность невозможного события равна нулю $P(\emptyset) = 0$.

Случайное событие считается **невозможным** если при данном эксперименте оно не может произойти.

2) Случайные события, действия над случайными событиями

Теория вероятности изучает неслучайные закономерности массовых случайных явлений. Причем, рассматривает те явления, которые могут быть неоднократно повторены в одинаковых условиях.

Набор условий называется **случайным экспериментом.**

Результаты случайного эксперимента называют **случайным событием или событием** (обозн.: A, B, C).

Случайное событие – это то что может произойти или не произойти в результате ряда экспериментов.

Теория вероятности изучает явления обладающие статистической устойчивостью (эксперимент может повторяться многократно).

Множество всевозможных итогов случайного эксперимента называется **вероятностным пространством** (+ $\Omega=\{ \omega_1 ,\omega_2 ,\ldots\omega_n\}$)

Случайные события – это всегда подмножество вероятносного пространства.

Для случайных событий определены алгебраические действия:

1. Суммой, или объединением, двух событий A и B называется такое событие C , которое состоит в осуществлении события A или события B , или событий A и B вместе.

$$C = A + B, \text{ или } C = A \cup B .$$

Сумма событий A + B состоит из всех элементарных событий, принадлежащих событиям A и B.

2. Произведением, или пересечением, двух событий A и B называется событие C, которое состоит в осуществлении события A и события B одновременно.

$$C = AB , \text{ или } C = A \cap B .$$

Произведение событий AB состоит из элементарных событий, одновременно входящих в событие A и событие B .

3. $\overline{A}$ – **противоположное событие** – событие при котором событие A никогда не произойдет

3) Теорема сложения и умножения вероятностей. Совместные и несовместные события. Зависимые и независимые события

События А и В называются **совместными**, если они могут появиться одновременно в одном и том же испытании. Это значит, что существуют такие элементарные события, которые входят в состав и А, и В одновременно, другими словами, произведение событий АВ не пустое множество.

События А и В называются **несовместными**, если появление одного из них исключает появление другого, т. е. если АВ = ∅. Иными словами, нет ни одного элементарного события, которое входило бы в состав и А, и В одновременно. В частности, противоположные события А и А всегда несовместны.

Два события А и В называются **зависимыми**, если вероятность появления одного из них зависит от наступления или не наступления другого.

В противном случае события А и В называются **независимыми**. Несколько событий называются независимыми в совокупности, если каждое из них и любая комбинация остальных есть события независимые.

Теорема сложения вероятностей совместных событий

Вероятность суммы 2-х несовместных событий = сумме вероятностей этих событий. Для совместных событий вероятность суммы = сумме вероятностей этих событий - вероятность их совместного происхождения

$$P(A+B)=P(A)+P(B)\_P(AB)$$

$P(\overline{A})=1-P(A)$ — вероятность происхождения противоположных событий

Теорема умножения вероятностей

Вероятность произведения 2-х событий =произведение вероятности 1-го события на условную вероятность 2-го при условии что 1-е произошло.

$$P(AB)=P(A)*P(B|A)= P(B)*P(A|B)$$

Вероятность произведения 2-х независимых событий = произведению вероятностей этих событий

4) Формула полной вероятности. Примеры

Пусть событие А происходит при условии происхождения 1-го из событий H_1, H_2,…,$H_п$. которые попарно несовместны и образуют полную группу.

Событие H_i называется **гипотезой** когда вероятность события А = сумме произведения вероятностей гипотез на условную вероятность события а при условии, что данная гипотеза произошла.

$$P(A)=\sum_{i=1}^{n}P(H_i)$$ *P(A|H_i)

Задача 5. Из двух цехов поступили заготовки для дальнейшей обработки, причем из первого цеха поступило 2000 заготовок, а из второго – 3000 заготовок. Брак среди заготовок первого цеха составляет 5%, а среди заготовок второго цеха 2%. Найти вероятность того, что наугад взятая для обработки заготовка бракованная.

Решение. Событие A, состоящее в том, что наугад взятая заготовка бракованная, может наступить лишь при появлении одного из несовместных событий H_1 (деталь изготовлена первым цехом) или H_2 (деталь изготовленная вторым цехом). Учитывая количество изготовленных цехами заготовок, получим:

$$P(H_1)=\frac{2000}{2000+3000}=\frac{2}{5};\quad P(H_2)=\frac{3000}{2000+3000}=\frac{3}{5}.$$

По условию задачи $P_{H_1}(A)=\frac{5\%}{100\%}=0{,}05$, $P_{H_2}(A)=\frac{2\%}{100\%}=0{,}02$.

По формуле полной вероятности (12.17) находим вероятность события A:

$$P(A)=P(H_1)P_{H_1}(A)+P(H_2)P_{H_2}(A)=\frac{2}{5}\cdot 0{,}05+\frac{3}{5}\cdot 0{,}02=0{,}032.$$

Итак, вероятность того, что наугад взятая заготовка бракованная, равна 0,032.

5) Схема Бернулли. Предельные теоремы в схеме Бернулли

Пусть производится n независимых испытаний, в каждом из которых событие A может появиться с вероятностью p или не появиться с вероятностью q =1 – p. В этом случае говорят, что имеет место *схема испытаний Бернулли*.

Вероятность того, что в описанных n испытаниях событие A появиться ровно k раз $(0 \le k \le n)$, вычисляется по формуле Бернули:

$$P_n(k) = C_n^k p^k q^{n-k}$$

Вероятность того, что событие A в схеме Бернулли появится не менее m_1 раз и не более m_2 раз, равна $P_n(m_1 \le m \le m_2) = \sum_{k=m_1}^{m_2} C_n^k p^k q^{n-k}$.

Если после независимых испытаний проводимых достаточно большое число раз, то в формуле Бернули появляются большие числа и требуется больший обьем вычислений в этом случае используются **предельные теоремы**:

- если число испытаний велико, а вероятность происхождения события мала, то используется формула Пуасона:

$$P_n(k) \approx \frac{\lambda^k e^{-\lambda}}{k!}, \text{где } \lambda = np$$

- если вероятность не является малой, то используется локальная теорема Муавра Лапласа:

$$P_n(k) \approx \frac{1}{\sqrt{npq}}\varphi(x) \text{ где } x = \frac{k-np}{\sqrt{npq}};\ \varphi(x) = \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}}$$

- Если вероятность p появления события A в каждом испытании постоянна и не близка к нулю или единице, то вероятность $P_n(k_1; k_2)$ того, что событие A появится в n испытаниях от k1 до k2 раз, вычисляется по формуле

$$P_n(k_1; k_2) = \Phi(x_2) - \Phi(x_1)$$

$$x_1 = \frac{k_1 - np}{\sqrt{npq}};\quad x_2 = \frac{k_2 - np}{\sqrt{npq}},\ \text{а}\ \ \Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{x_1}^{x_2} e^{-\frac{t^2}{2}} dt$$

6) Определение случайной величины. Функция распределения СВ и ее свойства

Случайной величиной называют величину, которая в результате испытания принимает одно и только одно возможное значение, наперед неизвестное и зависящее от случайных причин, которые заранее не могут быть учтены.

Случайные величины обычно обозначают греческими буквами ξ, η, ζ,… или заглавными буквами X, Y, Z,… латинского алфавита, а их возможные значения – строчными латинскими буквами x, y, z,….

Случайные величины делятся на *дискретные* и *непрерывные*.

Дискретной называют случайную величину, если ее возможные значения можно пронумеровать. Дискретная случайная величина принимает изолированные значения.

Непрерывной называют случайную величину, которая может принимать все значения из некоторого конечного или бесконечного промежутка.

Законом распределения случайной величины называется любое соответствие между возможными значениями случайной величины и их вероятностями. Это соответствие можно задать таблицей, графически и аналитически

При табличном способе задания *дискретной случайной величины* в первой строке указывают ее возможные значения, а во второй – их вероятности

ξ	x_1	x_2	…	x_n
p	p_1	p_2	…	p_n

Законы распределения как дискретных, так и непрерывных случайных величин можно задать с помощью интегральной функции распределения F(x).

Интегральной функцией распределения случайной величины ξ называется функция F(x), определяющая вероятность того, что случайная величина ξ примет значение, меньшее x:

$$F(x) = P(\xi < x)$$

свойства F(x):

1) $0 \le F(x) \le 1$;

2) F(x) – неубывающая и непрерывная слева функция, т. е. если $x_2 > x_1$, то $F(x_2) > F(x_1)$

3) $\lim\limits_{x \to -\infty} F(x) = 0$, $\lim\limits_{x \to +\infty} F(x) = 1$.

При решении задач наиболее часто используется следующее свойство F(x) :

$$P(a \le \xi < b) = F(b) - F(a)$$

7) Дискретные СВ, способы их задания

Дискретной называют случайную величину, если ее возможные значения можно пронумеровать. Дискретная случайная величина принимает изолированные значения.

При табличном способе задания *дискретной случайной величины* в первой строке указывают ее возможные значения, а во второй – их вероятности

ξ	x_1	x_2	…	x_n
p	p_1	p_2	…	p_n

$$\sum_{i=1}^{n} p_i = 1$$

Следует иметь в виду, что . Такую таблицу называют также *рядом распределения дискретной случайной величины*.

Законы распределения как дискретных величин можно задать с помощью интегральной функции распределения F(x).

$$F(x) = P(\xi < x).$$

Математическим ожиданием дискретной случайной величины ξ называют сумму произведений всех ее возможных значений на их вероятности:

$$M_\xi = \sum_{i=1}^{n} x_i p_i$$

Для дискретной случайной величины **дисперсия** вычисляется по формуле

$$D_\xi = \sum_{i=1}^{n} (x_i - M_\xi)^2 p_i$$

8) Непрерывные СВ, способы их задания

Непрерывной называют случайную величину, которая может принимать все значения из некоторого конечного или бесконечного промежутка.

Законы распределения непрерывных величин можно задать с помощью интегральной функции распределения F(x).

$$F(x) = P(\xi < x).$$

Математическим ожиданием непрерывной случайной величины ξ, возможные значения которой принадлежат отрезку [a; b], называют определенный интеграл

$$M_\xi = \int_a^b x\,p(x)\,dx.$$

Для непрерывной случайной величины **дисперсия** равна

$$D_\xi = \int_a^b (x - M_\xi)^2\,p(x)\,dx$$

если возможные значения принадлежат отрезку [a; b], и

$$D_\xi = \int_{-\infty}^{+\infty} (x - M_\xi)^2\,p(x)\,dx,$$

если возможные значения принадлежат всей оси Ox.

9) Плотность распределения СВ и ее свойства

Плотностью распределения вероятностей, или дифференциальной функцией распределения, непрерывной случайной величины называется функция p(x), такая, что

$$p(x) = F'(x).$$

Свойства функции $p(x)$:

1) $p(x) \geq 0$, т. е. плотность распределения неотрицательна;

2) $\int_{-\infty}^{+\infty} p(x)dx = 1$.

При решении задач часто используется следующая формула:

$$P(a < \xi < b) = \int_{a}^{b} p(x)dx . \quad ($$

Откуда следует, что

$$F(x) = \int_{-\infty}^{x} p(t)dt .$$

10) Математическое ожидание СВ, формулы для вычисления

Математическим ожиданием дискретной случайной величины ξ называют сумму произведений всех ее возможных значений на их вероятности

$$M_\xi = \sum_{i=1}^{n} x_i p_i$$

Математическим ожиданием непрерывной случайной величины ξ, возможные значения которой принадлежат отрезку [a; b], называют определенный интеграл

$$M_\xi = \int_a^b x\,p(x)\,dx\,.$$

Если возможные значения принадлежат всей оси Ox, то

$$M_\xi = \int_{-\infty}^{+\infty} x\,p(x)\,dx\,.$$

Вероятностный смысл математического ожидания состоит в том, что оно приближенно равно среднему ожидаемому значению случайной величины.

Отклонением случайной величины от ее математического ожидания называют разность $\xi - M_\xi$ между случайной величиной и ее математическим ожидание

11) Дисперсия СВ и ее свойства. Среднеквадратическое отклонение

Дисперсией (рассеиванием) случайной величины называют математическое ожидание квадрата отклонения случайной величины от ее математического ожидания:

$$D_\xi = M((x_i - M_\xi)^2)$$

Для дискретной случайной величины дисперсия вычисляется по формуле

$$D_\xi = \sum_{i=1}^{n} (x_i - M_\xi)^2 p_i$$

Для непрерывной случайной величины дисперсия равна

$$D_\xi = \int_a^b (x - M_\xi)^2 p(x) dx$$

если возможные значения принадлежат отрезку [a; b], и

$$D_\xi = \int_{-\infty}^{+\infty} (x - M_\xi)^2 p(x) dx$$

если возможные значения принадлежат всей оси Ox.

На практике, как правило, используют другие формулы. Поскольку верно, что

$$D_\xi = M(\xi^2) - M_\xi{}^2$$

то дисперсия для дискретной случайной величины вычисляется по формуле

$$D_\xi = \sum_{i=1}^{n} x_i{}^2 p_i - M_\xi{}^2$$

Для непрерывных случайных величин по формуле

$$D_\xi = \int_a^b x^2 p(x) dx - M_\xi{}^2$$

или

$$D_\xi = \int_{-\infty}^{+\infty} x^2 p(x) dx - M_\xi{}^2.$$

Дисперсия характеризует степень рассеяния возможных значений случайной величины относительно ее математического ожидания.

12) Биномиальное распределение

Биноминальный закон распределения

Если вероятности возможных значений дискретной случайной величины ξ вычисляются по формуле Бернулли $p(\xi = k) = C_n^k p^k q^{n-k}$, то распределение называется биноминальным. Числовые характеристики биноминального распределения:

$$M_\xi = np;\ \ D_\xi = npq;\ \ \sigma_\xi = \sqrt{npq}\ .$$

13) РАСПРЕДЕЛЕНИЕ ПУАССОНА

Распределение Пуассона – это распределение числа появления редких случайных событий, которые могут принимать только два противоположных значения. Это распределение возникает, когда вероятность наступления одного из признаков мала, а число испытаний **n** большое. Если известна вероятность успеха **p** в каждом испытании, то вероятность того, что в **n** независимых испытаниях событие наступит **k** раз. Т.е. это распределение вероятностей случайной величины X с целочисленными неотрицательными значениями k=0,1,2,.., заданное формулой

$$p_k(\lambda) = \frac{\lambda^k}{k!} e^{-\lambda}$$

Его числовые характеристики:

$M_\xi = D_\xi = np = \lambda;\ \ \sigma_\xi = \sqrt{np}$, где

λ – параметр распределения

ξ – вероятность возможных значений дискретной случайной величины

M_ξ – математическое ожидание

σ_ξ – стандартное отклонение

или может быть это-?

2. Дискретная СВ ξ имеет ***распределение Пуассона*** с параметром a, если она принимает значения 0, 1, 2, ..., n, ... с вероятностями:

$$P(\xi = m) = \frac{a^m}{m!} e^{-a},\ m = 0, 1, 2, ..., n, ...$$

Математическое ожидание и дисперсия СВ ξ, распределенной по закону Пуассона, равны $M\xi = D\xi = a$.

Закон распределения Пуассона (*закон редких явлений*) является хорошим приближением для биномиального распределения при больших значениях n и малых p (или $1 - p$).

14) ГЕОМЕТРИЧЕСКОЕ РАСПРЕДЕЛЕНИЕ

Дискретная случайная величина имеет ***геометрическое распределение*** с параметром , если она принимает значения 0,1,2, ..., m, … (бесконечное, но счетное множество значений) с вероятностями:

$$P_m = q^m p, \qquad \text{где } m = 0,1,2,\dots, \qquad \text{где } 0 < p < 1$$

Вероятности P_m для последовательности значений m образуют геометрическую прогрессию с первым членом p и знаменателем q.

На практике геометрическое распределение появляется при независимых испытаниях с целью получения положительного результата – наступления события A, вероятность появления которого $=p$. СВ X – число неудачных попыток – имеет геометрическое распределение. В этом случае имеем:

P{X=0}=P{первая попытка успешная}=p;

$$P\{X=1\}\begin{Bmatrix}\text{первая попытка безуспешная,}\\ \text{вторая успешная}\end{Bmatrix} = qp;$$

…

$$P\{X=m\}\begin{Bmatrix}\text{первые } m \text{ попыток безуспешная,}\\ (m+1) \text{ успешная}\end{Bmatrix} = q^m p;$$

Ряд геометрического распределения случайной величины имеет вид:

x_i	1	2	3	…	m	…
p_i	p	pq	pq^2	…	pq^{m-1}	…

Дисперсию и среднее квадратичное отклонение случайной величины X вычисляем по формулам:

$$D_X = \alpha_2 - m_X^2 = \frac{2q^2}{p^2} + \frac{q}{p} - \frac{q^2}{p^2} = \frac{q}{p^2}\,;\ \sigma_X = \sqrt{D_X} = \frac{\sqrt{q}}{p}.$$

15) РАВНОМЕРНОЕ РАСПРЕДЕЛЕНИЕ

Равномерным распределением непрерывной случайной величины называется распределение, в котором значения случайной величины с двух сторон ограничены и в границах интервала имеют одинаковую вероятность. Это означает, что в данном интервале плотность вероятности постоянна. Т.е. СВ называется *равномерно распределенной* на [a,b], если её плотность вероятности на этом интервале постоянна, а вне [a,b] равна 0.

1. НСВ ξ имеет ***равномерное распределение*** на отрезке $[a, b]$, если ее плотность распределения постоянна на этом отрезке, а вне его равна нулю:

$$p(x)=\begin{cases}\dfrac{1}{b-a} & \text{при } x\in[a,b],\\ 0 & \text{при } x\notin[a,b].\end{cases}$$

Функция распределения равномерно распределенной на $[a, b]$ СВ имеет следующий вид:

$$F(x)=\begin{cases}0 & \text{при } x<a,\\ \dfrac{x-a}{b-a} & \text{при } a\le x\le b,\\ 1 & \text{при } x>b,\end{cases}$$

а вероятность попадания этой СВ в некоторый интервал, лежащий внутри отрезка $[a, b]$, зависит только от длины этого интервала и не зависит от его положения:

$$P(x_1<\xi<x_2)=\int_{x_1}^{x_2}p(x)dx=\frac{x_2-x_1}{b-a},\quad \text{если } a\le x_1<x_2\le b.$$

Числовые характеристики равномерного распределения:

$$M\xi=\frac{a+b}{2},\ D\xi=\frac{(b-a)^2}{12},\quad \sigma_\xi=\frac{b-a}{2\sqrt{3}}.$$

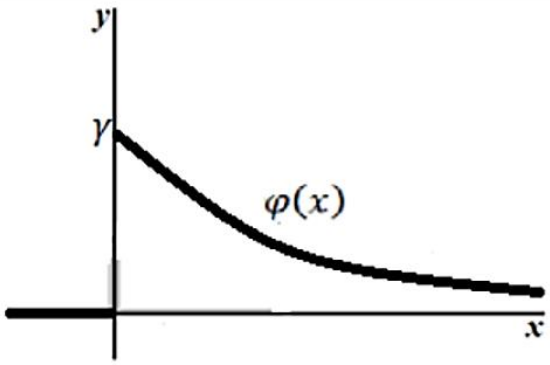
Примерами равномерно распределенных СВ могут служить: время ожидания пассажиром транспорта, курсирующего с определенным интервалом; ошибка округления числа до ближайшего целого.

16) ПОКАЗАТЕЛЬНОЕ РАСПРЕДЕЛЕНИЕ

Показательным или экспоненциальным распределением, называется распределение вероятностей непрерывной случайной величины x, которое описывается плотностью с параметром $\lambda > 0$(единственным), в этом и есть его преимущество.

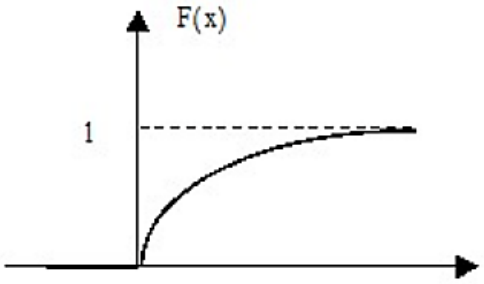
$$p(x) = \begin{cases} \lambda e^{-\lambda x} & \text{при } x \geq 0, \\ 0 & \text{при } x < 0. \end{cases}$$

График плотности показательного распределения имеет вид



Функция показательного распределения:

$$F(x) = \begin{cases} 1 - e^{-\lambda x} & \text{при } x \geq 0, \\ 0 & \text{при } x < 0. \end{cases}$$



Числовые характеристики показательного распределения:

$$M\xi = \frac{1}{\lambda}, \quad D\xi = \frac{1}{\lambda^2}, \quad \sigma_\xi = \frac{1}{\lambda}.$$

Показательное распределение является одним из основных в теории массового обслуживания и теории надежности. Примером СВ, имеющей показательное распределение, является время ожидания редких явлений: время между двумя вызовами на АТС, продолжительность безотказной работы приборов и т. д.

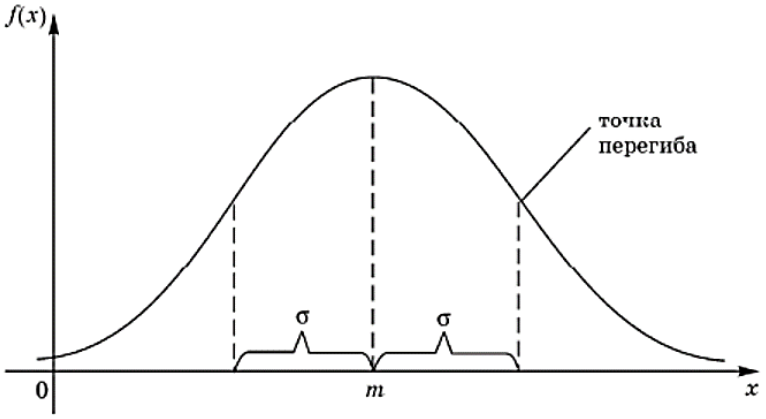
17) НОРМАЛЬНЫЙ ЗАКОН РАСПРЕДЕЛЕНИЯ. ПРАВИЛО ТРЕХ СИГМ

Нормальный закон распределения имеет плотность вероятности

$$p(x)=\frac{1}{\sigma_\xi\sqrt{2\pi}}e^{-\frac{(x-a)^2}{2\sigma_\xi^2}} \quad \text{где } M_\xi=a;\ D_\xi=\sigma_\xi^2\ \ x\in(-\infty,+\infty)$$

График функции плотности вероятности имеет максимум в точке x=m а точки перегиба отстоят от точки m на расстояние δ.

При $x\to\pm\infty$ функция асимптотически приближается к нулю.



Помимо геометрического смысла, параметры нормального закона распределения имеют и вероятностный смысл. Параметр m равен математическому ожиданию нормально распределенной случайной величины, а дисперсия $D_\xi=\sigma_\xi^2$.

Вероятность попадания случайной величины в заданный интервал $(\alpha;\beta)$ вычисляется по формуле:

$$p(\alpha<\xi<\beta)=\Phi\left(\frac{\beta-a}{\sigma_\xi}\right)-\Phi\left(\frac{\alpha-a}{\sigma_\xi}\right)$$

Вероятность отклонения СВ от математического ожидания на величину δ равна:

$$p(|\xi-M_\xi|<\delta)=2\Phi\left(\frac{\delta}{\sigma_\xi}\right)$$

Используя табличные значения ф-ии Лапласа, найдем вероятность

$P(|X-a|\le 3\delta)=\Phi\left(\frac{3\delta}{\delta}\right)=\Phi(3)=0{,}9973.$ Эту особенность нормального распределения называют "***правилом трех сигм***":

Правило трех сигм: Если СВ имеет нормальный закон распределения с параметрами a и δ, то практически достоверно, что её значение заключены в интервале $(a-3\delta, a+3\delta)$

Практическое применение правила 3δ:

1. для оценки нормального распределения
2. для выявления ошибочно полученных результатов
3. для грубого определения δ

18) ПОНЯТИЕ О ДВУМЕРНОЙ СВ. ФУНКЦИЯ РАСПРЕДЕЛЕНИЯ ДВУМЕРНОЙ СВ И ЕЕ СВОЙСТВА

Двумерной называют СВ (X,Y), возможные значения которой есть пары чисел (x,y). Составляющие X и Y, рассматриваемые одновременно, образуют систему двух случайных величин. При этом предполагаются определенными вероятности произведения событий $X<x$ и $Y<y$ для любых вещественных x,y. Одномерные СВ X,Y называются компонентами двумерной СВ (X,Y).

Способы задания двумерной случайной величины

1) *Законом распределения дискретной двумерной случайной величины* называется перечень возможных значений этой величины, то есть пар чисел (x_i, y_i) и их вероятностей $P_{ij} = P(X = x_i, Y = y_i)$, удовлетворяющих условию $\sum_i \sum_j p_{ij} = 1$

2) *Функцией распределения системы двух случайных величин* называется функция $F(x,y)$, которая для любых действительных чисел x и y равна вероятности совместного выполнения двух событий $\{X<x\}$ и $\{Y<y\}$, то есть

$$F(x,y) = P\{X < x, Y < y\}$$

Свойства функции распределения двумерной случайной величины:

1.Функция $0 \le F(x,y) \le 1$, т.е. величина неотрицательная меньше 1.

2.Функция F(x,y) есть возрастающая функция по каждому из аргументов.

$$F(x_2,y) \ge F(x_1,y) \qquad \text{при } x_2 > x_1$$

$$F(x,y_2) \ge F(x,y_1) \qquad \text{при } y_2 > y_1$$

3.Функция распределения F(x,y) = 0, если хотя бы один из аргументов x или y стремится к минус бесконечности.

$$F(x,-\infty) = 0$$
$$F(-\infty,y) = 0$$
$$F(-\infty,-\infty) = 0$$

4.Функция F(x,y) равна функции от одного аргумента F(x) (F(y)), если y (x) стремится к бесконечности.

$$F(x,+\infty) = F_1(x)$$
$$F(+\infty,y) = F_2(y)$$

5. Функция F(x,y) равна 1, если оба аргумента стремятся к плюс бесконечности.

$$F(+\infty,+\infty) = 1$$

19) РАСПРЕДЕЛЕНИЕ НЕПРЕРЫВНОЙ ДВУМЕРНОЙ СВ. СОВМЕСТНАЯ ПЛОТНОСТЬ РАСПРЕДЕЛЕНИЯ. РАСПРЕДЕЛЕНИЕ СВ ПО ОТДЕЛЬНОСТИ

Функций распределения (*или* ***интегральным законом распределения***) двумерной СВ (X,Y) (*дискретной или непрерывной*) *называется функция* $F(x,y)$, *определяемая равенством* $F(x,y) = P\{X < x,\ Y < y\}$.

Плотностью распределения вероятностей (или совместной плотностью) непрерывной двумерной случайной величины (X, Y) называется вторая смешанная производная её функции распределения.

Обозначается совместная плотность системы двух непрерывных СВ (X, Y) через $f(x,y)$.

Таким образом, по определению

$$f(x,y) = \frac{\partial^2 F(x,y)}{\partial x \partial y} = F''(x,y).$$

Зная плотность совместного распределения, можно найти одномерные плотности для X и Y:

$$f(x) = \int_{-\infty}^{\infty} f(x,y)dy, \quad f(y) = \int_{-\infty}^{\infty} f(x,y)dx.$$

Как и для случая дискретных двумерных СВ вводится понятие условного закона распределения, плотности которых можно найти так:

$$f(x|y) = f_y(x) = \frac{f(x,y)}{f(y)}, \quad f(y|x) = f_x(y) = \frac{f(x,y)}{f(x)}$$

Если для всех значений (x, y) выполняется равенство

$$f(x,y) = f(x) \cdot f(y),$$

20) УСЛОВИЕ НЕЗАВИСИМОСТИ И НЕКОРРЕЛИРУЕМОСТИ СВ "ПСИ" И "ЭТА", СВЯЗЬ МЕЖДУ НИМИ

Случайные величины ξ и η называются *независимыми*, если

$$F_{\xi\eta}(x, y) = F_\xi(x) F_\eta(y).$$

Теорема 2.2. Необходимым и достаточным условием независимости случайных величин ξ и η является

$$\mathsf{P}(a \leqslant \xi < b, c \leqslant \eta < d) = \mathsf{P}(a \leqslant \xi < b)\mathsf{P}(c \leqslant \eta < d)$$

для любых $a < b$ и $c < d$.

Ковариацией(корреляционным моментом) СВ ξ и η называют число $\operatorname{cov}(\xi, \eta) = \mathsf{M}\big((\xi - \mathsf{M}\xi)(\eta - \mathsf{M}\eta)\big)$

Используя св-ва мат ожидания, получ ф-лу $\operatorname{cov}(\xi, \eta) = \mathsf{M}\xi\eta - \mathsf{M}\xi\,\mathsf{M}\eta.$

Теорема 2.3. Пусть ξ и η — дискретные случайные величины, причем $\sum\limits_{i,j} \mathsf{P}(\xi = x_i, \eta = y_j) = 1$, а последовательности $\{x_i\}$ и $\{y_j\}$ не имеют предельных точек. Случайные величины ξ и η независимы тогда и только тогда, когда для любых значений x_i и y_j выполнено

$$\mathsf{P}(\xi = x_i, \eta = y_j) = \mathsf{P}(\xi = x_i)\mathsf{P}(\eta = y_j).$$

Коэффициентом корреляции величин ξ и η называют отношение ковариации к произведению средних квадратических отклонений этих величин:

$$\rho_{\xi\eta} = \frac{\operatorname{cov}(\xi, \eta)}{\sqrt{\mathsf{D}\xi\,\mathsf{D}\eta}}.$$

Коэффициент корреляции — безразмерная величина, причем $|\rho_{\xi\eta}| \leqslant 1$. Коэффициент корреляции служит для оценки тесноты *линейной* связи между ξ и η

Если коэффициент корреляции =0, то величины называют *некоррелированными*.

Заметим, что для некоторых распределений понятия независимости и некоррелированности являются эквивалентными. В частности, если случайные величины ξ и η имеют нормальное распределение и $\rho_{\xi\eta} = 0$, то они независимы.

21) ЧИСЛОВЫЕ ХАРАКТЕРИСТИКИ ДВУМЕРНЫХ СВ "ПСИ" И "ЭТА", МАТЕМАТИЧЕСКОЕ ОЖИДАНИЕ, ДИСПЕРСИЯ, СИГМА, КОВАРИАЦИЯ СВ

Среди числовых характеристик двумерной случайной величины важнейшими являются условное математическое ожидание и ковариация.

Математическое ожидание

Пусть (ξ , η) - двумерная случайная величина, тогда $\boldsymbol{M}(\xi , \eta)=(\boldsymbol{M}(\xi), \boldsymbol{M}(\eta))$, т.е. математическое ожидание случайного вектора - это вектор из математических ожиданий компонент вектора.

то математические ожидания компонент вычисляются по формулам:

$$M\xi = \sum_{i=1}^{n}\sum_{j=1}^{m} x_i p_{ij} \ , \ M\eta = \sum_{i=1}^{n}\sum_{j=1}^{m} y_j p_{ij} \ .$$

Если $p_{(\xi , \eta)}(x, y)$- совместная плотность распределения непрерывной двумерной случайной величины (ξ , η), то

$$M\xi = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} x p_{(\xi, \eta)}(x, y)\,dx\,dy \text{ и } M\eta = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} y p_{(\xi, \eta)}(x, y)\,dx\,dy .$$

Поскольку $\int_{-\infty}^{\infty} p_{(\xi, \eta)}(x, y)\ dy = p_{\xi}(x)$ -плотность распределения случайной величины ξ , то

$$M\xi = \int_{-\infty}^{\infty} x p_{\xi}(x)\ dx \text{ и, аналогично, } M\eta = \int_{-\infty}^{\infty} y p_{\eta}(x)\ dy .$$

Дисперсией (рассеянием) случайной величины называется математическое ожидание квадрата ее отклонения от ее математического ожидания.

Если (ξ , η) - двумерная случайная величина, то

$$\boldsymbol{D}\xi = \boldsymbol{M}(\xi - \boldsymbol{M}\xi)^2 = \boldsymbol{M}\xi^2 - \boldsymbol{M}(\xi)^2, \ \boldsymbol{D}\eta = \boldsymbol{M}(\eta - \boldsymbol{M}\eta)^2 = \boldsymbol{M}\eta^2 - \boldsymbol{M}(\eta)^2$$

Если между случайными величинами "ПСИ" И "ЭТА" существует стохастическая связь, то одним из параметров, характеризующих меру этой связи является *ковариация*. ***Ковариацию*** вычисляют по формулам

$$\operatorname{cov}(\xi , \eta)=\boldsymbol{M}[(\xi - \boldsymbol{M}\xi)(\eta - \boldsymbol{M}\eta)] = \boldsymbol{M}(\xi \eta) - \boldsymbol{M}\xi \, \boldsymbol{M}\eta$$

Если случайные величины (ξ , η) *независимы*, то $\operatorname{cov}(\xi , \eta)=0$

Свойства ковариации:

$\operatorname{cov}(\xi , \xi) = \boldsymbol{D}\xi$;

$$\operatorname{cov}(\xi + C_1, \eta + C_2) = \operatorname{cov}(\xi, \eta);$$

$$\operatorname{cov}(\xi, \eta) = \operatorname{cov}(\eta, \xi);$$

$$\operatorname{cov}(C_1\xi + C_2\eta, \varsigma) = C_1 \operatorname{cov}(\xi, \varsigma) + C_2 \operatorname{cov}(\eta, \varsigma),$$

где C_1 и C_2 - произвольные константы.

22) КОЭФФИЦИЕНТ КОРРЕЛЯЦИИ СВ И ЕГО СВОЙСТВА

Коэффициентом корреляции величин ξ и η называют отношение ковариации к произведению средних квадратических отклонений этих величин:

$$\rho_{\xi\eta} = \frac{\operatorname{cov}(\xi, \eta)}{\sqrt{\mathrm{D}\xi\,\mathrm{D}\eta}}.$$

Коэффициент корреляции — безразмерная величина, причем $|\rho_{\xi\eta}| \leqslant 1$. Коэффициент корреляции служит для оценки тесноты *линейной* связи между ξ и η: чем ближе абсолютная величина коэффициента корреляции к единице, тем связь сильнее; чем ближе абсолютная величина коэффициента корреляции к нулю, тем связь слабее. Коэффициент корреляции равен 1 тогда и только тогда, когда случайные величины линейно связаны[1]. Если коэффициент корреляции равен нулю, то величины называют *некоррелированными*.

Свойства коэффициента корреляции СВ:

- коэффициент корреляции по абсолютной величине не превосходит 1: $-1 < r_{xy} < 1$;
- если X и Y независимы, то $r_{xy} = 0$;
- если X и Y связаны линейной зависимостью, т.е.

$X = a\,Y + в$, где $a \neq 0$, то $r_{xy} = 1$ или $r_{xy} = -1$,

Причём $r_{xy} = 1$ при $a > 0$

и $= -1$ при $a < 0$;

- если $r_{xy} = 1$ или $r_{xy} = -1$,

то X и Y связаны линейной зависимостью.

23) ОСНОВНЫЕ ЗАДАЧИ МАТЕМАТИЧЕСКОЙ СТАТИСТИКИ. ВЫБОРКА, ВАРИАЦИОННЫЙ РЯД

Математическая статистика изучает закономерности, которые имеют место в массовых совокупностях однородных объектов.

Основные задачи математической статистики: 1. Разработка методов сбора и группировки статистических сведений, полученных в результате наблюдений или в результате специально поставленных экспериментов. 2. Разработка методов анализа статистических данных в зависимости от целей исследования.

Т.е. разработка методов получения вероятностных характеристик случайных явлений на основе результатов эксперимента. Исходными понятиями математической статистики являются понятия генеральной и выборочной совокупностей.

Выборка (случайная выборка, выборочная совокупность) - множество значений результатов наблюдений над одной и той же случайной величиной при одних и тех же условиях. Элементы выборки называются ***выборочными значениями***. Количество проведенных наблюдений называется ***объемом выборки***.

Пусть имеется выборка объема n: $x_1, x_2, \ldots, x_n$.

Вариационным рядом выборки $x_1, x_2, \ldots, x_n$ называется способ её записи, при котором её элементы упорядочены (как правило, в порядке не убывания): $x_1 \le x_2 \le \ldots \le x_n$. Разность ω между максимальным и минимальным элементами называется ***размахом выборки***:

$$\omega = x_{\max} - x_{\min}.$$

Как правило, некоторые выборочные значения могут совпадать, поэтому часто выборку представляют в виде статистического ряда.

24) ЭМПИРИЧЕСКАЯ ФУНКЦИЯ РАСПРЕДЕЛЕНИЯ И ЕЕ СВОЙСТВА

Эмпирической функцией распределения (функцией распределения выборки) называется функция $F^*(x)$, которая определяет для каждого значения x относительную частоту события $X<x$:

$F^*(x)=\frac{n_x}{n}$, где n_x – число выборочных значений, меньших x; n – объем выборки.

Основное значение эмпирической функции распределения в том, что она используется в качестве оценки теоретической функции распределения $F(x) = P(\xi < x)$ наблюдаемой случайной величины ξ и обладает всеми свойствами функции распределения дискретной случайной величины:

1) $0 \le F^*(x) \le 1$;

2) $F^*(x)$ – неубывающая непрерывная слева кусочно-постоянная функция;

3) если x_1 – наименьшее, а x_n – наибольшее значения статистического ряда, то $F^*(x) = 0$ при $x \le x_1$ и $F^*(x) = 1$ при $x > x_n$.

Эмпирическая функция распределения $F^*(x)$ является случайной: для разных выборок она получается разной. Если график $F^*(x)$ строится по группированным данным, то скачки происходят в точках, соответствующих серединам интервалов группировки.

25) ТОЧЕЧНАЯ ОЦЕНКА ПАРАМЕТРОВ РАСПРЕДЕЛЕНИЯ, ИХ СВОЙСТВ

Точечной называют статистическую оценку, которая определяется одним числом. Точечная оценка

Выборочная характеристика

$$\Theta^* = f(x_1, x_2, ..., x_n)$$

используемая для нахождения приближённого значения неизвестной генеральной характеристики Θ, называется её ***точечной статистической оценкой***.

$$\Theta \approx \Theta^*$$

характеризуется **свойствами:** несмещенность, состоятельность и эффективность.

Несмещенной называют точечную оценку, математическое ожидание которой равно оцениваемому параметру при любом объеме выборки.

Точечная оценка называется ***состоятельной***, если при неограниченном увеличении объема выборки (n ® ¥) она сходится по вероятности к истинному значению параметра, то есть стремится к истинному значению оцениваемого параметра генеральной совокупности.

Эффективной называют точечную оценку, которая (при заданном объеме выборки n) имеет наименьшую возможную дисперсию, те есть гарантирует наименьшее отклонение выборочной оценки от такой же оценки генеральной совокупности.

Качество точечной оценки характеризуется следующими основными свойствами.

1. Оценка $\hat{\theta}$ называется ***несмещённой,*** если её математическое ожидание равно оцениваемому параметру: $M[\hat{\theta}] = \theta$. Разность $M[\hat{\theta}] - \theta$ называется *смещением.*

Требование несмещенности гарантирует отсутствие систематических ошибок при оценивании. Оно особенно важно при малом числе наблюдений (в случае выборок объема не более 30).

2. Оценка $\hat{\theta}_n$ называется ***состоятельной***, если при увеличении объёма выборки n оценка $\hat{\theta}_n$ сходится по вероятности к θ:

$$\lim_{n\to\infty} P(|\theta - \hat{\theta}_n| < \varepsilon) = 1.$$

Это свойство означает, что при большом объеме выборки практически достоверно, что $\hat{\theta}_n \approx \theta$. Чем больше объем выборки, тем более точные оценки можно получить.

3. Пусть $\hat{\theta}_1$ и $\hat{\theta}_2$ – две различные *несмещённые* оценки параметра. Если для дисперсий $D[\hat{\theta}_1]$ и $D[\hat{\theta}_2]$ выполняется условие $D[\hat{\theta}_1] < D[\hat{\theta}_2]$, то говорят, что оценка $\hat{\theta}_1$ более эффективна, чем оценка $\hat{\theta}_2$. Оценка с наименьшей дисперсией называется ***эффективной.***

26) Точечная оценка математического ожидания, его свойства

Точечная оценка математического ожидания

Пусть $x_1, x_2, \ldots, x_n$ выборка из генеральной совокупности, соответствующей случайной величине x с неизвестным математическим ожиданием $Mx = q$ и известной дисперсией $D\xi = \sigma^2$.

Рассмотрим оценку неизвестного математического ожидания

$$\hat{\theta}_n = \frac{x_1 + x_2 + \ldots + x_n}{n}.$$

Оценка несмещённая, поскольку её математическое ожидание равно $Mx = q$:

$$M\hat{\theta}_n = M\left(\frac{x_1 + x_2 + \ldots + x_n}{n}\right) = \frac{1}{n}(Mx_1 + Mx_2 + \ldots + Mx_n) = \frac{1}{n} \cdot n \cdot \theta = \theta,$$

Оценка состоятельная, поскольку при $n \to \infty$, $D\hat{\theta}_n = \frac{1}{n}\sigma^2 \to 0$:

$$D\hat{\theta}_n = D\left(\frac{x_1 + x_2 + \ldots + x_n}{n}\right) = \frac{1}{n^2}(Dx_1 + Dx_2 + \ldots + Dx_n) = \frac{1}{n^2} \cdot n \cdot \sigma^2 = \frac{1}{n}\sigma^2 \to 0.$$

Итак, для оценки неизвестного математического ожидания случайной величины будем использовать выборочное среднее: $\theta_n = \bar{x} = \frac{1}{n}(x_1 + x_2 + \ldots + x_n)$.

a - математическое ожидание нормального закона

$$\overline{x_в} = \frac{x_1 + x_2 + \cdots + x_n}{n}$$

$$M(\overline{x_в}) = M\left(\frac{x_1 + x_2 + \cdots + x_n}{n}\right) = \frac{1}{n}(Mx_1 + Mx_2 + \cdots + Mx_n) = \frac{1}{n}(a + a + \cdots + a) = a$$

$$p(|\overline{x_в} - a| < \varepsilon) = 1, n \to \infty$$

$$p\left(\left|\frac{x_1 + \cdots + x_n}{n} - a\right| < \varepsilon\right) = 1, n \to \infty$$

По теореме Чебышева $\overline{x_в}$ является состоятельной оценкой математического ожидания. Теорема Чебышева. Если $X_1, X_2, \ldots X_n$ — попарно независимые случайные величины, причем дисперсии их равномерно ограничены (не превышают постоянного числа C), то, как бы мало ни было положительное число e, вероятность неравенства

$$\left|\frac{X_1 + X_2 + \ldots + X_n}{n} - \frac{M(X_1) + M(X_2) + \ldots + M(X_n)}{n}\right| < \varepsilon$$

будет как угодно близка к единице, если число случайных величин достаточно велико.

$$\lim_{n \to \infty} P\left(\left|\frac{X_1 + X_2 + \ldots + X_n}{n} - \frac{M(X_1) + M(X_2) + \ldots + M(X_n)}{n}\right| < \varepsilon\right) = 1.$$

Если рассматривается достаточно большое число независимых случайных величин, имеющих ограниченные дисперсии, то почти достоверным можно считать событие, состоящее в том, что отклонение среднего арифметического случайных величин от среднего арифметического их математических ожиданий будет по абсолютной величине сколь угодно малым.

27) Точечная оценка дисперсии, формула ее вычисления, свойства

Точечная оценка дисперсии

Оценкой дисперсии является выборочная дисперсия

$$s^2 = \frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^2$$

Вычислим математическое ожидание выборочной дисперсии. Для этого преобразуем выражение для s^2 (через M обозначено математическое ожидание генеральной совокупности):

$$s^2 = \frac{1}{n}\sum_{i=1}^{n}\left((x_i - M) - (\bar{x} - M)\right)^2 =$$

$$= \frac{1}{n}\left[\sum_{i=1}^{n}(x_i - M)^2 - 2(\bar{x} - M)\sum_{i=1}^{n}(x_i - M) + n(\bar{x} - M)^2\right] =$$

Точечная оценка дисперсии

Для дисперсии σ^2 случайной величины ξ можно предложить следующую оценку:

$\overline{DX} = \frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^2$, где $\bar{x}$ — выборочное среднее.

Доказано, что эта оценка состоятельная, но *смещенная*.

В качестве состоятельной *несмещенной* оценки дисперсии используют величину

$$s^2 = \frac{1}{n-1}\sum_{i=1}^{n}(x_i - \bar{x})^2 = \frac{1}{n-1}\left(\sum_{i=1}^{n}x_i^2 - n(\bar{x})^2\right).$$

Именно несмещенностью оценки s^2 объясняется ее более частое использование в качестве оценки дисперсии.

$$\overline{D_в} = \frac{1}{n}\sum_{i=1}^{k} n_i(x_i - \overline{x_в})^2$$

$$\frac{1}{n}\sum_{i=1}^{k}\left((n_i x_i) - (\overline{x_в})^2\right)$$

Отметим, что выборочная дисперсия является смещенной оценкой генеральной дисперсии. $M(\overline{D_в}) = \frac{n-1}{n}D$

Поэтому рассмотрим исправленную выборочную дисперсию

$D_{исправл\ выб} = \frac{n}{n-1}D_в$ Эта дисперсия является состоятельной и эффективной оценкой генеральной дисперсии.

28) Интервальные оценки доверительной вероятности

Интервальной называют оценку, которая определяется двумя числами – началом и концом интервала. Интервальные оценки позволяют установить точность и надежность оценок.

Доверительной вероятностью, или ***надежностью, оценки*** называется вероятность γ, с которой выполняется неравенство $|\theta - \tilde{\theta}| < \varepsilon$, т. е. $\gamma = P(|\theta - \tilde{\theta}| < \varepsilon)$, где θ – оцениваемый параметр, ε – точность оценки.

Интервальной оценкой параметра θ называется интервал, границы которого $\hat{\theta}_1 = \hat{\theta}_1(x_1, x_2, \ldots, x_n)$ и $\hat{\theta}_2 = \hat{\theta}_2(x_1, x_2, \ldots, x_n)$ являются функциями выборочных значений и который с заданной вероятностью γ накрывает истинное значение оцениваемого параметра θ:

$$\mathbf{P}(\hat{\theta}_1(x_1, x_2, \ldots, x_n) < \theta < \hat{\theta}_2(x_1, x_2, \ldots, x_n)) = \gamma.$$

Интервал $(\hat{\theta}_1; \hat{\theta}_2)$ называется ***доверительным интервалом***; число γ - ***доверительной вероятностью*** или ***надёжностью*** интервальной оценки; значение $\alpha = 1 - \gamma$ - ***уровнем значимости***.

Доверительную вероятность обычно берут близко к 1. Т.к концы доверительного интервала случайны, мы можем доверительным интервалом называть такой интервал, который с заданной вероятностью покрывает значение оцениваемого параметра. Обычно его берут симметричным. Для построения доверительного интервала необходимо знать/предполагать закон распределения генеральной совокупности (для точечных он не требовался). Доверительный интервал для наизвестного мат.ожидания нормального распредеения случайной величины при известной дисперсии

$$p\left(\bar{x}_в - t_\gamma \frac{\delta}{\sqrt{n}} < a < x_в + t_\gamma \frac{\delta}{\sqrt{n}}\right) = \gamma$$

n – объем выборки, $\delta = \sqrt{D_\xi} = \sqrt{\delta^2} = \delta$, t_γ-квантираспределение Лапласа при значении $\gamma/2$

Выбор доверительной вероятности определяется конкретными условиями. Обычно используются значения 0,90; 0,95; 0,99; 0,9973, т. е. такие, чтобы получить интервал, который с большой вероятностью накроет истинное значение оцениваемого параметра.

- Уровень значимости α - это вероятность, с которой значение параметра не попадает в доверительный интервал.

29) Доверительный интервал для неизвестного математического ожидания нормального распределения СВ при известной дисперсии

Доверительный интервал для математического ожидания m ***в случае выборки из нормального распределения с известной дисперсией*** σ^2 определяется соотношением

$$\bar{x} - u_\alpha \frac{\sigma}{\sqrt{n}} < m < \bar{x} + u_\alpha \frac{\sigma}{\sqrt{n}},$$

где n – объем выборки; $\bar{x}$ – выборочное среднее; α – уровень значимости; u_α – квантиль нормального распределения, удовлетворяющая уравнению $\Phi(u_\alpha) = \gamma/2$ и определяемая из таблицы функции Лапласа; $u_\alpha \frac{\sigma}{\sqrt{n}} = \varepsilon$ – точность оценки.

Доверительный интервал — это интервал, построенный с помощью случайной выборки из распределения с неизвестным параметром, такой, что он содержит данный параметр с заданной вероятностью.

30) Доверительный интервал для неизвестного математического ожидания нормального распределения СВ при НЕизвестной дисперсии

Доверительный интервал — это интервал, построенный с помощью случайной выборки из распределения с неизвестным параметром, такой, что он содержит данный параметр с заданной вероятностью.

Доверительный интервал для математического ожидания m ***в случае выборки из нормального распределения с неизвестной дисперсией*** σ^2 определяется формулой

$$\bar{x} - t_{\alpha;n-1}\frac{s}{\sqrt{n}} < m < \bar{x} + t_{\alpha;n-1}\frac{s}{\sqrt{n}},$$

где n – объем выборки; $\bar{x}$ – выборочное среднее; s^2 – несмещенная оценка дисперсии; α – уровень значимости, $t_{\alpha;n-1}$ – квантиль распределения Стьюдента, удовлетворяющая уравнению $P(|t_{n-1}| \geq t_{\alpha;n-1}) = \alpha$ для случайной величины t_{n-1}, имеющей распределение Стьюдента с числом степеней свободы $k = n - 1$.

- Уровень значимости α - это вероятность, с которой значение параметра не попадает в доверительный интервал.

Обычно уровень значимости равен 0.01, 0.05, 0.1.

Теорема

Доверительный интервал для среднего при неизвестной дисперсии, но большой выборке ($n > 30$), *имеет вид* $\left(\bar{x} - \frac{s}{\sqrt{n}}z_\alpha; \bar{x} + \frac{s}{\sqrt{n}}z_\alpha\right)$.

Самый проблемный случай для любого исследователя, когда выборка маленькая и про её параметры ничего неизвестно. Если дисперсия неизвестна и объем выборки небольшой ($n \leq 30$), тогда вместо нормального распределения теперь используется t-распределение.

Теорема

Доверительный интервал в этом случае имеет вид
$(\bar{x} - \frac{s}{\sqrt{n}}t_\alpha(n-1); \bar{x} + \frac{s}{\sqrt{n}}t_\alpha(n-1))$

31) Проверка статистических гипотез

Цель статистической проверки гипотез состоит в том, чтобы на основании выборочных данных принять решение о справедливости основной гипотезы H0. Гипотезы называются статистическими, если они касаются параметров СВ или вида ф-ии распределения, к-е формулируются на основании выборки. Если з.распределения выборки известен и рассм. Гипотеза о параметрах этого закона, то такая гипотеза называется параметрической. Если рассм. Вопрос о неизвестном з.распределения генеральн.совокупности, то говорят о непараметрических гипотезах.Статистическая гипотеза – простая,если она содержит только 1 предположение.

Шаги проверки статистических гипотез следующие:

- формулируется основная гипотеза H_0 и альтернативная гипотеза H_1;
- выбирается статистический критерий, с помощью которого будет проверяться гипотеза;
- задаётся значение уровня значимости α;
- находятся границы области принятия гипотезы;
- делается вывод о принятии или отвержении основной гипотезы H_0.

Рассмотрим эти шаги и связанные с ними понятия подробнее.

Нулевая гипотеза (H_0) – утверждение о параметре генеральной совокупности (параметрах генеральных совокупностей) или распределении, которое необходимо проверить.

Альтернативная гипотеза (H_A) – утверждение, противоположное нулевой гипотезе. Выдвигается, но не проверяется.

Все гипотезы можно разделить на двусторонние (ненаправленные) и односторонние (направленные).

Проверка гипотезы о равенстве мат ожидания заданному значению (критерий Стьюдента**). Проверка гипотезы о равенстве (может ещё быть а) больше, б) меньше) заданному значению дисперсии норм. Распределения (**Критерий хи-квадрат**). Сравнение двух дисперсий нормально распределённых случайных величин**(критерий Фишера). **Сравнение нескольких дисперсий нормально распределённых случайных величин, если объём выборок одинаковый (**критерий Кофмана**). Сравнение двух математических ожиданий в случаи независимых нормально распределённых случайных величин.** Этот критерий используется, когда мы хотим, например, узнать, дают ли два способа, две технологии и т.д. одинаковый результат. Тогда используем этот критерий. И, выбрав этот критерий, нужно сначала проверить однородность дисперсий, т.е. проверить 3 критерий выборок. Если приняли гипотезу 3-его критерия, то использовать 5-ый критерий.

Для проверки статистических гипотез по данным выборки находят частное значение критерия $К_{наблюдаемое}$, после выбора определенного статистич.критерия множество его возможных значений разбивают на 2 непересекающ. множества, одно из к–х назыв обл принятия гипотезы или обл допустимого значения критерия, второе – критическая область. Это такая совокупность значений критерия К, при котором нулевую гипотезу отвергают.

Соотв. областью принятия гипотезы называют совокупность значений критерия К, при котором нулевую гипотезу принимают.

Если наблюдаемое значение статистического критерия Кнабл. $\in$ критической области, то нулевую гипотезу H0 отвергают в пользу альтернативной. Иначе нет оснований по выборке отвергнуть гипотезу.

32) Критерий Пирсона

Критерий Пирсона - это универсальный метод математической статистики. Он применяется для оценки значимости различий между двумя или несколькими относительными признаками. **Это критерий согласия.**

$\chi^2_{\text{наблюдаемое}} = \sum_{i=1}^{k} \frac{(n_i - npi)^2}{np_i}$. Сравнивается с табличной величиной $\chi_{\propto, k-l-1}$, l – число параметров распределения, определяемых по выборке.

Если предполагаемое распределение имеет нормальный закон распределения, то число степеней свободы оценивают по двум параметрам (математическое ожидание и среднеквадратическое отклонение) и формула имеет вид: **k=*l*−3**

Критерий Пирсона

Назначения критерия

Критерий χ^2 применяется в двух целях:

1) для сопоставления *эмпирического* распределения признака с *теоретическим* - равномерным, нормальным или каким-то иным;

2) для сопоставления *двух, трех или более эмпирических* распределений одного и того же признака.

Алгоритм:

1. Выбор теоретического закона распределения (обычно задан заранее, если не задан - анализируем выборку, например, с помощью гистограммы относительных частот, которая имитирует плотность распределения).
2. Оцениваем параметры распределения по выборке (для этого вычисляется математическое ожидание и дисперсия): a, σ для нормального, a, b - для равномерного, λ - для распределения Пуассона и т.д.
3. Вычисляются теоретические значения частот (через теоретические вероятности попадания в интервал) и сравниваются с исходными (выборочными).
4. Анализируется значение статистики χ2 и делается вывод о соответствии (или нет) теоретическому закону распределения.

Если хи-квадрат наблюдаемое будет меньше хи-квадрат табличное, то мы принимаем гипотезу.

Критерий Пирсона, или критерий χ2(Хи-квадрат) - применяют для проверки гипотезы о соответствии эмпирического распределения предполагаемому теоретическому распределению F(x) при большом объеме выборки ($n \geq 100$). Критерий применим для любых видов функции F(x), даже при неизвестных значениях их параметров, что обычно имеет место при анализе результатов механических испытаний. В этом заключается его универсальность.

33) Целые числа. Свойства делимости. Простые числа и их свойства

N={0,1,2,…} множество натуральных чисел, Z = {0, ±1,±2,…} множество целых чисел, Q={m/n, m∈ $Z, n \in N *$}, N* = {1,2,..} – множество натуральных положительных чисел, R – множество действительных (вещественных чисел). **Целые числа** — это расширенное множество натуральных чисел, которое можно получить, если добавить к ним нуль и противоположные натуральным отрицательные числа. Множество целых чисел обозначают **Z**.

Делимость

Определение. Пусть $a,b \in \mathbf{Z}$, $b \neq 0$. Числа $q \in \mathbf{Z}$ и $r \in \{0,1,\ldots,|b|-1\}$ называются соответственно неполным частным и остатком от деления a на b, если выполнено равенство

$$a = bq + r.$$

При этом, если $r = 0$, то говорят, что a делится на b, или что b делит a, или что b является делителем a (обозначение $a \vdots b$ или $b|a$.

Для каждого a и b существуют числа q и r, такие что a=bq+r, r – остаток, q – частное. Если r=0, то говорят, что a делится на b, и a делится на q. Или говорят, что число a кратно числу b, b и q – называются делителями числа a.

Определение. Наибольшим общим делителем целых чисел $a_1, a_2, \ldots, a_n$, из которых хотя бы одно отлично от нуля, называется наибольшее натуральное число, на которое делится каждое из этих чисел (обозначение $(a_1, a_2, \ldots, a_n)$).

Определение. Числа $a,b \in \mathbf{Z}$ называются взаимно простыми, если $(a,b) = 1$.

Свойства. Пусть $a,b,c \in \mathbf{Z}$.

1. Если $a|b$, $b|c$, то $a|c$ (свойство транзитивности).
2. Если $a|b$, $a|c$, то $a|b + c$.
3. Если $a|b$, то для всех целых c имеет место $a|bc$.
4. Если $ac|bc$ и $c \neq 0$, то $a|b$.
5. Пусть $a|bc$ и $(a,c) = 1$. Тогда $a|b$.
6. Если $a|c$, $b|c$ и $(a,b) = 1$, то $ab|c$.
7. $(a,b)\cdot[a,b] = a\cdot b$.
8. $(a,b\pm a) = (a,b)$.

Все целые числа делятся на 1. Все натуральные числа являются делителями нуля. Единственный делитель единицы – сама единица. Пусть целое число a делится на натуральное число m, а число m в свою очередь делится на натуральное число k, тогда a делится на k (свойство транзитивности деления). Натуральное число n>1 называется **простым**, если оно имеет в точности два различных натуральных делителя – 1 и n, в противном случае n называется составным. 1) Если простое число p делится на простое число q, то эти числа равны (p=q). 2) Если p- простое число, то любое натуральное число либо делится на p, либо взаимно простое с p. 3) Произведение натуральных чисел a и b делится на простое число p в том случае, когда хотя бы одно из этих чисел делится на p. 4) Любое натуральное число, отличное от 1, является либо простым, либо произведением простых чисел

5) Среди простых чисел нет наибольшего, множество простых чисел бесконечно
6) Если m*n делится на простое число p , то m делится на p или n делится на p.

34) Критерий взаимной простоты чисел. Основная теорема арифметики

Простые числа делятся на себя и на единицу. Если число n>1 не делится ни на одно простое число $p \le \sqrt{n}$, то n – простое.

Два целых числа a и b называются взаимно простыми, если их наибольший общий делитель равен единице, то есть, НОД(a, b)=1. Проще говоря, взаимно простые числа — это целые числа, у которых нет общих делителей, кроме единицы. **Наибольшим общим делителем** двух чисел a и b называется наибольшее число, на которое a и b делятся без остатка. Для записи может использоваться аббревиатура НОД. Для двух чисел можно записать так: НОД (a, b). Числа, которые содержат больше двух множителей, то есть делятся на несколько чисел, называют **сложными**. Сложные числа состоят из перемноженных простых.

Любое целое положительное и отличное от единицы число a либо делится на простое число p, либо a и p – взаимно простые числа. Если произведение нескольких целых положительных и отличных от единицы множителей делится на простое число p, то хотя бы один множитель делится на p.

Основная теорема арифметики утверждает возможность разложения любого целого числа, которое больше единицы, на простые множители. Любое целое число, которое больше 1, можно разложить на произведение простых множителей, причем это разложение единственно, если не учитывать порядок следования множителей. Все составные числа, которые могут быть разложены на множители, представлены произведением простых чисел; то есть все их множители — простые числа.

каждое натуральное число $n > 1$ можно факторизовать (разложить) в виде $n = p_1 \cdot \ldots \cdot p_k$, где $p_1, \ldots, p_k$ — простые числа, причём такое представление единственно, если не учитывать порядок следования множителей.

Как следствие, каждое натуральное число n представимо в виде

$n = p_1^{d_1} \cdot p_2^{d_2} \cdot \ldots \cdot p_k^{d_k}$, где $p_1 < p_2 < \ldots < p_k$ — простые числа, а $d_1, \ldots, d_k$ — некоторые натуральные числа,

и притом *единственным* образом. Такое представление числа n называется его **каноническим разложением** на простые сомножители.

35) НОК и НОД, алгоритм Евклида

Наибольшим общим делителем чисел *a* и *b* называется наибольшее число, на которое *a* и *b* делятся без остатка. Обозначается (a,b). Наименьшее общее кратное (НОК) чисел *a* и *b* — это наименьшее число, которое кратно *a* и *b*. Другими словами, это такое маленькое число, которое делится без остатка на число *a* и число *b*.

Для любых чисел A и B, B≠0 существуют такие q, r, что A=B*q+r, причем 0≤r<|B|. q называется полным частным, а r называется остатком от деления, они единственны. Алгоритм Евклида – это алгоритм нахождения наибольшего общего делителя (НОД) пары целых чисел.

Алгоритм Евклида заключается в построении ряда чисел следующего вида (|a|>|b|):

$a = b*q_1 + r_1;$

$b = r_1*q_2 + r_2;$

$r_1 = r_2*q_3 + r_3;$

…

$r_{n-1} = r_n*q_{n+1} + 0$

Для нахождения наибольшего общего делителя двух чисел a и b (a и b – целые положительные числа, причем a больше или равно b) последовательно выполняется деление с остатком, которое дает ряд равенств вида

$$a = b \cdot q_1 + r_1, \quad 0 < r_1 < b$$

$$b = r_1 \cdot q_2 + r_2, \quad 0 < r_2 < r_1$$

$$r_1 = r_2 \cdot q_3 + r_3, \quad 0 < r_3 < r_2$$

$$r_2 = r_3 \cdot q_4 + r_4, \quad 0 < r_4 < r_3$$

$$\vdots$$

$$r_{k-2} = r_{k-1} \cdot q_k + r_k, \quad 0 < r_k < r_{k-1}$$

$$r_{k-1} = r_k \cdot q_{k+1}$$

Деление заканчивается, когда $r_{k+1}=0$, при этом r_k=НОД(a, b).

36) Соотношение Безу

Соотношение Безу — соотношение между парой целых чисел и их наибольшим общим делителем. Это следует из алгоритма Евклида. НОД (a,b) = xa + yb, x, y – коэффициенты Безу. Числа a и b называются взаимно простыми, если их НОД = 1. Из соотношения Безу следует, что для взаимно простых чисел существуют числа au + bV = 1. Для взаимно простых чисел можем записать следующее свойство: 1) Если НОД (a_1, a_2, …, a_k) = d, то $(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_k}{d}) = 1$ – взаимно простые числа. 2) Если число c делит произведение ab, и число c взаимно просто a, то c делит b, записывается c | a*b и (c,a)=1, то c | b. 3) Если a и b1 взаимно простые, а и b2 тоже взаимно простые, то a взаимно просто b1*b2, записывается (a,b1)=1, (a,b2)=1, то (a,b1*b2)=1.

Пусть a, b – целые числа, хотя бы одно из которых не ноль. Тогда существуют такие целые числа x, y, что выполняется соотношение

$$\text{НОД}(a, b) = x \cdot a + y \cdot b$$

$\text{НОД}(12, 30) = 6$. Соотношение Безу имеет вид:

$$6 = 3 \cdot 12 + (-1) \cdot 30$$

- Возможны и другие варианты разложения НОД, например:

$$6 = (-2) \cdot 12 + 1 \cdot 30.$$

Следствие:

Если числа a, b взаимно простые, то уравнение:

$$ax + by = 1$$

имеет целочисленные решения[4]. Этот важный факт облегчает решение диофантовых уравнений первого порядка.

$\text{НОД}(a, b)$ является наименьшим натуральным числом, которое может быть представлено в виде линейной комбинации чисел a и b с целыми коэффициентами[5].

Нахождение коэффициентов Безу эквивалентно решению диофантового уравнения первого порядка с двумя неизвестными:

$$ax + by = d, \text{ где } d = \text{НОД}(a, b).$$

Или, что то же самое:

$$\frac{a}{d}\, x + \frac{b}{d}\, y = 1$$

Отсюда следует, что коэффициенты Безу x, y определены неоднозначно — если какие-то их значения $x_0 . y_0$ известны, то всё множество коэффициентов даётся формулой[7]:

$$\left\{ \left(x_0 + \frac{kb}{d},\ y_0 - \frac{ka}{d} \right) \mid k = 0, \pm 1, \pm 2, \pm 3 \ldots \right\}$$

Ниже будет показано, что существуют коэффициенты Безу, удовлетворяющие неравенствам $|x| < \left|\frac{b}{d}\right|$ и $|y| < \left|\frac{a}{d}\right|$.

37) Диафантовые линейные уравнения

Таким уравнением называется уравнение вида $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$, где a_1,a_2,a_n,b – целые числа и решение ищут в целых числах. Чаще всего уравнение рассматривается относительно двух переменных ax+by=c. Если НОД (a,b) не существует, то уравнение не имеет решений. ax+by=c при условии (a,b)|c (НОД чисел a и b делим с c). $\frac{A}{d}x + \frac{b}{d}y = \frac{c}{d}$. Шаги решения 1) Находим НОД (a,b) = d. 2) Проверяем, что c/d, если это так то 3) находим коэффициенты соотношения Безу au+bV=d 4) Умножаем обе части соотношения Безу на отношение $\frac{c}{d}$, получаем $\frac{auc}{d} + \frac{bVc}{d} = c$, причем $x0 = \frac{uc}{d}, y0 = \frac{Vc}{d}$

Общее решение диафантового уравнения имеет вид:

$$x = x_0 + \frac{b}{d}t$$

$$y = y_0 + \frac{a}{d}t, t \in Z$$

38) Сравнение целых чисел. Свойства сравнений

Пусть имеется произвольное число m. Тогда для любых чисел a и b равносильно следующее утверждение: 1) a и b имеют одинаковые остатки от деления на m

2) a-b делится на m, a-b=mq для некоторого целого q 3) a = b+mq Определение. Целые числа a и b называются сравнимыми по модулю m, если они удовлетворяют любому из трех условий, названных выше. Записывается a≡b(mod m). Сравнение обладает следующими свойствами: 1) Обеим частям сравнения можно прибавить/вычесть одно и то же число, $a \pm c \equiv b \pm c (mod\ m)$ 2) Можно почленно складывать и вычитать сравнения по модулю, a≡b(mod m), c≡d(mod m) значит $a \pm c = (b \pm d)$mod m 3) Сравнение по модулю m можно почленно перемножать a≡b(mod m), c≡d(mod m) значит a*c = (b*d) mod m 4) Сравнение можно возводить в любую натуральную степень $a^k=b^k$(mod m) 5) Если сравнении a≡b(mod m) числа a,b,m имеют общий делитель d, то их можно на него сократить 6) Сравнение можно сократить на общий множитель a и b, если он взаимно простой с модулем m $a=a_1d$, $b=b_1d$, (d,m)=1. Тогда a≡b(mod m) => $a_1 \equiv b_1$(mod m).

Также существуют такие свойства как 1) Рефлексивность сравнения a≡a(mod m) 2) Симметричность сравнения. Если a≡b(mod m), то b≡a(mod m) 3) Транзитивность (свойство переходит) Если a≡c(mod m), а c≡b(mod m), то a≡b(mod m). Эти 3 свойства означают, что отношение сравнимости на множестве целых чисел есть отношение эквивалентности. Это означает, что множество целых чисел разбивается на непересекающиеся классы попарно сравнимых друг с другом по mod m целых чисел. Каждый класс сравнимых друг с другом целых чисел характеризуется общими свойствами представителей этого класса: (a,m)=(b,m), если a≡b(mod m). Такие классы называются классами вычетов.

39) Множество классов вычетов

Множество целых чисел разбивается на непересекающиеся классы попарно сравнимых др с др по mod m целых чисел. Каждый класс сравнимых друг с другом чисел характеризуется общими св-ми представителей этого класса.

(a,m)≡(b,m); если a≡b(mod m). Такие классы называют классами вычетов. При делении любого целого числа на число m существуют m-остатки: 0, 1, 2…m-1. Обозначать классы будем $\bar{0}, \bar{1}, \bar{2}, \ldots \overline{m-1}$. Любой представитель конкретного класса полностью определяет свойства класса, множество всех классов называется множеством классов вычетов по mod m, обозначение Z/mZ=$\{\bar{0}, \bar{1}, \bar{2}, \ldots \overline{m-1}\}$ Пусть $\bar{k}, \bar{l} \in$ Z/mZ. Возьмем представителей k1, k2 $\in \bar{k}$; $l1, l2 \in \bar{l}$. Тогда k1+k2 $\in \bar{k}$, $l1+l2 \in \bar{l}$. А вот k1+ $l1 \in \bar{k}+\bar{l}$; k2+ $l2 \in \bar{k}+\bar{l}$. Аналогично с произведением. Сложение и умножение классов вычетов определяется через сложение и вычитание чисел, поэтому для них стандартные свойства: коммутативность, ассоциативность, существует нейтральный элемент по сложению и нейтральный элемент по умножению. Например $Z/_6Z = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$. Тогда $\bar{3} + \bar{5} = \bar{2}$, мы складываем 3+5 = 8 и делим на 6, остаток будет 2. В каждом множестве класса вычетов числа, которые дают одни остатки при делении на 1, 2 и так далее.

Для каждого класса существует противоположный класс по сложению. Если класс $\bar{k} \in$ Z/mZ, (k,m) ≡1. Для каждого класса $\bar{l}$, отличного от 0, произведение $\bar{k}*\bar{l} \neq 0$. Произведение k на любой из классов ≠ произведению k на другой класс. Существует обратимый класс $\bar{k}$ ∃ k^{-1}. Множество обратимых классов образует ПСВ (приведенную с-му вычетов). Z*/mZ включает только те классы, остатки которых взаимно просты с m. Их количество – функция $\varphi(m)$ штук – описывается функцией Эйлера. Класс обратим, если найдется другой класс из класса вычетов, что $\bar{a}$ обратим если существует $\bar{b} \in$ Z/mZ, что $\bar{a}*\bar{b}=1$ (в остатке дает 1 их произведение). $\bar{b}$ обратимый к $\bar{a}$, он единственный, обратный класс определяется однозначно.

Класс $\bar{k} \in$ Z/mZ обратим тогда и только тогда, когда представитель класса взаимно прост с m. Если m – простое число, то во множестве Z/mZ каждый ненулевой элемент обратим. Поскольку Z/mZ состоит из конечного числа элементов, то + и * в нем можно задавать таблицами Кэли. Например, таблица Кэли для $Z/_6Z$.

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

*	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

40) Функция Эйлера. Теорема Эйлера. Малая теорема Ферма

$\varphi(m)$, φ – количество чисел, взаимно простых с m и меньших m. Например, для числа 36 существует 12 меньших его и взаимно простых с ним чисел (1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35), поэтому φ (36)=12. Функция Эйлера определена на множестве натуральных чисел, и значения её лежат в множестве натуральных чисел. Чтобы вычислить $\varphi(p)$, нужно перебрать все числа от 1 до p-1, и для каждого проверить, имеет ли оно общие делители с p, а затем подсчитать, сколько чисел оказались взаимно простыми с p. Свойства функции:

1) $\varphi(p) = p - 1$ 2) $\varphi(p^s) = p^s - p^{s-1}$ 3) Если (n,m)=1 φ (m*n) = φ (m) * φ (n)

4) $\varphi(n)$, $n = p_1^s p_2^s \ldots p_k^{S_k}$ $\varphi(n) = n\left(1 - \frac{1}{p1}\right)\left(1 - \frac{1}{p2}\right) \ldots (1 - \frac{1}{p_k})$ – нахождение функции Эйлера.

Теоре́ма Э́йлера в теории чисел гласит:

Если a и m взаимно просты, то $a^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — функция Эйлера.

Важным следствием теоремы Эйлера для случая простого модуля является малая теорема Ферма:

Если a не делится на простое число p, то $a^{p-1} \equiv 1 \pmod{p}$.

φ(m) Функция Эйлера ставит в соответствие каждому натуральному числу m>1 количество натуральных чисел (<m), взаимно простых с m. Если, например, m=45, то функция Эйлера покажет, сколько чисел <45 взаимно просты с числом 45.

Малая теорема Ферма. Если p простое, а целое, НОД(a,p)=1 тогда и только тогда, когда (a,p)=1 ⇔ $a^{p-1} - 1 \equiv 0 \pmod{p}$.

41) Решение линейных сравнений

5.1. Решение линейного сравнения. Сравнение степени $n = 1$ имеет вид $a_0 + a_1 x \equiv 0 \pmod m$, $a_1 \not\equiv 0 \pmod m$, поэтому его можно записать в виде

$$ax \equiv b \pmod m, \quad a \not\equiv 0 \pmod m. \tag{5.1}$$

Предложение 5.2 (критерий совместности линейного сравнения)**.** *Сравнение 5.1 совместно тогда и только тогда, когда* $(a, m) \mid b$.

Теорема 5.1. *Пусть* $ax = b \pmod m$ *— совместное сравнение первой степени,* $d = (a, m)$*. Тогда множество* X *всех решений этого сравнения состоит из одного класса вычетов по модулю* m/d*:*

$$X = \bar{x}_0 \in \mathbb{Z}_{m/d}, \quad x_0 \text{ — частное решение.}$$

Решить сравнение — значит найти все удовлетворяющие ему x. Если x - решение сравнения, то решением является весь класс вычетов, содержащий x. Сравнения с одинаковым множеством решений называются равносильными. Пусть НОД(a,m)=d. Сравнение $ax \equiv b \pmod m$ невозможно, если b не делится на d. При b, кратном d, сравнение имеет d решений.

$ax \equiv b \pmod m$, (a,b)=d. Составим новое сравнение $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$, обозначим его $a_d x \equiv b_d \pmod{m_d}$ Пусть его решением будет x0, тогда остальные решения найдутся по следующей формуле: $x_n = x_{n-1} - m_d$ (следует понимать, что x_i вычет по модулю, поэтому в этой формуле можно сменить знак, для удобства), всего решений будет d.

Пример 1.

$12x \equiv 6 (mod\ 18)$

Найдем НОД $(12, 18) = 6$

Перейдем к новому сравнению $2x \equiv 1(3)$

Легко находится $x_0 = 2$

Тогда ответом будет $x_0 = 2, x_1 = x_0 - \frac{m}{(a,m)} = -1, x_2 = -4$

42) Алгебраические операции. Понятие группы и подгруппы, примеры

Пусть X – некоторое множество и введем на множестве X бинарную алгебраическую операцию – правило, по которому каждой упорядоченной паре (x,y) ∈ X x X, где x ∈ X, y ∈ X элементов ставит в соответствие единственный элемент Z из множества X: (x,y) -> Z∈ X. Алгебраическую операцию обозначают *. Это общее обозначение. +, x, *, °, бинарная алгебраическая операция – такая операция, которая каждой упорядоченной паре например множества G ставит в соответствие некоторый элемент c ∈ G, a*b=c, c∈ G

Группа – непустое множество G с определенной на нем бинарной алгебраической операцией *, обозначаем {G, *}, эта операция обладает свойствами: 1) Ассоциативность: (a*b)*c = a*(b*c) 2) Существует нейтральный элемент, такой что a*e = e*a = a 3) Для любого a ∈ G существует обратный элемент a^{-1}, такой что $a^{-1} * a = a * a^{-1} = e$. Если соблюдается, что алгебраическая операция имеет свойство коммутативности, a*b=b*a, то группа является АБЕЛЕВОЙ (коммутативной). Группы с операцией умножения называются мультипликативными группами. Группы бывают конечные и бесконечные. Один из примеров группы - множество целых чисел, снабжённое операцией сложения: сумма любых двух целых чисел также даёт целое число, роль нейтрального элемента играет ноль, а число с противоположным знаком является обратным элементом. Пусть имеется группа (G, *), тогда подгруппой H ⊂ G (входит в G) называется такое множество, которое является группой относительно той же алгебраической операции, что и в G. Подгруппа называется собственной, если она не совпадает с этой группой и единичным элементом.

Подгруппа — подмножество H группы G, само являющееся группой относительно операции, определяющей G.

Подмножество H группы G является её подгруппой тогда и только тогда, когда:

1. H содержит единичный элемент из G
2. содержит произведение любых двух элементов из H,
3. содержит вместе со всяким своим элементом h обратный к нему элемент h^{-1}.

Подмножество группы G, состоящее из одного элемента 1, будет, очевидно, подгруппой, и эта подгруппа называется единичной подгруппой группы G. Сама G также является своей подгруппой. Пересечение двух подгрупп будет также подгруппой. Напр, группа четных чисел будет подгруппой группы целых чисел.

Подгруппа – подмножество в группе, которое обладает теми же свойствами, что и группа. У любой группы 2 тривиальные подгруппы: нейтральный элемент и сама группа.

43) Порядок элементов в группе. Циклические группы

Рассмотрим фиксированный элемент данной группы G и подгруппу из всевозможных степеней целых данного элемента: a∈ G, H=$\{a^{-2}, a^{-1}, a^0, \dots a^k, \dots\}$ a^0- единичный элемент. Это множество является подгруппой. Такая подгруппа называется циклической подгруппой, порожденной данным элементом <a>. Если a∈ G, a^n = e, тогда циклическая группа, порожденная a, конечная и имеет порядок n. Величина n – порядок элемента в данной группе. Если для всех n $a^n \neq e$, то говорят об элементе бесконечного порядка. Порядок элемента a группы G - это минимальное положительное число k, для которого справедливо равенство a^k=e (где e - единичный элемент группы). То есть - порядок элемента группы - это минимальная положительная степень, в которой данный элемент равен единице. Циклическая группа - группа (G, *), которая может быть порождена одним элементом a, то есть все её элементы являются степенями a. Обозначение: G=<a>.

Теорема 1.3.2. *Пусть a – фиксированный элемент произвольной группы G. Пусть* $< a >= \{a^0 = e, a, a^2, \dots, a^{-1}, a^{-2}, \dots\}$ *– множество всевозможных степеней элемента a. Тогда* $< a >$ *– подгруппа группы* G*, причем абелева.*

Определение 1.3.8. Подгруппа $< a >$ из теоремы 1.3.2 называется циклической подгруппой группы G, порожденной элементом a. Если в группе G найдется такой элемент b, что $G =< b >$, то такую группу называют циклической.

При этом элемент b называют примитивным, или образующим элементом группы.

44) Смежные классы. Теорема Логранжа

Пусть H – подгруппа группы G и произвольный элемент a∈ G, H<G, тогда левым смежным классом группы G по H называется множество элементов aH={ah | h∈ H}. Аналогично определяется и правый смежный класс aH.

Пусть G — группа, H — подгруппа группы G, $x \in G$. *Левым смежным классом группы G по подгруппе H*, порожденным элементом x, называется множество

$$xH = \{xh \mid h \in H\}.$$

Аналогично, *правый смежный класс* определяется как

$$Hx = \{hx \mid h \in H\}.$$

1) Теорема: Левые(правые) смежные классы G по подгруппе H либо не пересекаются, либо совпадают. 2) 2 любых элемента a и b ∈ G принадлежат одному левому смежному классу, когда a^{-1}*b ∈ H. Для правых смежных классов: a * b^{-1}∈ H. 3) Если H – конечная группа, то для всякого a из группы G число элементов множеств aH совпадают. 4) Группа G – всегда объединение попарно непересекающихся левых(правых) смежных классов по подгруппе H. Количество всех различных левых(правых) смежных классов группы по подгруппе называется индексом подгруппы H в группе G, обозначается G:H. Порядок конечной группы = произведению порядка и индекса любой ее подгруппы.

Теорема Логранжа: В конечных группах порядок любой подгруппы делит порядок группы. Таким образом если G конечная группа порядка n, то для любого элемента из этой группы a^n=e.

Пусть группа G конечна, и H - её подгруппа. Тогда порядок G равен порядку H, умноженному на количество её левых или правых классов смежности (индекс подгруппы). Количество правых и левых смежных классов любой подгруппы H в G одинаково и называется индексом подгруппы H в G (обозначается G:H).

45) Нормальные подгруппы. Фактор группы

Подгруппа H группы G называется нормальной, если каждый ее правый смежный класс по подгруппе совпадает с левым смежным классом, то есть aH = Ha. Если группа коммутативна, то в ней все подгруппы нормальные.

Теорема 3. *Подгруппа $H = (T; *)$ является нормальной подгруппой группы $G = (S, *)$ тогда и только тогда, когда для каждого элемента $a \in S$ для любого элемента $h \in H$ верно, что*

$$a' * h * a \in H,$$

где элемент a' симметричен элементу a в группе G.

Факторгруппа — множество смежных классов группы по её нормальной подгруппе, само являющееся группой с определённой специальным образом групповой операцией. Факторгруппа группы G по нормальной подгруппе H обычно обозначается G/H.

Пусть G — произвольная группа, A — ее нормальная подгруппа и S — множество всевозможных смежных класов группы G по подгруппе A (напоминаем, что левые и правые смежные классы в этом случае совпадают). *В множестве классов S введем операцию умножения, полагая*

$$xA \cdot yA = xyA.$$

Так как подгруппа A является нормальной, то *произведение $xA \cdot yA$ не зависит от выбора представителей x и y в перемножаемых классах.*

Полученная группа обозначается через G/A и называется ***фактор-группой*** *группы G по нормальной подгруппе A.*

Группа смежных классов группы G по нормальной ее подгруппе N с операцией их умножения называется **фактор-группой** группы G по подгруппе N и обозначается G/N.

Теорема 5. *Порядок фактор-группы G/N конечной группы G по нормальной ее подгруппе N равен индексу подгруппы N в группе G, т.е.*

$$|G/N| = (G : N) = \frac{|G|}{|N|}.$$

46) Понятие кольца и подкольца, примеры

Кольцо — алгебраическая структура, в которой определены операция обратимого сложения и операция умножения (2 бинарные операции), по свойствам похожие на соответствующие операции над числами. Простейшими примерами колец являются совокупности чисел (целых, вещественных, комплексных), совокупности числовых функций, определённых на заданном множестве.

Обозначается K={G, +, *}. К свойствам относятся: 1) Относительно сложения выполняется ассоциативность, коммутативность (абелева относительно сложения), существует обратный и нейтральный элемент. 2) Относительно умножения выполняется ассоциативность (ab)c = a(bc). 3) Относительно сложения и умножения выполняется дистрибутивность a(b+c) = ab+ac, (b+c)a=ab+ac.

1. $a + b = b + a$ — коммутативность сложения;
2. $a + (b + c) = (a + b) + c$ — ассоциативность сложения;
3. $\exists 0 \in R \ (a + 0 = 0 + a = a)$ — существование нейтрального элемента относительно сложения;
4. $\forall a \in R \, \exists b \in R \, (a + b = b + a = 0)$ — существование противоположного элемента относительно сложения;
5. $(a \times b) \times c = a \times (b \times c)$ — ассоциативность умножения;
6. $\begin{cases} a \times (b + c) = (a \times b) + (a \times c) \\ (b + c) \times a = (b \times a) + (c \times a) \end{cases}$ — дистрибутивность.

Кольца бывают неассоциативные, с единицей и без единицы, коммутативные и некоммутативные. Множество A⊂R, которое определено относительно операций, определенных в кольце R, называеств подкольцом. Другими словами, A называется подкольцом в R, если оно само является кольцом относительно сужения операций, определенных на R.

При обычных операциях сложения и умножения кольцом является:

1. Множество целых чисел.
2. Множество рациональных чисел.
3. Множество действительных чисел.
4. Множество рациональных чисел.

Кольцо четных целых чисел является подкольцом кольца целых чисел. Кольцо целых чисел является подкольцом кольца рациональных чисел.

47) Мультпликативная группа кольца, делители нуля

Если кольцо является ассоциативным кольцом с единицей, то множество обратимых элементов относительно умножения образуют группу, которую называют мультипликативной группой кольца. Если мультипликативная группа кольца = кольцу без 0, то такое множество называют телом, или алгеброй с делением. Коммутативное тело называют полем. Если в кольце 2 элемента, произведение которых = 0, их называют делителями нуля. К примеру, в кольцах целых чисел делителей 0 нет. В кольце векторов с операциями + и * (векторное умножение) каждый отличный от 0 элемент является делителем 0.

Определение. Пусть К—кольцо $a \in К$, $a \neq 0$. Элемент a называют делителем нуля, если существует элемент $b \in К$, $b \neq 0$ такой, что $a \cdot b = 0$.

Определение. Пусть К—коммутативное кольцо с 1 и некоторый элемент $a \in К$. Элемент a называется обратимым в кольце К, если в К существует обратный к нему элемент относительно операции умножения, т.е.

$$\exists\, a^{-1} \in К\ (a \cdot a^{-1} = a^{-1} \cdot a = 1)$$

Свойство. Обратимые элементы кольца не является делителем нуля.

Свойство. Пусть К—коммутативное кольцо с 1, через $К^*$ будем обозначать множество обратимых элементов кольца. Тогда $<К^*, \cdot>$—мультипликативная группа.

Ненулевые элементы a и b кольца $\mathbb{R}$ называют делителями нуля, если $a \cdot b = \mathbf{0}$ или $b \cdot a = \mathbf{0}$.

Элемент $x \in R$ называется **левым делителем нуля**, если существует такой $y \neq 0$, что $xy = 0$. Элемент $x \in R$ называется **правым делителем нуля**, если существует такой $y \neq 0$, что $yx = 0$. Элемент $x \in R$ называется **делителем нуля**, если он является одновременно левым и правым делителем нуля. Если умножение в кольце коммутативно, то понятия правого и левого делителя совпадают. Элемент кольца, который не является ни правым, ни левым делителем нуля, называется обычным элементом. Пример: в кольце $\mathbb{Z}_6$ элементы 2, 3, 4 — делители нуля.

48) Идеалы колец. Кольцо полиномов

Подкольцо G кольца K – левый идеал кольца K, если для любого k из кольца и для каждого j из подкольца jk ∈ J, то есть: ∀k ∈ K, ∀j ∈ J, такие что $jk \in J$

Правый идеал кольца K: ∀k ∈ K, ∀j ∈ J, такие что kj с J.

Определение 3.4.2. *Подкольцо J кольца K называется левым идеалом кольца K, если для любого $k \in K$ и для каждого $j \in J$ произведение $jk \in J$, то есть $Jk \subseteq J$. Если же $kJ \subseteq J$ для всех элементов $k \in K$, то J называют правым идеалом. Двусторонний идеал – идеал, являющийся одновременно и левым и правым идеалом.*

Двусторонний идеал является и правым, и левым. Отметим, что в коммутативном кольце все идеалы двусторонние. Ясно, что нулевой элемент и все кольцо являются тривиальными идеалами любого кольца. Если рассматривать множество кратных чисел, то оно образует двусторонний идеал кольца целых чисел. Для каждого элемента a кольца K множество aK является левым идеалом кольца K, он называется главным идеалом, порожденным элементом a, обозначение <a>. Кольцо, в котором каждый идеал главный, называется кольцом главного идеала. Отметим, что в поле нет собственных идеалов. Если в кольце есть делители 0, то они порождают собственные идеалы.

Множество целых чисел является кольцом главных идеалов.

Примером коммутативного кольца является множество полиномов (многочленов).

G={ $A(x) = a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} \ldots + a_1 x + a_0$ }

Сложение, умножение многочленов определяются обычным образом, и мы получаем коммутативное кольцо с 1. Обратимые элементы – это числа. Число x0 является корнем многочлена, если A(x0)=0.

Пусть P – поле, то есть произвольное коммутативное кольцо с единицей, у которого все элементы, отличные от нуля, обратимы, иными словами, $P^*=P\backslash\{0\}$. Например, $P=Q, R, C, Z/pZ$.

Пусть $P[x]$ – кольцо полиномов с коэффициентами из P с обычными операциями сложения и умножения многочленов. По своим свойствам полиномы близки к целым числам. Например, как и для целых чисел имеет место

Теорема 3.5.1 (о делении с остатком). *Для любых двух многочленов $f(x)$ и $g(x) \neq 0$ из кольца $P[x]$ существуют единственные многочлены $q(x)$ и $r(x)$, такие, что $f(x) = g(x)q(x) + r(x)$, причем $r(x) = 0$ или степень $r(x)$ меньше степени $g(x)$.*

49) Теорема Безу и корни многочленов

В общем случае теорема Безу звучит так: остаток от деления многочлена P(x) на двучлен (x-a) равен P(a). Отсюда также следует что множество корней многочлена P(x) тождественно множеству корней соответствующего уравнения P(x)=0.

Если в поле P существует такое натуральное n, что сумма n единичных элементов равна 0, то наименьшее n с таким свойством называется характеристикой Безу. Если для любого n сумма единичных элементов не равна 0, то говорят, что характеристика в поле равна 0.

Пусть коммутативное кольцо R с единицей содержится в целостном кольце S.

ОПРЕДЕЛЕНИЕ 1. Элемент $c \in S$ называется *корнем* (или *нулем*) *многочлена* $f \in R[X]$, если $f(c) = 0$.

Говорят также, что c — корень уравнения $f(x) = 0$.

Необходимость рассмотрения колец, содержащих кольцо R собственным образом, станет понятной, если вспомнить, что многочлен $f(X) = X^2 + 1$ не имеет корней над полем $\mathbb{R}$, но при этом для $i \in \mathbb{C}$ имеет место $f(i) = 0$.

При этом сначала мы рассмотрим случай $S = R$.

Теорема 1 (теорема Безу). *Элемент $c \in R$ является корнем многочлена $f \in R[X]$ тогда и только тогда, когда многочлен $X - c$ делит f в кольце $R[X]$.*

Пусть есть кольцо A - коммутативное с 1 целостное кольцо.

Определение. $c \in A$ - корень многочлена $f(x)$, если $f(c) = 0$.

Теорема Безу. Элемент $c \in A$ является корнем многочлена $f(x) \Leftrightarrow (x - c)$ делит $f(x)$.

Пример

Задание. Найти остаток от деления многочлена $f(x) = 3x^2 - 4x + 6$ на двучлен $(x - 1)$

Решение. Согласно теореме Безу искомый остаток равен значению многочлена в точке $a = 1$. Найдем тогда $f(1)$, для этого значение $a = 1$ подставим в выражение для многочлена $f(x)$ вместо x. Будем иметь:

$$f(1) = 3 \cdot 1^2 - 4 \cdot 1 + 6 = 3 - 4 + 6 = 5$$

Ответ. Остаток равен 5

50) Поле. Примеры полей

Поле — это числовая область, в которой есть четыре обычных арифметических операции: сложение, вычитание, умножение и деление, обладающие привычными свойствами соответствующих действий над рациональными числами. Обозначается P = {G, +, x}. Кольцо -> поле, если: 1) есть нейтральный элемент по x 2) выполняются все свойства кольца 3) нет делителей нуля (каждый элемент обратим, то есть нет чисел, что a x b = 0)

Множество $\mathbb{F}$ с двумя операциями $\mathbb{F} \times \mathbb{F} \to \mathbb{F}$: *сложением* $(a, b) \mapsto a + b$ и *умножением* $(a, b) \mapsto ab$ называется *полем*, если выполняются следующие три набора аксиом:

свойства сложения

коммутативность:	$a + b = b + a \quad \forall a, b \in \mathbb{F}$	(2-1)
ассоциативность:	$a + (b + c) = (a + b) + c \quad \forall a, b, c \in \mathbb{F}$	(2-2)
наличие нуля:	$\exists\, 0 \in \mathbb{F} : \quad a + 0 = a \quad \forall a \in \mathbb{F}$	(2-3)
наличие противоположных:	$\forall a \in \mathbb{F} \quad \exists\, (-a) \in \mathbb{F} : \quad a + (-a) = 0$	(2-4)

свойства умножения

коммутативность:	$ab = ba \quad \forall a, b \in \mathbb{F}$	(2-5)
ассоциативность:	$a(bc) = (ab)c \quad \forall a, b, c \in \mathbb{F}$	(2-6)
наличие единицы:	$\exists\, 1 \in \mathbb{F} : \quad 1a = a \quad \forall a \in \mathbb{F}$	(2-7)
наличие обратных:	$\forall a \in \mathbb{F} \setminus 0 \quad \exists\, a^{-1} \in \mathbb{F} : \quad aa^{-1} = 1$	(2-8)

свойства, связывающие сложение с умножением

дистрибутивность:	$a(b + c) = ab + ac \quad \forall a, b, c \in \mathbb{F}$	(2-9)
нетривиальность:	$0 \neq 1$	(2-10)

Пример 2.1 (поле из двух элементов)
Простейший объект, удовлетворяющий всем аксиомам из опр. 2.1 — это поле $\mathbb{F}_2$, состоящее из 0 и 1, таких что $0 + 1 = 1 \cdot 1 = 1$, а все остальные суммы и произведения равны нулю (включая $1 + 1 = 0$).

Для поля выполняются все свойства кольца (для колец нужна ассоциативность, коммутативность, обратный и нейтральный элемент по +, ассоциативность по *, дистрибутивность по * и +), есть нейтральный элемент по умножению, нет делителей нуля. Поле – коммутативное кольцо, где есть нейтральный элемент по умножению и для каждого элемента есть обратный. В поле нет делителей нуля. Рациональные, вещественные, комплексные числа, вычеты по модулю заданного простого числа образуют поля. Кольцо, состоящее из одного нулевого элемента (в котором 1 = 0), полем не считается.

Если Z/mZ, +, * m – простое, то поле, а если m – составное, это будет коммутативное кольцо. Множества рациональных чисел Q и вещественных чисел R являются примерами полей, хорошо знакомых читателю из школьного курса.

51) Характеристика поля. Примеры конечных полей. Поля Галуа

Полем называется коммутативное ассоциативное кольцо с единицей, в котором любой ненулевой элемент обратим. Кольцо, состоящее из одного нулевого элемента (в котором 1 = 0), полем не считается.

Характеристикой поля P называется число 0, если na ≠ 0 для любого элемента a ≠ 0 и любого целого числа n ≠ 0 и простое число p такое, что pa = 0 для любого элемента a в противном случае.

Пусть R — произвольное кольцо. Если существует такое целое положительное число n что для каждого элемента $r \in R$ выполняется равенство

$$n \cdot r = \underbrace{r + \cdots + r}_{n} = 0,$$

то наименьшее из таких чисел n называется *характеристикой* кольца R.

Т.к поле — это «хорошее» кольцо, то данное определение относится и к полям: существуют поля характеристики 0 и характеристики, отличной от нуля. Характеристики кольца целых чисел Z, поля рациональных чисел Q, поля веществ енных чисел R, поля комплексных чисел C равны нулю. Конечное поле, или поле Галуа, обозначается GF — поле, состоящее из конечного числа элементов; это число называется порядком поля. Конечным полем называется конечное множество, на котором определены произвольные операции, называемые сложением, умножением, вычитанием и делением, (кроме деления на 0).

Конечным полем GF называется конечное множество элементов, замкнутое по отношению к двум заданным в нем операциям комбинирования элементов. Под замкнутостью понимается тот факт, что результаты операций не выходят за пределы конечного множества введенных элементов. Для конечных полей выполняются следующие аксиомы.

1. GF.1. Из введенных операций над элементами поля одна называется сложением и обозначается как $a+b$, а другая - умножением и обозначается как ab.
2. GF.2. Для любого элемента a существует обратный элемент по сложению $(-a)$ и обратный элемент по умножению a^{-1} (если $a \neq 0$) такие, что $a+(-a)=0$ и $a \cdot a^{-1}=1$. Наличие обратных элементов позволяет наряду с операциями сложения и умножения выполнять также вычитание и деление: $a-b=a+(-b)$, $a/b = a \cdot b^{-1}$. Поэтому иногда просто говорят, что в поле определены все четыре арифметические операции (кроме деления на 0).
3. GF.3. Поле всегда содержит мультипликативную единицу 1 и аддитивную единицу 0, такие что $a+0=a$, и $a \cdot 1=a$ для любого элемента поля.
4. GF.4. Для введенных операций выполняются обычные правила ассоциативности $a+(b+c)=(a+b)+c$, $a(bc)=(ab)c$, коммутативности $a+b=b+a$, $ab=ba$ и дистрибутивности $a(b+c)=ab+ac$.
5. GF.5. Результатом сложения или умножения двух элементов поля является третий элемент из того же конечного множества.

Пример поле из двух элементов. Множество F2={0,1} из двух чисел «0» и «1», на котором операции сложения и умножения определены как сложение и умножение чисел с приведением результата по модулю 2. С обычной арифметикой 0+0=0, 0+1=1+0=1, 1+1=0, 0*0=0*1=1*0=0, 1*1=1. Эта логика лежит в основе двоичной системы компьютеров