ОГЛАВЛЕНИЕ

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

A, B, C, … - заглавные буквы латинского алфавита, обозначение множеств

a, b, c, … - строчные буквы латинского алфавита, обозначение элементов множеств (могут быть с индексами, обозначающими принадлежность перечисляемых элементов к множеству для удобства)

{} - множество перечисляют или задают обычно в фигурных скобках

a ∈ A — «элемент a принадлежит множеству A»;

a ∉ A — «элемент a не принадлежит множеству A»;

∀ — квантор произвольности, общности, обозначающий «любой», «какой бы не был», «для всех»;

∃ — квантор существования: ∃ y ∈ B — «существует (найдется) элемент y из множества B»;

∃ ! — квантор существования и единственности: ∃ !b ∈ C — «существует единственный элемент b из множества C»;

: — «такой, что; обладающий свойством»;

→ — символ следствия, означает «влечёт за собой»;

⇔ — квантор эквивалентности, равносильности — «тогда и только тогда»

↔ - сопоставление элементов множества

cap(A), **capA** - мощность множества A, количество элементов во множестве A.

A ⊆ B - множество A является подмножеством множества B. (A может быть равно B)

A⊂B - множество A является подмножеством множества B. (A не может быть равно B)

ГЛАВА 1. ДИСКРЕТНЫЕ СТРУКТУРЫ

В широком понимании дискретная математика есть дисциплина, рассматривающая совокупность конечных математических структур, задачи над ними, построение и реализацию алгоритмов над рассматриваемыми структурами. Таким образом она находит широкое применение в науке и технике, особенно в таких разделах информатики и вычислительной техники как: теория графов, теория автоматов, теория функциональных систем. Но так же наряду с данными широкими темами среди задач, решаемых дискретной математикой также существуют такие разделы как: теория кодирования, комбинаторика и целочисленное программирование. В процессе повествования настоящего пособия будет очень развёрнуто показано каким образом это соотносится с научным интересом теории групп и теории чисел.

Для понимания реализации различного рода математических структур необходимо базовое понимание множеств, их исчислимости и действий над ними.

1.1. Теория множеств

Множеством называется совокупность определённых вполне различаемых объектов, рассматриваемых как единое целое. Проще говоря, **множество** - перечисление конкретных объектов одного класса. Создатель теории множеств Георг Кантор давал следующее определение множества — «множество есть многое, мыслимое нами как целое».

Примерами множеств, не в отрыве от темы повествования, могут быть: наборы классов чисел (множества некоторых натуральных, целых, рациональных, комплексных чисел - всё это разные множества), наборы символов алфавита, наборы слов алфавита.

Множества могут быть заданы также различными способами:

1) Описательный (На основе закономерностей, логические описания элементов, принадлежащих определенным классам, в том случае если они подчиняются определённой логике или порядку следования)

Пример: A = {x | x N: $1 < x < 8$} - множество натуральных чисел на интервале от 1 до 8.

2) Перечислительный (на основе явного задания элементов класса)

Пример: B = {1, 3, 6, 10, 15, 21, 28, …} - множество треугольных чисел, C = {a, b, c, d, e, f, …, x, y, z} - множество символов латинского алфавита.

3) И т.д.

Классификация способов задания множеств носит больше условно-демонстрационный характер, и таких способов может быть больше чем приведено здесь.

Подмножеством называется такое множество элементов, которое содержит в себе только элементы из определённого множества. Подмножеством A множества B является множество A, элементы которого принадлежат также и множеству B: $A \subseteq B$.

Счётные и несчётные. Множества по свойству перечислимости их элементов делятся на счётные и несчётные. Элементы счётного множества можно последовательно пронумеровать в порядке их следования. В несчётных множествах между любыми двумя элементами множества располагается бесконечное количество элементов данного множества в порядке их следования, таким образом пронумеровать элементы не представляется возможным.

Даже некоторые бесконечные множества могут быть перечислимыми, например такие как: класс натуральных чисел **N**, класс целых чисел **Q**. Примером же несчётных множеств служит класс действительных чисел **R**.

Конечное и бесконечное. *Мощность множества* - количество элементов данного множества (cap). Про конечные и бесконечные множества говорят, что бесконечные множества имеют мощность равную бесконечности. Элементов таких множеств бесконечное количество. В это же время, установить мощность конечных множеств не составляет труда. Однако, перечислить элементы множеств, мощности равной бесконечности мы всё же можем благодаря сравнимости множеств, их поэлементного сопоставления.

В случае, когда нам известно понятие мощности множества, можно сказать, что счётные бесконечные множества, это множества *равномощные* множеству натуральных чисел.

Сравнение. В теории множеств с помощью сравнения множеств можно установить счётность множеств, и установить их мощность в случае конечности данного множества. Таким образом, сравнение это:

1) способ посчитать (только для фактических множеств);

2) способ установить однозначное взаимное соответствие (ещё и для ∞ множеств).

Примеры счётных множеств. Как уже было сказано ранее, с помощью класса натуральных чисел можно определить счётность множеств. Множество является счётным, если его элементы можно перечислить элементами из множества натуральных чисел, произведя поэлементное сопоставление между

двумя заданными множествами. Таким образом, можно привести некоторые примеры счётных множеств а именно:

1. Положительные чётные числа

$$n \leftrightarrow 2n$$

2. Подмножество всех целых чисел

$$Z : n \geq 0 \leftrightarrow N : 2n+1$$
$$Z : n < 0 \leftrightarrow N : 2|n|$$

3. Подмножество всех степеней числа 2

$$n \leftrightarrow 2^n$$

4. Подмножество рациональных чисел

Перед нами встаёт закономерный вопрос о том, как посчитать при помощи множества натуральных чисел элементы множества рациональных чисел, т.е. как посчитать элементы данного множества?

Введём понятие высоты подмножества рациональных чисел - h_Q, которое определяется как:

$$a = \frac{p}{q}, \qquad h_Q = |p| + q \tag{1.1}$$

где a - это элемент подмножества рациональных чисел, p - числитель, q - знаменатель элемента соответственно.

Сопоставим элементы данного подмножества с соответствующими высотами, тогда заметим, что число дробей высоты **n** конечно:

$$h_Q = 1 \Leftrightarrow \left\{\frac{0}{1}\right\}$$
$$h_Q = 2 \Leftrightarrow \left\{\frac{1}{1}, \frac{-1}{1}\right\}$$
$$h_Q = 3 \Leftrightarrow \left\{\frac{1}{2}, \frac{-1}{2}, \frac{2}{1}, \frac{-2}{1}\right\}$$
$$\dots$$

Будем считать N - это все числа по порядку возрастания высоты, тогда сперва выпишем 1, далее 2, и т.д. При этом будет представлено отображение: $n \to h_Q$.

Из этого будет следовать и перечислимость, т.е. установлена счётность подмножества рациональных чисел.

1.2. Счётные подмножества

В данном подразделе приведём некоторые теоремы, позволяющие раскрыть некоторые свойства счётных подмножеств.

Теорема. Любое под-подмножество счётного подмножества либо конечно, либо счётно.

Теорема. Сумма конечного или счётного чисел конечного или счётного подмножества есть опять конечное или счётное подмножество.

Теорема. Любое бесконечное подмножество M содержит счётное под-подмножество. Т.е. счётные подмножества – квант ∞ подмножества.

Теорема. Под-подмножества, лежащие на отрезке [0; 1] подмножества действительных чисел являются несчётными множествами.

Доказательство. Предположим что дан счётный перечень действительных чисел α_i на отрезке [0; 1] подмножества действительных чисел.

$$\begin{gathered}\alpha_1 = 0, a_{11}a_{12}a_{13}a_{14}\ldots a_{1n}\ldots \\ \alpha_2 = 0, a_{21}a_{22}a_{23}a_{24}\ldots a_{2n}\ldots \\ \ldots \\ \alpha_n = 0, a_{n1}a_{n2}a_{n3}a_{n4}\ldots a_{nn}\ldots\end{gathered} \qquad (1.2)$$

Построим дробь: $\beta = 0, b_1 b_2 b_3 b_4 \ldots b_n \ldots$. Если $a_{ii} = 1$, то примем $b_i > 2$, а если $a_{ii} \neq 1$, то $bi = 1$. По построению β не совпадает ни с одним из α_i . Действительно , β отличается от α_1 , по крайней мере первой цифрой; от α_2 - второй и так далее. Таким образом, никакой счётный перечень действительных чисел из отрезка [0; 1] не исчерпывает этого множества.

Приведём ещё некоторые примеры несчётных множеств:

1) $\forall[a;b] \in R \quad или \quad \forall(a;b) \in R$

2) все точки на прямой;

3) все прямые на плоскости;

4) все непрерывные функции от одного или нескольких аргументов.

1.2.1 Свойства счётных множеств

1. Объединение двух счётных множеств счётно.
2. Всякое подмножество счетного множества конечно или счетно.
3. Всякое бесконечное множество содержит счётное подмножество.
4. Множество рациональных чисел Q счетно.
5. Объединение конечного или счётного числа конечных или счётных множеств конечно или счётно
6. Декартово произведение двух счётных множеств $A \times B$ счётно.
7. Множество рациональных чисел счётно

1.2.2 Свойства несчётных множеств

По теореме Кантора $Card\ N < Card\ R$. Следствия:

1. $Q \neq R$ и существуют иррациональные числа

2. Существуют трансцендентные числа, поскольку множество всех алгебраических чисел счётно

1.2.3 Универсальное и пустое множества

Понятие универсального и пустого множества отводят нас к пониманию важности нуля и единицы в любой алгебре, которую необходимо построить. В основе любых бинарных преобразований лежат нейтральные элементы действия с которыми дают в качестве результата исходное множество. Таким образом для важнейших операций или действий над множествами необходимо определение таких множеств.

Множеством, которое содержит в себе всевозможные элементы заданного множества A, содержащиеся и не содержащиеся в данном множестве, составляют для данного множества универсальное множество I, Ω. Данное определение приводит нас к мысли о том, что для разных классов множеств, содержащих различные классы элементов такие универсальные множества являются разными и заранее определёнными. Относительно некоторых частных случаев определение универсальных множеств является даже очень простой задачей. Например,

1. Для множества X = {1, 3, 6, 10, 18} универсальным множеством будет являться множество всех натуральных или целых чисел в зависимости от определения класса X.

2. Для множества A = {а, г, е, ж, з, ы, я} универсальным множеством будет являться множество всех букв алфавита.

Как можно заметить, универсальное множество в реальных примерах может быть расширено для некоторых классов множеств, поэтому необходимо заранее определить класс элементов множеств исходной задачи.

Пустым множеством будем называть множество, не содержащее в себе каких-либо элементов. Обозначается как O, {}, $\varnothing$.

1.2.4 Действия над множествами

Для множеств определены некоторые действия над ними, такие операции могут быть как бинарными так и унарными.

1. **Объединение множеств** - бинарная операция над множествами, определяющая результирующее множество как совокупность элементов,

содержащихся или в первом или во втором множестве. Простыми словами, результатом операции является набор неповторяющихся элементов из двух данных множеств. Обозначается символом «$\cup$», операция записывается как:

$$A \cup B = C, \tag{1.3}$$

где A, B - множества, над которыми производится операция объединения, C - результирующее множество. Тогда по определению $A \subseteq C$ и $B \subseteq C$. Если $A \subseteq B$, тогда по определению подмножеств и объединения множеств: $A \cup B = B$.

2. **Пересечение множеств** - бинарная операция над множествами, определяющая результирующее множество как совокупность элементов, содержащихся как в первом так и во втором множестве. Таким образом, результат операции - множество состоящее из одинаковых элементов множеств A и B. Обозначается символом «$\cap$», операция записывается как:

$$A \cap B = C, \tag{1.4}$$

По определению подмножеств и пересечения множеств получаем, что $C \subseteq B$, $C \subseteq A$. Если $A \subseteq B$, тогда по определению: $A \cap B = A$.

Также важно понимать в связи данными ранее определениями универсальных и пустых множеств: если A не является подмножеством множества B и множество B также не является подмножеством множества A, то:

$$A \cap B = \{\}, \tag{1.5}$$

3. **Разность множеств** - бинарная операция над множествами, определяющая результирующее множество как совокупность элементов, содержащихся в первом множестве, но не содержащихся во втором. Обозначается « \ », операция записывается как:

$$A \setminus B = C, \tag{1.6}$$

По определению получаем, что если $A \subseteq B$, то $A \setminus B = \{\}$ или $\varnothing$ (пустое множество).

4. **Дополнение множества** - унарная операция над множеством, определяющая результирующее множество как последовательность элементов, не присутствующих в изначальном операнде, заданном на универсальном множестве I. Обозначается « $\neg$ », операция записывается как:

$$\neg A = C, \tag{1.7}$$

где C, результат операции - дополнение до универсального множества относительно исходного множества A.

По определению операции, можно также определить данную операцию как:

$$\neg A = I \setminus A, \qquad (1.8)$$

где I - универсальное множество, на котором определено множество A

В дальнейшем повествовании будет важным понимание данных операций над множествами.

1.3. Эквивалентность подмножеств

Обо всех явных числовых множествах можно сказать, что они являются подмножествами некоторых классов чисел, в таком случае в рамках подмножеств одного класса чисел можно установить соответствие в плане равенства их мощностей. Тогда получаем, что множество A эквивалентно множеству B, если можно поставить во взаимно однозначное соответствие элементы множеств A и B:

$$A \sim B, \ \textit{если} \ \exists B_i(A; B). \qquad (1.9)$$

Справедливо также, для конечных множеств:

capA = n (размерность множества A равняется n)

capB = m (размерность множества B равна m)

1. $A \sim B \Leftrightarrow n = m$
2. $A \sim C, \quad C \sim B \Rightarrow A \sim B$ – транзитивно
3. $A \sim |N|$ счётно (A есть счётное бесконечное множество и может быть посчитано элементами множества натуральных чисел ~ мощности счётного множества) и все счётные эквивалентны между собой.

Говорят, что *между множествами A и B установлено взаимно однозначное соответствие*, если каждому $a \in A$ сопоставлен единственный элемент $b \in B$, причём каждый элемент b оказывается сопоставленным только одному a. Соответствие между a и b: $a \leftrightarrow b$

Два *множества A и B называются эквивалентными или имеющими одинаковую мощность* $(A \sim B)$, если между множествами A и B может быть установлено взаимно однозначное соответствие.

Предлагается доказать самостоятельно:

1. доказать, что $IR > [a; b]$ эквивалентно $[c; d] < IR$
2. подмножество всех точек на C тождественно точке на сфере
3. подмножество всех точек на прямой тождественно точке $(a; в)$ $(0; 1)$

NB: Иногда ∞ подмножество оказывается эквивалентно своей переменной части.

Подмножества N (натуральных чисел), Z (целых чисел), Q (рациональных чисел) эквивалентны.

$$N \sim Z \sim Q \tag{1.10}$$

Под-подмножество чисел в промежутке между 0 и 1 подмножества вещественных чисел эквивалентно подмножеству вещественных чисел.

$$(0;1) \sim R$$

Теорема. Любое бесконечное множество эквивалентно некоторому своему истинному подмножеству.

Доказательство:

$$A = \{a_1, a_2, \ldots, a_n, \ldots\}, \quad M$$

Разобьём множество А на 2 подмножества $A_1 \quad и \quad A_2$:

$$A_1 = \{a_1, a_3, \ldots, a_{2n-1}, \ldots\}$$
$$A_2 = \{a_2, a_4, \ldots, a_{2n}, \ldots\}$$
$$A_1 A_2$$

это соответствие может быть затем продолжено до взаимно однозначного соответствия между

$$\begin{aligned} A \cup (M \setminus A) &= M \\ A_1 \cup (M \setminus A) &= M \setminus A_2 \end{aligned} \tag{1.11}$$

отнеся каждому элементу из $M \setminus A$ сам этот элемент.

Подмножество $M \setminus A_2$ является истинным подмножеством множества А.

1.3.1 Кардинальные числа

Для сравнения бесконечных множеств были введены так называемые кардинальные числа, показывающие счётность бесконечных множеств: $\aleph$ («Алеф») и $\aleph_0$ («Алеф ноль»)

1. $cap\ N = \aleph_0$
2. $cap\ R = cap[\ 0;1\ ] = \aleph - >$ мощность континуум

Итак, пусть существуют некоторые множества $A\ и\ B$ и соответствующие им мощности $|A|\ и\ |B|$.

Возможно:

1. $A \sim B => |A| = |B|$
2. $A \sim C < B$,*но* $A \neg \sim B => |A| < |B|$
3. В содержит часть $\sim A$
4. А содержит часть $\sim B$

1.3.2 Теорема Кантора-Бернштейна

Пусть множества A, B - $\forall$ произвольные, и $A_1 < A$, и $B_1 < B$, и $A_1 \sim B$, и $B_1 \sim A$, следовательно $A \sim B$ и $|A| = |B|$

Теорема. M – $\forall$, Z – подмножество всевозможных подмножеств M $|Z| > |M|$

1.4. Отношения на множествах

1.4.1 Декартово произведение множеств

В продолжение тем алгебры множеств, важных для введения в аппарат теории групп, необходимо упомянуть о декартовом произведении множеств.

Определение. Декартовым произведением множеств X, Y, заданных на некоторых классах элементах, называется множество, составленное по следующему правилу:

$$C = X \times Y = \{(x, y) \mid x \in X; y \in Y\} \qquad (1.12)$$

и для обобщения на n-мерные пространства множеств, далее введём декартово произведение n множеств $\{X_1, X_2, \ldots, X_n\}$:

$$C = X_1 \times X_2 \times \ldots \times X_n = \{(x_1, x_2, \ldots, x_n) \mid x_1 \in X_1, \ldots, x_n \in X_n\}, \qquad (1.13)$$

где (x_1, x_2, …, x_n) упорядоченные «n-ки». Далее $\forall\, i, j$ если X_i тождественно равно X_j следовательно $C = X^n$ - декартова степень подмножества X.

1.4.2 Бинарные отношения на множествах

Пусть R – бинарное отношение. Соответственно обозначается это как xRy, x, y – соответственно подмножества «x находится в отношении R к y».

Для бинарного отношения R:

1. Область определения R:

$$Dom(R) = \{x \mid \exists y, \textit{что } xRy\}, \qquad (1.14)$$

2. Область замены

$$Rang(R) = \{y \mid \exists x, \textit{что } xRy\}, \qquad (1.15)$$

3. Симметричные (обратные) отношения $R^{-1}R < X * Y$

$$R^{-1} = \{(y, x) \mid xRy\}, \qquad (1.16)$$

NB

4. Сечение бинарного отношения R по элементу a :

$$R = \{y \mid aRy\}$$
$$x = a$$

NB

5. Фактор–подмножества подмножества Y по отношению R – есть подмножество всех его сечений к точке.

$$Y / R = (R_{x=xi})$$
$$i = 1,2,\ldots$$

Пример: пусть даны некоторые множества X и Y, соответственное равные:

$$X = \{1, 2, 3\}$$
$$Y = \{1, 2, 3, 4\}'$$

тогда для данных множеств зададим некоторое утверждение, относительно которых представимо отношение R:

$$R: \quad "x \in X \text{ есть делитель } y \in Y".$$

Для множеств X и Y построим таблицу бинарного отношения R:

(x, y)	1	2	3
1	(1,1)	(2,1)	(3,1)
2	(1,2)	(2,2)	(3,2)
3	(1,3)	(2,3)	(3,3)
4	(1,4)	(2,4)	(3,4)

$$\Rightarrow \begin{cases} Dom(R) = \{1, 2, 3\} = X \\ Rang(R) = \{1, 2, 3, 4\} = Y \\ R^{-1} = \{(1,1); (2,1); (3,1); (4,1); (2,2); (4,2); (3,3)\} \end{cases}$$

На данном примере была продемонстрирована операция составления множества бинарного отношения *xRy*

Определение. Бинарное отношение R на множестве A называется рефлексивным на A, если: {x | ∀x ∈ A: xRx}. То есть существует отношение элемента относительно самого себя, в случае если данный элемент принадлежит заданному множеству.

Соответственно с данным определением задаётся понятие антирефлексивного отношения. Оно определяется в том случае, если не существует отношения элемента относительно самого себя, в случае если данный элемент также принадлежит исходному множеству.

1.5. Факторизация множеств

Важнейшим выводом темы бинарных отношений на множествах является существование фактор-множества. Определение фактор-множества дадим на

основе некоторых фактов также предшествующих данному понятию и необходимых для его понимания.

Для определения фактор-множества важно понимание отношения эквивалентности. Повторим его здесь:

Отношение эквивалентности - бинарное отношение на некотором множестве, удовлетворяющее условиям *рефлексивности*, *транзитивности* и *симметричности*. Отношение эквивалентности будем обозначать символом "~".

Также в связи с данным определением введём в рассмотрение понятий: *класс эквивалентности*, *полная система представителей класса эквивалентности*, *разбиение исходного множества.*

Класс эквивалентности - множество $\{x \in A \mid xRa\}$, где R - отношение эквивалентности, заданное на множестве A и $a \in A$. То есть класс эквивалентности, это множество всех x из A, что $\langle x, a \rangle \in R$.

Любой элемент, принадлежащий классу эквивалентности называется представителем этого класса. **Полная система представителей классов эквивалентности** - множество представителей всех классов, по одному из каждого класса.

Разбиение множества - семейство непустых подмножеств исходного множества, такое что каждый элемент исходного множества входит в точности в единственных из членов семейства.

Фактор-множеством множества A *по отношению эквивалентности* R называется множество A/R всех классов эквивалентности. Или, если R - отношение эквивалентности на непустом множестве A, то фактор-множество A/R является разбиением множества A. Тогда факторизацией исходного непустого множества A по отношению эквивалентности R будет являться нахождение разбиений множества, чтобы все разбиения составляли множество A/R всех классов эквивалентности.

1.6. Комбинаторика. Необходимый аппарат

1.6.1 Определение комбинаторики. Отображения. Числа Стирлинга

Комбинаторика - раздел математики, в котором изучаются подмножества, различные конфигурации и комбинации, составимые из элементов данного подмножества, предпочтительные тем или иным условиям.

Сочетание в комбинаторике - подсчёт числа элементов в конечном множестве.

Основные направления комбинаторики:

1. изучение известных конфигураций
2. исследование неизвестных конфигураций
3. подсчёт их числа
4. приблизительный подсчёт числа конфигураций
5. перечисление конфигураций

Принципы (аксиомы) комбинаторики.

1. **Правило суммы.** Если элемент a может быть выбран m способами, а элемент b другими K способами, то выбор одного из этих элементов a или b может быть сделан (m + k) способами.

2. **Правило произведения.** Если элемент a может быть выбран n способами, а затем элемент b выбирается m способами, то выбор пары элементов (a, b) в указанном порядке может быть произведён m*n способами.

3. **Правило включения-исключения.** Если M элементов обладают свойством S и k элементов обладают свойством P, то свойством S или P обладает (m + k - l) элементов, где l - количество элементов, которые имеют свойство S и свойство P.

Классическая задача комбинаторики - определить число способов размещения некоторых объектов в каком-либо объёме так, чтобы были выполнены заданные ограничения. Объемами в таком смысле являются мощности соответствующих множеств объектов:

$$|X| = n\ (capX = n)$$
$$|Y| = m\ (capY = m)$$

Отображение $f : X \to Y$, где X – объекты, Y – ящики. Каждое отображение f определяет размещение объектов по ящикам. То есть задаёт правила размещения по которому элементы одного множества возможно (или невозможно) соотнести с элементами другого множества, например

Пусть Y – подмножество цветов; f(X) – цвет объекта X. Таким образом, отображение f - *своего рода функция на множестве действительных чисел*.

В связи с этим можно задать типовую задачу для понимания отображений. «Сколькими способами можно покрасить объекты таким образом, чтобы были соблюдены некоторые ограничения».

В терминах алфавита можно перевести решение в данной задаче к теории множеств. Каждому отображению f сопоставимо слово

$$< f(x_1)\, f(x_2) \ldots f(x_n) > = < y_1; y_2; \ldots; y_n > \qquad (1.17)$$

в алфавите из m символов, то есть это эквивалентно подсчёту числа слов в алфавите, удовлетворяющем заданным ограничениям.

Теорема: для $f : X \to Y$, пусть:

$$|X| = n; \quad |Y| = m$$

Число $f = m^n$ - число слов длины n в алфавите из m символов

NB о свойствах отображений

Если *f - сюръективно*, т.е. для каждого ящик не пуст или все цвета использованы при раскраске или слова в заданном алфавите таковы, что в каждом слове используются все буквы алфавита.

Если *f - инъективно*, в каждом ящике меньше или ровно один объект; цвет всех объектов различен; слова в алфавите, все буквы которых различны.

$\forall x \in Z, [x]_n$: факториал от x «вниз» или нижняя n-я степень x.

$$[x]_n := x(x-1)(x-2)\ldots(x-n+1), \text{при } x \geq n$$
$$[x]_n := 0, \text{при } x < n \qquad (1.18)$$

NB

$$[x]_{n+1} := [x]_n * (x-n) \qquad (1.19)$$

Теорема. Пусть даны некоторые конечные множества X, Y, имеющие мощность n, m соответственно, причём n < m, тогда отображение f из X в Y есть инъективное отображение.

$$X, Y : capX = n, capY = m, n < m \Rightarrow f : X \to Y \Rightarrow f\ in(X; Y)$$
$$|f| = |m|_n \qquad (1.20)$$

NB

$$[m]_n = m(m-1)(m-2)\ldots(m-n+1) = \frac{m(m-1)(m-2)\ldots 1}{(m-n)(m-n-1)\ldots 1} = \frac{m!}{(m-n)!} \qquad (1.21)$$

Каждое взаимно однозначное отображение $f : X \to X$ по определению есть перестановка множества X.

⇒ число перестановок из n для n-элементного подмножества - n!

⇒ обратное вложение n!

Выражение $[x]_n$ является полиномом степени n от переменной X, следовательно может быть представлено как:

$$[x]_n = S(n;0) + S(n;1) * x + \ldots + S(n;n) * x^n, \qquad (1.22)$$

где S(n;k) - числа Стирлинга I-го рода.

Теорема. Числа Стирлинга I рода удовлетворяют следующему соотношению:

$$S(n+1;k) = S(n;k-1) - n * S(n;k), \qquad (1.23)$$

где, $S(n;0) = 0, S(n;n) = 1$. Данные числа как и перестановки можно найти рекурсивно.

1.6.2 Упорядоченные разложения

Пусть x - переменная или действительное число. Положим, по определению,

$$[x]^n = x(x+1)(x+2)\ldots(x+n-1). \qquad (1.24)$$

Обозначение $[x]^n$ читается как "n факториал от x вверх" или "верхняя n-ая степень x" .

$$[x]_n = x(x-1)(x-2)\ldots(x-n+1). \qquad (1.25)$$

Обозначение $[x]_n$ читается как "n факториал от x вниз".

Определение. Пусть X-множество из n объектов $1,2,\cdots,n$, которые должны быть помещены в m ящиков так, чтобы каждый ящик содержал последовательность, а не набор объектов, помещенных в него, как раньше. Два размещения являются одинаковыми (равными), если каждый почтовый ящик содержит одну и ту же последовательность объектов. Места размещения такого типа называются упорядоченных размещений N объектов по M ящикам.

Приведём пример всех возможных упорядоченных размещений двух объектов 1 и 2 в двух ящиках. Ящики будут представлены в виде последовательности вертикальных чёрточек , представляющих собой перегородки. 2 | 1 представляет собой размещение, в котором первый ящик содержит элемент 2, а второй ящик содержит элемент 1.

Таблица всевозможных размещений двух объектов в двух ящиках имеет следующий вид:

$$\varnothing|1\ \ 2\ \ ;\ 1|\ \ 2\ \ ;\ 1\ \ 2|\ \ \varnothing$$
$$\varnothing|2\ \ 1\ \ ;\ 2|\ \ 1\ \ ;\ 2\ \ 1|\ \ \varnothing$$

Утверждение 1.1. Число упорядоченных размещений n объектов по m ящикам равно:

$$[m]^n = m(m+1)\cdots(m+n-1),\ \textit{полагаем}\quad [m]^0 = 1. \tag{1.26}$$

Доказательство. Построим сначала таблицу T_{n-1} всех упорядоченных размещений объектов $1,2,...,n-1$ по m ящикам. Каждое размещение

$$i_1 i_2 \ldots | i_k i_{k+1} \ldots | \ldots | \ldots i_{n-1}. \tag{1.27}$$

можно представить как последовательность $(n-1)+(m-1)$ символов, являющихся либо буквой i_j, либо вертикальной чертой |. Чтобы получить последовательность из этой последовательности, представляющую собой упорядоченное размещение n объектов, достаточно добавить символ n всеми возможными способами. символ n можно добавлять к этой последовательности $(n-1)+(m-1)$ различными способами, помещая его перед самым первым символом, между любыми двумя символами и после последнего символа. Таким образом

$$|T_n| = (m+n-1)|T_{n-1}| = (m+n-1)(m+n-2)\ldots(m+1)|T_1| = [m]^n. \tag{1.28}$$

Очевидно, что $|T_1| = 1$. Отметим простые, часто используемые соотношения:

$$\begin{gathered}
[m]_n = (m-n+1)[m]_{n-1};\quad [m]^n = (m-n+1)[m]^{n-1};\\
[m]_n = m!/(m-n)! \quad ;\quad [m]^n = (m-n+1)!/(m-1)!;.\\
[m]^n = [m+n-1]_n \quad ;\quad [m]^n = [m]^{n-1}(m-n+1).
\end{gathered} \tag{1.29}$$

Определение. Пусть А-алфавит (т. е. конечный набор символов) с набором букв $a_1,\ldots,a_m$, упорядоченных так, что

$$a_1 < a_2 < \ldots < a_m.$$

Слово $x_1,\ldots,x_n$ длины n - монотонное, если слово состоит из расставленных по порядку элементов:

$$x_1 x_2 \ldots x_n.$$

Пример. Пусть $A = \{a,b,c,d\}, a < b < c < d$. Тогда монотонными будут, например, следующие слова:

$$aaa, aab, abc, aad, bcd, ddd.$$

(По несколько устаревшей терминологии, это комбинации с повторениями из m объектов, взятые по n штук).

Утверждение 1.2. Число монотонных слов длины n в алфавите из m букв равно $[m]^n / n!$.

Доказательство. Рассмотрим упорядоченное размещение n объектов $1,2,\ldots,n$ по m ящикам $a_1,\ldots,a_m$ и пусть ему соответствует монотонное слово следующим образом:

$$|\underbrace{3}_{a_1}|\underbrace{251}_{a_2}|\underbrace{87}_{a_3}|\ldots|\underbrace{64}_{a_n}| \quad \Rightarrow \quad a_1\, a_2\, a_2\, a_2\, a_3 \ldots a_n\, a_n\, a_n \ .$$

В соответствующем слове буква a_1 пишется столько раз, сколько есть объектов в ящике a_1, затем буква a_2 столько же раз, сколько есть объектов в ящике a_2 и так далее.

Каждое упорядоченное размещение n объектов соответствует одному монотонному слову. Таким образом можно получить все монотонные слова. Монотонному слову, с другой стороны, соответствует ровно n! различных упорядоченных размещений. Так что количество монотонных слов равно $[m]^n \ / \ n!$.

1.6.3 Задача Муавра

Найти количество способов представления положительного целого числа m в виде упорядоченной суммы n неотрицательных целых чисел

$$m = u_1 + \ldots + u_n . \tag{1.30}$$

Два таких представления

$$\begin{aligned} m &= u_1 + \ldots + u_n \\ m &= u_1^{'} + \ldots + u_n^{'} \end{aligned} \tag{1.31}$$

будем считать совпадающими тогда и только тогда, когда

$$u_1 = u_1^{'}, \ldots, u_n = u_n^{'}, \tag{1.32}$$

то есть когда совпадают слагаемые и порядок их следования.

Положим значение σ_k равным частичной сумме первых k членов последовательности $n_1,\ldots,n_k : s_k = n_1 + n_2 + \ldots + n_k$. Каждому представлению m в виде суммы n слагаемых взаимно однозначно соответствует слово

$$\sigma_1\sigma_2\ldots\sigma_{n-1}, \text{ где } 0\ \sigma_1\sigma_2\ldots\sigma_{n-1}\ m$$

Таким образом, количество представлений m в виде упорядоченной суммы неотрицательных целых слагаемых равно количеству монотонных слов $\sigma_1\sigma_2\ldots\sigma_{n-1}$ длины (n - 1) в алфавите из (m + 1) символа

$$(\sigma_i \in \{0,1,\ldots,m\}, \quad i = 1,\ldots,n-1)$$

Число представлений равно:

$$\frac{[m+1]^{n-1}}{(n-1)!} = \frac{(m+n-1)!}{m!\,(n-1)!} \tag{1.33}$$

1.6.4 Сочетания и биномиальные коэффициенты

Простейшими комбинаторными объектами являются сочетания и биномиальные коэффициенты.

Пусть конечное множество X содержит n различных элементов. Нас интересует количество различных подмножеств k-элементов, которые могут быть сформированы из элементов множества X. два подмножества считаются различными, если они отличаются хотя бы одним включенным в них элементом.

Такие подмножества называются сочетаниями из m элементов по k элементов и обозначаются $\binom{\mathrm{X}}{\mathrm{k}}$, а их количество $\left|\binom{\mathrm{X}}{\mathrm{k}}\right|$ обозначается C_m^k или $\binom{m}{k}$. Обозначение читается как “число сочетаний из m по k “ или просто “из m по k”.

Утверждение. Число различных подмножеств из k элементов множества A, $|A| = m$ есть

$$C_m^k = \binom{m}{k} = \frac{[m]_k}{k!} = \frac{m(m-1)\ldots(m-k+1)}{1*2*\ldots*k} = \frac{m!}{k!\,(m-k)!} \tag{1.34}$$

Первое доказательство. Построим табличку T из всех строго возрастающих (монотонных, без повторяющихся букв) слов длины k в алфавите A из m букв.

Пример. Пусть множество A состоит из пяти различных элементов:

$$A = \{a,b,c,d,e\}$$

Положим $k = 3$. Тогда таблица T всех строго возрастающих слов длины 3 в алфавите A имеет следующий вид:

$$\mathrm{T}: \begin{Bmatrix} abc & bcd & cde \\ abd & bce & \\ abe & bde & \\ acd & & \\ ace & & \\ ade & & \end{Bmatrix}$$

Переставим буквы в каждом слове всеми возможными способами и обозначим получившуюся таблицу как T' . T' - это набор слов без повторяющихся букв длины k в алфавите A. В таблице T' нет пропусков: каждое слово длины k появится в таблице T'. В таблице T' нет повторов: два слова из T' либо происходят от одного и того же слова T и тогда отличаются по порядку букв, либо от разных слов T и тогда отличаются по буквам.

По утверждению:

$$\left|T'\right| = [m]_k$$

поэтому:

$$\left|T\right| = \frac{[m]_k}{k!}$$

Таким образом, окончательно получаем

$$C_m^k = \binom{m}{k} = \begin{cases} \dfrac{[m]_k}{k!}, & k \neq 0, m \geq k \\ 1, & k = 0, m \geq k \\ 0, & m < k \end{cases} \qquad (1.35)$$

Второе доказательство. Определим множество $\binom{\mathrm{X}}{\mathrm{k}}$ (иногда обозначаемое иначе) как множество всех подмножеств k-элементов (или k-подмножеств) множества S и положим по определению $\binom{\mathrm{n}}{\mathrm{k}} = \left|\binom{\mathrm{S}}{\mathrm{k}}\right|$ (игнорируя прошлое использование символа $\binom{\mathrm{n}}{\mathrm{k}}$). Вычислим двумя способами число N(n, k) способов, с помощью которых мы можем выбрать k-подмножество T множеств, а затем упорядочить его элементы линейно. Множество T мы можем выбрать $\binom{\mathrm{n}}{\mathrm{k}}$ способами, а затем k способами выбрать первый элемент множества T, k-1 способом - второй элемент T и так далее.

Таким образом

$$N(n,k) = \binom{\mathrm{n}}{\mathrm{k}} k! \qquad (1.36)$$

С другой стороны, вы можете взять n способов любой элемент множества S в качестве первого, (n - 1) способ любой из оставшихся элементов в качестве

второго, и так далее, k-й элемент может быть выбран из оставшихся (n - k + 1) способом.

Следовательно,

$$N(n,k) = n(n-1)\ldots(n-k+1) \tag{1.37}$$

Итак, мы дали комбинаторное доказательство того, что

$$\binom{n}{k} k! = n(n-1)\ldots(n-k+1) \tag{1.38}$$

и, следовательно,

$$\binom{n}{k} = \frac{n(n-1)\ldots(n-k+1)}{k!} \tag{1.39}$$

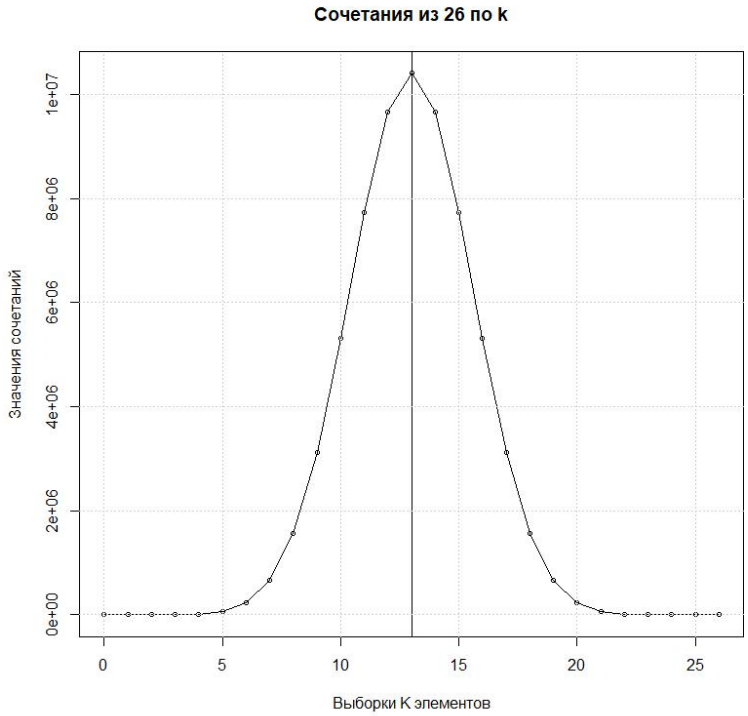


Рис. График значений числа сочетаний (ось ординат) для числа сочетаний из k элементов (по оси абсцисс) для n = 26.

Из представленного выше графика следует симметрия числа сочетаний относительно максимального (в случае чётного n) или максимальных (в случае нечётных n) значений числа сочетаний.

1.6.5 Производящие функции

Производящие функции неизменно и естественно появляются во всех разделах перечислительного комбинаторного анализа. Мы сосредоточимся на

наиболее органичном применении производящих функций для получения и проверки комбинационных тождеств, когда другие методы менее естественны или менее эффективны. Полученные функции часто используются в качестве альтернативы методу рекуррентных соотношений. в частности, они используются для получения взаимно обратных соотношений.

Путь задана последовательность $a_1, a_2, \ldots, a_n, \ldots$ (неважно, конечная или бесконечная). Производящей функцией последовательности $a_1, a_2, \ldots, a_n, \ldots$ называется функция

$$A(x) = \sum_{n=0} a_n \, X^n \tag{1.40}$$

В этом случае все рассматриваемые ряды считаются формально сходящимися в случае бесконечной последовательности (если эти ряды сходятся в некоторой области к функции *f(x)*), поскольку нас не интересует область совпадений корреляций. Например, из формулы

$$\frac{1}{1-x} = 1 + x + x^2 + \ldots + x^n + \ldots \tag{1.41}$$

вытекает, что функция $\frac{1}{1-x}$ является производящей функцией для последовательности чисел 1, 1, 1, ... , 1, ...

Возводя обе части последнего разложения в квадрат, получаем

$$\frac{1}{(1-x)^2} = 1 + 2x + 3x^2 + \ldots + (n+1)x^n + \ldots \tag{1.42}$$

откуда следует, что для последовательности 1, 2, 3, ... , n, ... производящей функцией является функция $\frac{1}{(1-x)^2}$

Нас будут интересовать производящие функции для последовательностей $a_1, a_2, \ldots, a_n, \ldots$, так или иначе связанные с комбинаторными задачами. С помощью производящих функций можно получить и исследовать различные свойства этих последовательностей.

Пусть $B(x) = \sum_{n=0} b_n \, X^n$ - производящая функция последовательности $b_1, b_2, \ldots, b_n, \ldots$ и $C(x) = \sum_{n=0} c_n \, X^n$ - производящая функция последовательности $c_1, c_2, \ldots, c_n, \ldots$. Тогда из равенства

$$c_0 + c_1 x + c_2 x^2 + \ldots + c_n x^n + \ldots =$$
$$= (a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n + \ldots) *$$
$$* (b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n + \ldots)$$

имеем

$$c_0 = a_0 b_0;$$
$$c_1 = a_1 b_0 + a_0 b_1;$$
$$c_2 = a_2 b_0 + a_1 b_1 + a_0 b_2;$$
$$\ldots$$

или в общем виде

$$c_n = a_n b_0 + a_{n-1} b_1 + a_{n-2} b_2 + \ldots + a_0 b_n = \sum_{k=0}^{n} a_{n-k} b_k \qquad (1.43)$$

В таком случае говорят, что последовательность коэффициентов c_n есть свёртка (произведение Коши) последовательностей a_n и b_n.

1.6.6 Биномиальные коэффициенты

Биномиальные коэффициенты получили своё имя от соответствующей производящей функции, которая является степенью бинома:

$$(1+x)^m = \sum_{k=0}^{m} \binom{m}{k} x^k \qquad (1.44)$$

Чтобы доказать справедливость написанного соотношения (1.44), достаточно отметить, что коэффициент при x^k равен числу способов, которыми из m сомножителей $(1+x)\ldots(1+x)$ можно выбрать k сомножителей.

Обратите внимание на некоторые наиболее важные соотношения для биномиальных коэффициентов (числа сочетаний).

1. $C_n^k = C_n^{n-k}$

Это важнейшее соотношение - прямое следствие того факта, что каждому k-элементному подмножеству $Y \subseteq X$ однозначно соответствует (n-k)-элементное подмножество $X \setminus Y$ множества X.

2. $C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$

Это так называемое рекуррентное соотношение, позволяющее однозначно определить значение n-го члена последовательности по его предыдущим состояниям. Важно заметить что такая постановка однозначно определяет

значение C_n^k и с помощью рекурсии такое значение можно найти за конечное число шагов, принимая во внимание, что $C_n^k = 0, k > n$ и $C_n^0 = 1$.

Зафиксируем некоторый элемент x из n-элементного множества X. Множество T всех k-элементных подмножеств множества X распадается на два непересекающихся класса:

$$T = T_1 \cup T_2; T_1 \cap T_2 = \{\}$$

класс T_1 подмножеств, которые не содержат элемент x, и класс T_2 подмножеств, которые его содержат. Мощность первого класса составляет C_{n-1}^k, а второго C_{n-1}^{k-1}, то есть столько, сколько имеется (k-1)-элементных подмножеств множества $X \setminus \{x\}$.

Продемонстрируем эффективность использования производящей функции биномиальных коэффициентов для получения комбинаторных соотношений, включающих число сочетаний.

3. Полагая в (1.44) $x = 1$ получим

$$\sum_{k=0}^{n} C_n^k = 2^n \tag{1.45}$$

Эта формула также вытекает из того факта, что сумма слева - это число всех подмножеств множества n-элементов.

4. Дифференцируя (1.44) и полагая x=1, получаем соотношение

$$\sum_{k=0}^{n} \hat{e}\, C_n^k \tag{1.46}$$

5.

$$\binom{m+n}{k} = \sum_{s=0}^{n} \binom{m}{s} \binom{n}{k-s} \tag{1.47}$$

Равенство легко следует из следующего равенства для производящих функций:

$$(1+x)^{m+n} = (1+x)^m (1+x)^n \tag{1.48}$$

Полагая в (1.47) $m = k = n$, получим

$$C_{2n}^n = \sum_{r=0}^{n} \binom{n}{r} \tag{1.49}$$

Заметим, что задача прямого доказательства последнего равенства без использования производящей функции достаточно сложна.

6. Полагая в (1.44) $x = -1$, получаем

$$\sum_{k=0}^{m}(-1)^k\binom{m}{k}=0 \tag{1.50}$$

отсюда следует, что:

$$\sum_{k=0}^{\left[\frac{m}{2}\right]}\binom{m}{k}=\sum_{k=0}^{\left[\frac{m}{2}\right]}\binom{m}{2k-1}=2^{m-1} \tag{1.51}$$

где через $\left[\frac{m}{2}\right]$ обозначена целая часть числа $m/2$.

ГЛАВА 2. ВВЕДЕНИЕ В АБСТРАКТНУЮ АЛГЕБРУ. НАЧАЛА АНАЛИЗА И ТЕОРИИ ВЕРОЯТНОСТЕЙ

2.1. Исчисление конечных разностей

Вот пример использования биномиальных коэффициентов в вычислительной математике.

Пусть дана функция φ , определённая на множестве действительных (возможно целых) чисел и принимающая действительные значения. Определим новую функцию $\Delta\varphi(x)$, называемую первой разностью φ, формулой:

$$\Delta\varphi(x) = \varphi(x+1) - \varphi(x) \tag{2.1}$$

Оператор Δ называется разностным оператором Первого порядка, и исчисление конечных разностей может быть определено кратко и очень просто как исследование оператора Δ.

Можно применить оператор Δk раз и получить k-ый разностный оператор:

$$\Delta^k\varphi(x) = \Delta(\Delta^{k-1}\varphi(x)) \tag{2.2}$$

Число $\Delta^k\varphi(x)$ называется k-ой разностью φ в точке x ($\Delta^k\varphi(0)$ называется k-ой разностью φ в 0). Определим другой оператор E, называемый оператором сдвига, формулой:

$$E\varphi(x) = \varphi(x+1) \tag{2.3}$$

Таким образом, $\Delta = E - I$, где I означает единичный оператор:

$$I\varphi(x) = \varphi(x) \tag{2.4}$$

Тогда первая разность функции может быть записана в виде:

$$\Delta\varphi(x) = \varphi(x+1) - \varphi(x) = E\varphi(x) - I\varphi(x) = (E-I)\varphi(x) \tag{2.5}$$

Разности более высоких порядков определяются рекуррентным соотношением:

$$\begin{aligned}\Delta^n\varphi(x) = (E-I)^n\varphi(x) = \Delta^{n-1}\varphi(x+1) - \Delta^{n-1}\varphi(x) = \\ = \left(E-I\right)\left((E-I)^{n-1}\varphi(x)\right)\end{aligned} \tag{2.6}$$

откуда получаем выражение для n -ой разности:

$$\begin{aligned}\Delta^n\varphi(x) = (E-I)^n\varphi(x) = \sum_{k=0}^{n}(-1)^{n-k}C_n^k E^k\varphi(x) = \\ = \sum_{k=0}^{n}(-1)^{n-k}C_n^k\varphi(x+k)\end{aligned} \tag{2.7}$$

в частности:

$$\Delta^k \varphi(0) = \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} \varphi(i) \qquad (2.8)$$

что дает явную формулу для k-ой разности в терминах значений $\varphi(0), \varphi(1), \ldots, \varphi(k)$. Нетрудно обратить формулу (2.8) и выразить $\varphi(n)$ через $\Delta^i \varphi(0)$. Именно,

$$\varphi(n) = E^n \varphi(0) = (\Delta - I)^n \varphi(0) = \sum_{k=0}^{n} \binom{n}{k} \Delta^k \varphi(0) \qquad (2.8)$$

Напишем теперь в строку значения:

$$\ldots \varphi(-2)\ \varphi(-1)\ \varphi(-0)\ \varphi(1)\ \varphi(2)\ \varphi(3) \ldots \qquad (2.9)$$

Если внизу написать между каждой парой последовательных членов $\varphi(i)$, $\varphi(i+1)$ их разность $\varphi(i+1) - \varphi(i) = \Delta\varphi(i)$, то получим последовательность:

$$\ldots \Delta\varphi(-2)\ \Delta\varphi(-1)\ \Delta\varphi(-0)\ \Delta\varphi(1)\ \Delta\varphi(2) \ldots \qquad (2.10)$$

Повторение этой процедуры приводит к таблице разностей функции φ, k-ая строка которой состоит из значений $\Delta^k \varphi(n)$. Диагональ, начинающаяся в $\varphi(0)$ и идущая направо вниз, состоит из разностей $\Delta^k \varphi(0)$ в 0. Например, пусть $\varphi(n) = n^4$. Таблица разностей (начинающаяся с $\varphi(0)$) выглядит так:

0		1		16		81		256		625	...
	1		15		65		175		369		
		14		50		110		194			
			36		60		84				
				24		24					
					0						

Из формулы (2.9) следует, что

$$n^4 = \binom{n}{1} + 14\binom{n}{2} + 36\binom{n}{3} + 24\binom{n}{4} + 0\binom{n}{5} + \ldots \qquad (2.11)$$

В этом случае, так как n^4 - многочлен четвёртой степени и $\binom{n}{k}$ при фиксированном k есть многочлен степени k, написанное выше разложение обрывается после члена $24\binom{n}{4}$, то есть $\Delta^k 0^4 = 0$, если $k > 4$ (или, более общим образом, $\Delta^k n^4 = 0$, если $k > 4$).

Предыдущее рассуждение, конечно, не относится лишь к функции n^4.

Подобные рассуждения приводят к следующим результатам.

1. Функция φ - полином степени, не превосходящей d, тогда и только тогда. когда $\Delta^{d+1}\varphi(n) = 0$ (или $\Delta^{d}\varphi(n)$ - постоянная).

2. Если многочлен φ(n) степени, не превосходящей d, разложен в ряд по базису $\binom{n}{k}$, $0 \prec k \prec d$, то коэффициенты разложения есть $\Delta^{k}\varphi(0)$, то есть

$$\varphi(n) = \sum_{k=0}^{n} \Delta^{k}\varphi(0)\binom{n}{k} \qquad (2.12)$$

2.2. Необходимые сведения из алгебры

2.2.1 Группа

Группа - G: <H; V> некоторое множество элементов H, с заданной на данном множестве групповой операцией V, удовлетворяющие следующим аксиомам:

1. Ассоциативность: $\forall\, a,b,c \in H:\ \ (a\ V\ b)V\ c = a\ V\ (b\ V\ c)$,

2. Существование нейтрального элемента: $\forall\, a \in H \quad \exists\, I \in H:\ \ a\ V\ I = I\ V\ a$,

3. Существование для каждого элемента группы обратного элемента относительно данной операции: $\forall\, a \in H \quad \exists\, a^{-1} \in H:\ \ a\ V\ a^{-1} = I$.

Примеры групп:

1. $< Z;\ + >$ целых
2. $< Q;\ + >$ рациональных
3. $< R;\ + >$ вещественных
4. $< C\ ;\ + >$ комплексных
5. $< Zn\ ;\ + >$ вычетов
6. $< F[x]\ ;\ + >$ многочлены над полем F
7. $< Mn[k]\ ;\ + >$ матрица над кольцом k

Среди этих групп также возможно что некоторые из них окажутся группами еще и относительно классического определения операции умножения из школьной математики. Такие группы называются **мультипликативными**. Группы же, где в качестве групповой операции на множестве определена операция сложения называются **аддитивными**. Мультипликативные группы не обязательно абелевы. **Абелевы группы** - группы, операция заданная на множестве которых удовлетворяет свойству коммутативности. В большинстве случаев, группы являются неабелевыми.

2.2.2 Подгруппа

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

Поскольку само множество является подмножеством самого себя, то любая группа является также примером подгруппы.

Важные определения подгрупп:

1. Исходная группа G, а так же её подгруппа, состоящая из нейтрального элемента составляет класс несобственных подгрупп, все остальные подгруппы, обратно, являются собственными.

2. Пересечение всех подгрупп, исходной группы G содержащих все члены некоторого непустого множества L, называется подгруппой, порождённой множеством L - $\langle L \rangle$.

3. Каждая подгруппа, отличная от всей группы, называется истинной подгруппой этой группы. Истинная подгруппа некоторой бесконечной группы может быть изоморфна самой группе.

2.2.3 Аддитивная абелева группа

Аддитивная абелева группа по определению это множество и определённый в нем бинарный оператор «+» со свойствами:

1. $a + в = в + a$ (коммутативности)
2. $(a + в) + c) = a + (в + c)$ (ассоциативности)
3. $\exists\ 0\ :\ a + 0 = a$ (существование нулевого элемента)
4. $\forall a$ ò$A\ \exists\ (-a)\ |\ (-a) + a = 0$ (∃ противоположного элемента)

Примеры:

1) Z; Q; R – подмножество аддитивных абелевых групп (∏аг) относительно обычного сложения.
2) множество $Z_0 = mod(N)$ – абелева группа, счётные операции модульного сложения
3) множество векторов (R2 или R3) - подгруппа абелевой группы относительно обычного сложения векторов
4) множество всех функций, определённых на заданном подмножестве R – подмножество подгруппа абелевой группы относительно обычного сложения функций

2.2.4 Мультипликативные подмножества абстрактных абелевых групп

По определению это множество множество/А с определённой в нём бинарной операцией умножения, удовлетворяющее аксиомам:

1. $ав = ва$
2. $(ав)c = a(вс)$
3. в $|A \exists e| ae = a \forall a$ ò$| A$, обозначает “1”
4. $\exists a$ 蝌$A \exists a^{-1} \quad |A| aa^{-1} = e$

Пример:

Пример мультипликативной аддитивной группы относительно обычного умножения

$$\mathbb{Q}^* = \mathbb{Q} \setminus \{o\}$$

$$\mathbb{R}^* = \mathbb{R} \setminus \{o\}$$

Пример:

Мультипликативные подмножества абелевых групп :

$$\begin{Bmatrix} + \\ - \end{Bmatrix} < Q^* < R^*$$

2.2.5 Порядок групп

Порядок групп - характеристика, определяемая мощностью подмножества А, на котором определена операция в случае конечной группы. Порядок группы – количество элементов в подмножестве на котором основана группа.

Подмножество В аддитивно подмножеству А определённого подгруппой, если:

1. В замкнуто относительно «+» $(\forall a, в$ 蝌$B ; a + в \quad B)$
2. из a 蝌$B \rightarrow (-a) \quad B : a + (-a) = 0$
3. 0 ò$B : 0 + a = a + 0 = a$

Пример:

Аддитивные абелевы группы: $Z < Q < R$. Подмножество τ мультипликативно подмножеству (∏аг) $/ A\ def$ подгруппе, если:

В замкнуто относительно Х (умножения)

1. $\forall a; в$ 蝌$B \rightarrow a \times в \quad B$
2. a 蝌$B \rightarrow a^{-1} \quad B$
3. e òB

2.2.6 Циклическая группа

Циклическая группа – порождение элемента a называется группа, все элементы которой являются произведением (для подгруппы аддитивной абелевой группы) или степенями для мультипликативной подгруппы.

Аддитивная циклическая группа - $< a > = \{k*a,\ k \in Z\}$

Мультипликативная циклическая группа - $< a > = \{a^k, k \in Z\}$

2.2.7 К-кольцо

К есть подгруппа абелевой группы относительно «+» (т.е. группа называется аддитивной группой кольца К):

1) $a(в + c) = ав + ac;\ (a + в)c = ac + вc;\ \forall a, в, c \in K$
2) (дистрибутивность относительно операции сложения элементов)
3) К – коммутативно, если $\forall a, в \in K: ав = ва$
4) К – ассоциативно, если $\forall a, в, c \in K: a(вc) = (ав)c$
5) 1 в $K \mid 1*a = a = a*1$

Пример:

1. Z, Q, R – коммутативные, ассоциативные кольца с 1 относительно обычных операций умножения * и сложения +.

2. $T = 2n,\ n \in Z,$ T - коммутативное, ассоциативное кольцо без «1».

3. Если к – ассоциативное кольцо с «1», абелева группа относительно +,* полугруппа – $(ав)c = a(вc)$ - Умножение 2-х сторонняя дистрибутивность

* $a(в + c) = (ав) + (ac)$
* $(в + c)a = (ва) + (ca)$

* кольцо т.е. $a*e = e*a = a$

* (!! некоммутативное умножение в общем случае)

Таким образом подмножество всех его обратимых (по умножению) элементов к* образует группу по умножению, называемую мультипликативной группой кольца к.

Если $K = F$ – поле, по F* - мультипликативная группа поля. Поле: это коммутативное кольцо с 1, плюс $\forall a \in F;\ a \neq 0\ \exists a^{-1} \in F: a * a^{-1} = e$

Исключив коммутативность умножения – получаем определение тела.

Характеристика поля ≡ кольцо :

$$\underbrace{1 + \ldots + 1}_{n} = n1 = 0$$

Если $\exists$ таких n, то характеристика ≡ 0.

Пример:

$Z^* = \{1;\ -1\}$ – мультипликативная группа кольца целых чисел.

2.2.8 Уравнение классов

Уравнение классов определено следующим соотношением:

$$|G| = |Z(G)| + \sum_i d_i \tag{2.13}$$

Σd_i – размер нетривиальных классов сопряжения

$Z(G)$ – центр группы. Множество элементов группы, которое коммутирует со всеми её элементами.

$$Z(G) = \{z \in G \mid \forall g \in G : zg = gz\} \tag{2.14}$$

* абелево (G) ≡ G
* неабелево – 0
* Гейзенберга

$$\begin{pmatrix} 1 & a & c \\ b & 1 & b \\ c & a & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ z & 0 & 1 \end{pmatrix}$$

Характеристика кольца К - называется целое неотрицательное число char(K) равное минимальному натуральному числу k, для которого при каждом a ϵ K соблюдается равенство:

$$\underbrace{a + a + \ldots + a}_{k} = 0 \tag{2.15}$$

$\kappa = 0$, если к ó конечно: ℵ

2.2.9 Поле

Полем называется коммутативное ассоциативное кольцо с «1», в котором $\forall a \neq 0$ элемент кольца обратим. Другими словами, ненулевые элементы поля образуют относительно умножения абелеву группу. Более подробное определение поля таково: полем называется множество F с двумя бинарными операциями (сложение и умножение), которые удовлетворяют следующим свойствам:

1. Относительно сложения F является абелевой группой.
2. Относительно умножения $F* = F \setminus \{0\}$ является абелевой группой. (Здесь 0 обозначает нулевой элемент относительно сложения.)

3. Аксиома дистрибутивности: $a(b + c) = ab + ac$.

Пример:

1. Q, R
2. Z не принадлежит полю, ибо в нем обратимый «1» и «-1».

2.3. Необходимый аппарат теории вероятностей

2.3.1 Основные определения теории вероятностей относительно теории множеств и алфавитного кодирования

Пусть мы имеем некоторые множества U, и множество двойных строк длины n — $\overline{B^n}$, тогда получаем:

U – конечно

B^n – подмножество двойных строк длины n.

Определение: распределение вероятности P(U) определено как отображение из U в B^1:

$$P : U \to B^1 \mid \sum_{x \in U} p(x) = 1 \tag{2.16}$$

Равномерное:

$$p(x) = \frac{1}{capU} \tag{2.17}$$

$$sign := \begin{cases} p(x_0) = 1, & x_0 \in U \\ p(x_0) = 0, & \forall x_0 \notin U \quad (x \neq x_0) \end{cases} \tag{2.18}$$

Исходя из данных введённых структур, определим распределение вероятностей над B^n – вектор:

$$(p(0, 0, \ldots, 0),\ p(0, 0, \ldots, 1), \ldots,\ p(1, 1, \ldots, 1)) \tag{2.19}$$

Для $\theta <= U$ событие в U:

$$P_r[\Theta] = \sum_{x \in \Theta} p(x) \tag{2.20}$$

Пример 1: $\tau \leq B^8$ подмножество x ò B^8 таких что 2 младших бита $=1$ $\left(lsb_2(x) = 11\right)$

$$P_r[\tau] = \frac{1}{4}$$

Пример 2: -“-“- старших

$$\Delta \leq B^8$$

$$\left(msb_2(x) = 11\right)$$

Теорема: Сложение вероятностей

$$P\left[A_1 \cup A_2\right] = P[A_1] + P[A_2]$$

$$P_2[\Delta] = \frac{1}{2}$$

для B^8:

$$P\left[\left(lsb_2(x) = 11\right) \cup \left(msb_2(x) = 11\right)\right] = \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

случайные величины – это

$$X : U \to V(B^n \to B^{\uparrow}) \tag{2.21}$$

Подмножество V заменит случайные величины

$$p[x = 0] = \frac{1}{2};\ p[x = 1] = \frac{1}{2}$$

Случайная переменная x порождает распределение над V:

$$P[x = v] := P\left[\ X^{-1}(v)\ \right]$$

Пусть U – конечно, к Правилу B^n чтобы показать равновероятный выбор r из U используют обозначение $r \overset{R}{\leftarrow} U$, т.е. $\forall a \in U : p\left[r = a\right] = 1/cap\ U$

NB

Формально $r(x) = x, \forall x \in U$

Пример:

Если r – равномерно распределено случайная величина из B^2 . Введем случайную переменную:

$$X = r_1 + r_2$$

$$P[X = 2] = \frac{1}{4}$$

2.3.2 Вероятностный алгоритм.

Введём алгоритм A - такой, который по входному значению m однозначно вычисляет выходное y:

$$y : y \leftarrow A(m) \tag{2.22}$$

Вероятностный A в отличии от детерминированного A :

$$r \overset{R}{\leftarrow} B^n \tag{2.23}$$

Содержащую случайную величину зависящую как от входного m, так и от r

$$r : y \leftarrow A(m, r) \tag{2.24}$$

т.е. $r \overset{R}{\leftarrow} A(m)$ – выходное значение является случайной величиной.

Алгоритм зашифровки открытого текста m на ключе k может быть представлено как вероятность алгоритм:

$$A(m,k) = E(h,m) = E_k(m) \tag{2.25}$$

шифротекст есть случайная величина

$$C \overset{R}{\leftarrow} A(m) \tag{2.26}$$

Определение: A и B – независимые события, если

$$P[A \cap B] = P[A] \cap P[B] \tag{2.27}$$

Случайные величины x,y независимы, если

$$\forall a,b \in V$$
$$P[(x=a) \cup (y=b)] = P[x=a] * P[y=b] \tag{2.28}$$

Пример: пусть

$V = B^2$ 00 R

$x = lsb(r)$ 01 r

$y = msb(r)$ 10

11

$=> P[(x=0)\ U\ (y=0)] = P[r=\infty] = 1/2 = P[x=0] \cdot P[y=0]$

Теорема. Пусть Y – сл. величина на B^n, X – независимая равномерно распределенная сл. величина на B^n. Следовательно : $Z = Y + X$ – равномерно распределенная случайная величина на B^n.

2.3.3 Парадокс дней рождения

$r_{1\ldots n} \in U$ – независимые в совокупности одинаково распределенные выличины, если

$$n = 1,2 \cdot \sqrt{|U|}$$

то

$$P[\exists\, i \neq j\ ;\ r_i = r_j] >= 1/2$$

Пример

$$U = B^{128}$$

После независимой выборки порядка 2^{64} случайных двоичных векторов из U почти наверно в выбор. подмножестве попадутся два одинаковые двоичные строчки.

ГЛАВА 3. ТЕОРИЯ ГРУПП И ТЕОРИЯ ЧИСЕЛ

3.1. Перестановки. Группы перестановок

3.1.1. Циклическая структура перестановки

Перестановки подмножеств и мульти-подмножеств являются самым богатым объектом перечислительной комбинаторики. Основной причиной этого является большое разнообразие способов представления перестановки комбинаторно.

Перестановку можно представлять как слово, и как функцию. В частности, функцию:

$$\pi : [n] \to [n], \tag{3.1}$$

где $\pi(i) = a_i, an$ - натуральное число, соответствует слову $a_1 a_2 \ldots . a_n$.

Если рассматривать перестановку π конечного подмножества S как :

$$\pi : S \to S, \tag{3.2}$$

то естественно для каждого x ϵ S рассмотреть последовательность :

$$x, \pi(x), \pi^2(x), \ldots \tag{3.3}$$

т.к. π – взаимно однозначное соответствие, а S – конечно, то в итоге последовательного применения операции к очередному получившемуся элементу перестановки - получим x.

Таким образом для некоторого единственного наименьшего $k >= 1$ имеем, что $\pi^k(x) = x$, а k элементов: x , $\pi(x)$, … , $\pi^{k-1}(x)$ все различны. Назовём последовательность $\pi(x)$, … , $\pi^{k-1}(x)$ циклом перестановки π длины k.

Циклы следующего вида:

$$\left(x, \pi(x), \ldots, \pi^{k-1}(x)\right) \tag{3.4}$$

и так же циклы:

$$\left(\pi^i(x), \pi^{i+1}(x), \ldots, \pi^{k-1}(x), x, \pi(x), \ldots, \pi^{k-1}(x)\right) \tag{3.5}$$

считаются эквивалентными.

Каждый элемент S встречается тогда в цикле " 1 " перестановки π, и мы можем рассматривать π как объединение непересекающихся циклов или, альтернативно, как произведение различных циклов $C_1, \ldots, C_n$.

Пример:

Перестановки $\pi : [\ 7\ ] \to [\ 7\ ]$

определены как:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 7 & 1 & 3 & 6 & 5 \end{pmatrix}$$
$$\pi(1)=4$$
$$\pi(2)=2$$
$$\pi(3)=7$$
$$\pi(4)=1 \qquad (3.6)$$
$$\pi(5)=3$$
$$\pi(6)=6$$
$$\pi(7)=5$$
$$\Rightarrow \pi = (1\ 4)\,(2)\,(3\ 7\ 5)\,(6)$$

Конечно, возможны различные обозначения такого представления перестановки подмножества π.

Пусть $C(n;k)$ – число таких перестановок подмножества из n элементов, которые имеют k циклов. Будем обозначать подмножество всех перестановок n-элементного подмножества символом G_n .

Теорема. Числа $C(n;k)$ удовлетворяют соотношению :

$$C(n,k)=(n-1)*C(n-1,k)+C(n-1,k-1), \qquad (3.7)$$

где $n,k \geq 1$, при этом: $C(n;k)=0 \, при \; n \leq 0; k \leq 0, но \; C(0;0)=1$.

Числа $C(n;k)$ можно получить из равенства:

$$C(n,k)=(-1)^{n-k} S(n,k), \qquad (3.8)$$

где $S(n;k)$ - числа Стирлинга I рода без знака.

Теорема. X - переменная, $n \geq 0$ фиксированное значение, тогда:

$$\sum_{k=0}^{n} C(n,k)*x^k = x(x+1)(x+2)\ldots(x+n-1), \qquad (3.9)$$

3.1.2. Последовательное выполнение перестановок

Отметим некоторые важнейшие свойства перестановок, вытекающие из основания комбинаторики

1) Один единственный элемент можно переставить одним единственным образом;
2) Два элемента, соответственно двумя способами, пример:

$$\begin{matrix} 1 & 2 \\ 2 & 1 \end{matrix} \qquad (3.10)$$

3) Три элемента можно переставить тремя способами: 1 , 2 , 3 – 3 элемента

$$\begin{matrix}1&2&3\\1&3&2\\2&1&3\\2&3&1\\3&1&2\\4&2&1\end{matrix} = \Sigma\ 6 \qquad (3.11)$$

4) Четыре различных элемента можно переставить 24 способами, что можно представить как перестановку по тройкам всех четырех из чисел: 1 , 2 , 3 , 4, на примере:

$$\begin{matrix}1&2&3&4&2&1&3&4&3&1&2&4&4&1&2&3\\&2&4&3&&1&4&3&&1&4&2&&1&3&2\\&3&2&4&&3&1&4&&2&1&4&&2&1&3\\&3&4&2&&3&4&1&&2&4&1&&2&3&1\\&4&2&3&&4&1&3&&4&2&1&&3&1&2\\&4&3&2&&4&3&1&&4&1&2&&3&2&1\end{matrix} = 24 \qquad (3.12)$$

или

$$(3.11)*4 = (3.11)*(3.10)*3 = 4*3*2*1 = 24$$

5) Тогда для пяти элементов соответственно получаем:

$$5*4*3*2*1 = 120 \qquad (3.13)$$

и так далее

6) Следовательно, перестановка множества из n элементов равна $n!$, ч.т.д

Выполнение перестановок за рамками комбинаторики:

Подстановка – совершает операцию определения и изменения порядка элементов в перестановке.

Пример:

Для произвольной перестановки, например: $\pi: 1\,4\,3\,2 \rightarrow 3\,1\,2\,4$, можно осуществить такую запись:

$$\begin{pmatrix}1&4&3&2\\3&1&2&4\end{pmatrix} \qquad (3.14)$$

Подстановки не зависят от порядка выписывания элемента и соответствующего ему элемента конечной перестановки.

Перестановка считается заданной, если:

1) известна вся совокупность элементов, над которыми осуществляется подстановка,
2) знаем алгоритм подстановки.

Две подстановки тождественны, если их область определения тождественна и каждый элемент принадлежит совместной области, отражается и переводится в один и тот же элемент.

NB

$$\begin{pmatrix}1&4&3&2\\3&1&2&4\end{pmatrix}\neq\begin{pmatrix}1&4&3&2&5\\3&1&2&4&5\end{pmatrix}$$

$$\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}=\ ?$$

NB

О перестановки может быть речь и для бесконечного ∞ множества

$$\begin{pmatrix}1&2&3&4&5&\dots\\3&4&5&6&7&\dots\end{pmatrix}$$

3.1.3. Разложение подстановок. Циклы, транспозиция

Введём в рассмотрение некоторые перестановки подмножества целых чисел: M = {0, 1, 2, 3, 4}:

$$\begin{pmatrix}0&1&2&3&4\\3&2&4&0&1\end{pmatrix}=P\quad\begin{pmatrix}0&1&2&3&4\\2&3&4&0&1\end{pmatrix}=Q \tag{3.15}$$

где P и Q - соответственно заданные перестановки подмножества M.

Удобно элементы Q расположить в порядке следования подстановок P, применим операцию композиции подстановок в заданном порядке :

$$PQ=\begin{pmatrix}0&1&2&3&4\\0&4&1&2&3\end{pmatrix} \tag{3.16}$$

интересным в данном случае будет проверка операции композиции элементов подстановок на обычные свойства умножения и также рассмотреть некоторые обычные случаи операции, тогда для композиции самих на себя получаем:

$$PP=\begin{pmatrix}0&1&2&3&4\\0&4&1&3&2\end{pmatrix}\quad QQ=\begin{pmatrix}0&1&2&3&4\\4&0&1&2&3\end{pmatrix} \tag{3.17}$$

Также произведём композицию элементов P и Q в обратном, от ранее заданного, порядке. Вопрос: «Будут ли выполняться свойства обычного умножения?», для этого вычислим QP:

$$QP=\begin{pmatrix}0&1&2&3&4\\4&0&1&3&2\end{pmatrix} \tag{3.18}$$

Вывод: каждое QP не тождественно PQ, но $PP = PP$.

Проверим для подстановок другое свойство умножения – ассоциативность.

$$a(bc) = (ab)c \tag{3.19}$$

области определения совпадают. Отметим существование перестановок вида:

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \tag{3.20}$$

$$Q = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \tag{3.21}$$

$$PQ = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \tag{3.22}$$

Это заданная на некотором подмножестве перестановка определяет тождественный, или «1» алгоритм, т.к. тождественный для тождественной перестановки алгоритм подстановки задан, т.е. «они ничего не делают в ответ области определения», тогда их можно считать независимыми от области определения.

Принято их обозначать всегда одной и той же буквой – I. Данный элемент играет роль единицы в умножении: $a * 1 = 1 * a = a$

$$P * I = I * P = P$$

т.е. для I умножение перестановок коммутативно.

Запись P из (3.20) в виде:

$$P = \begin{pmatrix} 4 & 3 & 1 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix} \tag{3.23}$$

без труда убедимся, что и

$$QP \equiv I \tag{3.24}$$

Принято считать, что если QP и $\mathrm{PQ} \equiv \mathrm{I}$, то Q называется *обратной перестановкой* к P.

Выясним, как происходит «поведение» перестановки в области определения. Рассмотрим обычную перестановку:

$$\tau \in S_4$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \tag{3.25}$$

Эта перестановка переводит единицу в четыре, четыре в один, два в три, а три в два. Если все перечисленные подстановки записаны в том порядке, в котором мы их сделали, то рассматриваемая перестановка примет вид:

$$\tau = \begin{pmatrix} 1 & 4 & 2 & 3 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

Нетрудно заметить, что перестановка была разложена на две части.

$$\tau = \left[\begin{pmatrix} 1 & 4 \\ 4 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} \right]$$

Это означает, что наша перестановка состоит из двух независимых частей, каждая из которых перемещает элементы, принадлежащие к своей собственной области определения (рис. 1).

Рис. 1 – Разложение перестановки $\tau \in S_4$.

Именно потому, что обе части перестановки τ независимы, не имеет значения, какую из перестановок

$$\begin{pmatrix} 1 & 4 \\ 4 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} \tag{3.26}$$

выполнить первой, а какую второй. Если перестановки (3.26) выполнять одну за другой, тогда такие действия можно рассматривать как умножение перестановок. Однако до сих пор мы говорили об умножении перестановок в тех случаях, когда области определения перестановок совпадали. Здесь области различны.

Нетрудно преодолеть возникшую проблему: предположим, что наши перестановки переводят каждый "недостающий" элемент в себя. Таким образом, перестановка τ допускает следующее разложение в произведение двух независимых перестановок:

$$\tau = \begin{pmatrix} 1 & 4 \\ 4 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix}.$$

Также нетрудно заметить, что в этой декомпозиции нижние строки совершенно не нужны. Действительно, верхние ряды состоят из тех же элементов, что и нижние, и каждый элемент под действием перестановки переходит к следующему. Это позволяет нам представить перестановку в виде

$$\tau = (1 \quad 4)\,(2 \quad 3). \tag{3.27}$$

Перестановки в правой части называются независимыми циклами, и представление перестановки (3.25) в виде (3.27) называется *разложением перестановки τ на произведение независимых циклов*.

Определение. Длина цикла называется количеством элементов, входящих в него (в этом случае циклы имеют длину, равную двум). Перестановка:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

допускает разложение только в один цикл

$$\sigma = (1\,2\,3\,4)$$

длиной 4.

Разложение перестановки τ в произведение независимых циклов эквивалентно разбиению множества X на непересекающиеся классы

$$X = \{1, 2, 3, 4\} = \{1, 4\} \cup \{2, 3\} = X_1 \cup X_2$$

где $X_1 = \{14\}, X_2 = \{23\}$

Хорошо известно, что разделение множеств на непересекающиеся классы эквивалентно введению некоторого отношения эквивалентности. Элементы, содержащиеся в одном из циклов, эквивалентны друг другу, а сами круги представляют свои собственные классы эквивалентности.

Если $\pi \in S_n$ некоторая перестановка, определённая на множестве $X = \{1,2,3,\ldots,n\}$, которую можно представить в виде произведения независимых циклов

$$\pi = \pi_1 \pi_2 \ldots \pi_n$$

то элементы множества X можно представить в виде объединения p попарно непересекающихся подмножеств

$$X = X_1 \cup X_2 \cup \ldots \cup X_k \cup \ldots \cup X_p$$

таких, что

$$\forall k, l \in Np = \{1, 2, \ldots, p\} : k \neq l \Rightarrow X_k \cap X_l = \{\}$$

Множества X_k называются π-орбитами. Название вполне обоснованно. Каждая точка $i \in X$ принадлежит в единственному классу эквивалентности, например X_k или X_k – орбите.

Если $i \in X_k$, то X_k состоит из образов точки i при действии степеней элемента

$$\pi : i, \pi(i), \pi^2(i), \ldots, \pi^{l_k - 1}(i)$$

где $l_k = |X_k|$ – длина k-го цикла орбиты X_k. Очевидно, что $l_k \leq q = |\langle \pi \rangle|$ и $\pi^{l_k}(i) = i$, причём l_k – наименьшее число, обладающее этим свойством.

Цикл π_k можно представить в виде:

$$\pi_k = \left(i, \pi(i), \pi^2(i), \ldots, \pi^{l_k-1}(i)\right) = \begin{pmatrix} 1 & \pi(i) & \ldots & \pi^{l_k-1}(i) \\ \pi(i) & \pi^2(i) & \ldots & \pi^{l_k}(i) \end{pmatrix}$$

Цикл πk оставляет на месте все точки из множества X / X_k, а для любой точки $i \in X_k$

$$\pi(i) = \pi_k(i) \tag{3.28}$$

Это свойство дает нам основание называть циклы $\pi_k, \pi_s, k \neq s$ независимыми или непересекающимися циклами.

Теорема. Каждую перестановку $\pi \in S_n : \pi \neq e$ можно представить в виде произведения p независимых циклов длины l_k k = 1, 2, …, p . Это разложение определено однозначно с точностью до порядка следования циклов.

$$\pi = \pi_1, \pi_2, \ldots, \pi_k, \ldots, \pi_p, \quad \text{где } l_k \geq 1, 1 \leq k \leq p \tag{3.29}$$

Замечание. Длина каждого k-го цикла – l_k, больше или равна двум. Если цикл $\pi_k = i$ имеет длину равную единице, то он действует как единичная перестановка и его в произведении (3.28) естественно опускать.

Например, перестановка:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix} \in S_8$$

может быть представлена в следующем виде:

$$\pi = (1 \quad 2 \quad 3 \quad 4 \quad 5)(6 \quad 7)(8) = (1 \quad 2 \quad 3 \quad 4 \quad 5)(6 \quad 7)$$

Запись π в виде произведения независимых циклов (3.28) позволяет быстро найти порядок перестановки

$$q = O(\pi)$$

Следствие 1. Порядок $q = O(\pi)$ перестановки $\pi \in S_n$ (порядок циклической подгруппы $|\langle \pi \rangle| = q$) равен наименьшему общему кратному (НОК) длин независимых циклов, входящих в разложение π.

$$q = HOK(l_1, l_2, \ldots, l_m) \tag{3.30}$$

Доказательство. Представим перестановку $\pi \in S_n$ в виде произведения независимых циклов:

$$\pi = \pi_1, \pi_2, \ldots, \pi_k, \ldots, \pi_m \tag{3.31}$$

тогда:

$$\pi^s = \pi_1^s, \pi_2^s, \ldots, \pi_k^s, \ldots, \pi_m^s; \quad s = 0, 1, 2, \ldots \tag{3.32}$$

Так как циклы $\pi_1, \pi_2, \ldots, \pi_m$ независимы (они действуют на различных множествах $X_1 X_2, \ldots, X_m$), и если q – порядок циклической подгруппы,

$$\left|\langle \pi \rangle\right| = q, \quad mo\ \pi^q = e \Leftrightarrow \pi_k^q = e, \tag{3.33}$$

где $k = 1, 2, 3, \ldots, m$.

Следовательно, q – общее кратное порядков циклов p_k, которые совпадают с их длинами l_k. Если q – наименьшее положительное число, для которого

$$\begin{gathered} \pi^q = e, \quad mo\ q = \left|\langle \pi \rangle\right| \\ q = HOK(l_1, l_2, \ldots, l_m). \end{gathered} \tag{3.34}$$

Замечание. Любые два целых числа m и n могут быть записаны как произведения одних и тех же простых чисел

$$p_1, p_2, \ldots, p_k.$$

Например:

$$n = \pm p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}, \quad m = \pm p_1^{\beta_1}, p_2^{\beta_2}, \ldots, p_k^{\beta_k} \tag{3.35}$$

Тогда:

$$HOK(n,m) = p_1^{\delta_1} p_2^{\delta_2} \ldots p_k^{\delta_k} \tag{3.36}$$

где:

$$\delta_i = \max(\alpha_i, \beta_i), i = 1, 2, \ldots, k. \tag{3.37}$$

Множество простых чисел

$$P = \{2, 3, 5, 7, 11, 13, \ldots\}.$$

Пример. Определить порядок перестановки $\pi \in S_{15}$ вида

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 3 & 4 & 2 & 1 & 7 & 8 & 6 & 5 & 11 & 12 & 13 & 15 & 10 & 9 & 14 \end{pmatrix}$$

Решение. Представим перестановку π в виде произведения независимых циклов, т.е.

$$p = (1 \quad 3 \quad 2 \quad 4)(5 \quad 7 \quad 6 \quad 8)(9 \quad 11 \quad 3 \quad 10 \quad 12 \quad 15 \quad 14) =$$

$$= p_1 * p_2 * p_3$$

Длины независимых циклов π_1, π_2, π_3 равны $l_1 = 4, l_2 = 4, l_3 = 7$.

$$HOK(4,4,7) = 4 * 7 = 28$$

Следовательно, порядок рассматриваемой перестановки π равен 28.

Определение. Цикл длиной два называется транспозицией. Любая транспозиция имеет вид $\pi_k = (i, j)$ и оставляет на местах все символы за исключением (i, j).

Теорема. Каждую перестановку $\pi \in S_n$ можно представить в виде произведения транспозиции.

Доказательство. Теорема будет доказана, если мы сможем представить в виде произведений транспозиций каждый из циклов π_k, входящих в разложения перестановки: $\pi = \pi_1, \pi_2, \ldots, \pi_k, \ldots, \pi_m$.

Рассмотрим произвольный цикл π_k, например $\pi_k = (12345)$ и разложим его в произведение транспозиций. Цикл $\pi_k = (12345)$ транспозиции:

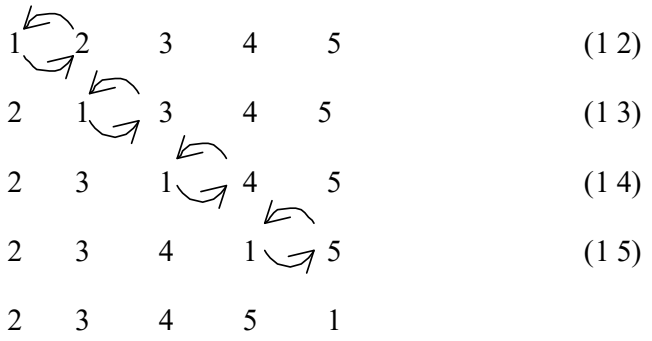


Рис 2. – Разложение цикла $\pi_k = (12345)$ в произведение транспозиций.

После того, как все операции были завершены, на месте каждого элемента цикла π_k оказался следующий за ним элемент, а первый элемент переместился на последнее место. Таким образом, цикл π_k был разложен в произведение транспозиций:

$$\pi_k = (1 \quad 2 \quad 3 \quad 4 \quad 5) = (1 \quad 5)(1 \quad 4)(1 \quad 3)(1 \quad 2)$$

Конечно, это разложение не единственно, например:

$$\pi_k = (1 \quad 2 \quad 3 \quad 4 \quad 5) = (2 \quad 3)(2 \quad 4)(2 \quad 5)(2 \quad 1)$$

Важно другое – и в первом и во втором его разложении имеется одинаковое количество транспозиций – четыре. Если $|\pi_k| = l_k$, то количество транспозиций будет $l_k - 1$. Раскладывая таким же образом каждый цикл $\pi_k, k = 1, 2, \ldots, m$ перестановки π в произведение транспозиции, мы получим разложение всей перестановки π в произведение транспозиций.

Замечание. *Число транспозиций в цикле* $(1\,2\,3\,4\,5)$ *может быть больше четырех*. Возьмем, например $(2\,3)$, произвольную транспозицию из разложения этого цикла. Тогда произведение $(2\,3)(2\,3)$ совпадает с идентичной перестановкой и цикл $(1\,2\,3\,4\,5)$ можно представить в виде

$$(1\quad 2\quad 3\quad 4\quad 5)=(1\quad 2)(1\quad 3)(1\quad 4)(1\quad 5),$$

либо

$$(1\quad 2\quad 3\quad 4\quad 5)=(1\quad 2)(1\quad 3)(1\quad 4)(1\quad 5)(2\quad 3)(2\quad 3),$$

либо

$$(1\quad 2\quad 3\quad 4\quad 5)=(2\quad 3)(2\quad 3)(1\quad 2)(1\quad 3)(1\quad 4)(1\quad 5)(2\quad 3)(2\quad 3)$$

Нетрудно заметить, что во всех случаях число транспозиций чётно и равно 4,6,8. Ясно, что метод, который "удлиняет" разложение, не изменяет чётности исходного разложения.

Теорема. Пусть π – перестановка из S_n, а

$$\pi = \pi_1, \pi_2, \ldots, \pi_k.$$

какое-либо разложение π в произведении транспозиций. Тогда число

$$\varepsilon_\pi = (-1)^k \tag{3.38}$$

называется *чётностью (сигнатурой или знаком) перестановки* π и полностью определяется π, т.е. не зависит от способа разложения перестановки π в произведение транспозиций. Кроме того, если $\pi, \sigma \in S_n$, то

$$\varepsilon_{\pi\sigma} = \varepsilon_\pi * \varepsilon_\sigma. \tag{3.39}$$

Данную теорему приводим без доказательства. Доказательство теоремы приведено в [1].

Определение. Перестановка $\pi \in S_n$ называется чётной, если $\varepsilon_\pi = 1$, и нечётной, если $\varepsilon_\pi = -1$.

Из определения чётности перестановки следует, что все транспозиции являются нечётными перестановками. Действительно, если π_k – транспозиция, то $l_k = 2$, тогда

$$\varepsilon_{\pi_k} = (-1)^1 = -1 \tag{3.40}$$

Следствие 1. Все четные перестановки степени n образуют подгруппу $A \subset S_n$ порядка $n!/2$ (она называется знакопеременной группой степени n).

Следствие 2. Пусть перестановка $\pi \in S_n$ разложена в произведение независимых циклов $\pi = \pi_1, \pi_2, \ldots, \pi_m$ длин $l_1, l_2, \ldots, l_k, \ldots, l_m$, где $|\pi_1| = l_1$, $|\pi_2| = l_2$, …, $|\pi_k| = l_k$, …, $|\pi_m| = l_m$ – длины независимых циклов. Тогда:

$$\varepsilon_\pi = (-1)^{\sum_{k=1}^{m}(l_k - 1)} \tag{3.41}$$

Доказательство. Действительно, по предыдущей теореме имеем

$$\varepsilon_\pi = \varepsilon_{\pi_1}, \varepsilon_{\pi_2}, \ldots, \varepsilon_{\pi_m} \tag{3.42}$$

Кроме того, $\varepsilon_{\pi_k} = (-1)^{l_k - 1}$ поскольку каждый π_k цикл записывается в виде произведения $l_k - 1$ транспозиций, то

$$\varepsilon_\pi = (-1)^{l_1 - 1}(-1)^{l_2 - 1}\ldots(-1)^{l_m - 1} = (-1)^{\sum_{k=1}^{m}(l_k - 1)} \tag{3.43}$$

3.2. Введение в теорию групп

3.2.1. Определение группы

Введём в рассмотрение подмножество N4. Мы рассмотрим операцию на подмножестве подстановок:

1. Ассоциативные: $\forall A, B, C: (AB)C = A(BC)$
2. Э единственный элемент подстановки, $I: \forall A : IA = AI = A$
3. Существует единственный обратный элемент такой, что $\forall A \; \exists A^{-1} : AA^{-1} = A^{-1}A = I$

> **NB**
> Не обязательно подстановка может быть другим подмножеством.

Принято говорить, что *выбранное подмножество с заданными на нём операциями образует группу*. Говоря об «умножении» подстановок говорят, что свойства «умножения» выбраны аналогичны свойствам умножения чисел. Обладает ли само умножение свойствами 1-3, это сильно зависит от природы множества, на котором определена данная операция.

Пример:

1. Множество целых чисел относительно операции умножения является группой: Z умножение (*) всегда Э. $(Z, \text{“*”})$

* Ассоциативность:

$$\forall a,b,c \in Z : (a*b)*c = a*(b*c) \tag{3.44}$$

* Существование единичного элемента

$$\left(\exists I \in Z : I \equiv 1\right) : \forall a \in Z : 1a = a1 = a \tag{3.45}$$

* Существование обратного элемента

$$a^{-1} ? : \exists x : 2x = 1 \in Z - \textit{неверно для } Z \tag{3.46}$$

* Поэтому G(Z, “*”) - *не является группой по определению*

Вообще, если $\{\exists e \mid \forall a : ea = a\}$, то это может быть единица: $e = 1$. Но если подмножество содержит 1 такую что $\forall a : 1a = a1x$ т.е. подмножество е должно быть таково: принадлежит ли «1» к подмножеству? *Исключение:* подмножество из 1 элемента «0».

2. Группа рациональных чисел Q по бинарной операции умножения: G(Q,“*”):

$$\{q_1, q_2\} \in Q$$

$$q_1 * q_2 = q_3 \in Q$$

* Ассоциативность

$$\forall a,b,c \in Q : (a*b)*c = a*(b*c)$$

* Существование единичного элемента множества

$$\left(\exists I \in Q : I \equiv 1\right) : \forall a \in Q : 1a = a1 = a$$

* Существование обратного элемента множества

$$q = \frac{m}{n} \Rightarrow \exists q^{-1} = \frac{n}{m} : \quad q * q^{-1} = \frac{m*n}{n*m} = 1$$

Всегда ли ∃? Нет, например если $q = 0$, поскольку $0*0 = 0$, но не 1.

Для группы рациональных чисел относительно операции умножения $(Q,*)$ аксиома 3. не выполнена. Следовательно, G(Q,*) - *не является группой*.

3. $(Q,*) = \{ Q \setminus \{0\}\}$ группа рациональных чисел относительно умножения исключая ноль. Исходя из рассмотрения, представленного выше, можно утверждать что данное множество с заданной на нём операцией *является группой по определению*. Так же данная группа является *мультипликативной абелевой группой*.

4. $(Q,**) = \{ Q \mid > 0 \} = Qt$ - группа рациональных чисел относительно возведения числа в степень, исключая отрицательные числа. Не является группой, по причине невыполнения аксиомы ассоциативности.

Пример:

$$\forall a,b,c \in Q : (a**b)**c = a**(b**c);$$
$$(2**2)**3 \neq 2**(2**3);$$
$$64 \neq 256$$

5. Группа, состоящая из множества T={-1, 1} и операции умножения: G(T,*):

$$1*1=1$$
$$1*(-1)=(-1)$$
$$(-1)*1=(-1)$$
$$(-1)*(-1)=1$$
$$(1)^{-1}=1$$
$$(-1)^{-1}=-1$$

= > T – *подмножество групп по операции умножения*, т.е. умножение не выводит за пределы T. Следовательно T является *мультипликативной абелевой группой*.

6. Группа рациональных чисел относительно операции умножения исключая положительные числа и ноль: $Q*** = \bar{Q} = \{ Q \mid \frac{m}{n} < 0 \}$

$$\left(-\frac{m}{n}\right)*\left(-\frac{m}{n}\right) > 0$$

Не является группой по операции умножения.

7. Группа из нуля по операции умножения: $\Phi = \{ 0 \}$

$0*0 = 0 - \neg$ за пределами Φ

$0(00) = (00)0 = 0$ – подмножество ассоциативно

Ф *является группой по умножению*. Интересно, а является ли подмножество Ф группой по операции сложения «+»?

1. подмножество ассоциативно
2. $e + a = a \Rightarrow e \equiv 0$, его надо проверять
3. $a^{-1} = ?\ a + b = 0 \Rightarrow b = -a$

Тогда G(Ф,*) - *мультипликативная абелева группа*, а G(Ф,+) - *аддитивная абелева группа*.

Пример:

1. Z – группа по операции сложения элементов (“+”), ибо:

$$\forall a,b \in Z : a + b = c \in Z$$
$$\exists 0 \in Z : \forall a \in Z \to a + 0 = 0 + a = a$$
$$\forall a \in Z \; \exists a^{-1} = -a \in Z$$

2. Q - группа по операции сложения элементов (“+”), ибо:

$$\forall a,b \in Q : a + b = c \in Q$$
$$\exists 0 \in Q : \forall a \in Q \to a + 0 = 0 + a = a$$
$$\forall a \in Q \; \exists a^{-1} = -a \in Q$$

3. $Q^* = \{Q \setminus \{0\}\}$ – нет свойства 2. Следовательно, группой не является.
4. Q^+ - тоже не является группой
5. $\Psi = Q^+ U \{0\}$
6. $\neg \exists a^{-1};\ q$ ðΨ
7. $T = \{1;\ -1\}$, $\neg$ *гр.* $-1+1=0,\ 0$ ¬ò T
8. «0» = τ – группа

3.2.2 Свойства элементов групп

Свойство 3.1. Для любого элемента а группы $a^{-1}a = e$, т. е. правый обратный к а элемент является также левым обратным.

Доказательство. Из второй и третьей аксиом группы следует, что

$$a^{-1} = a^{-1}e = a^{-1}(aa^{-1}) = (a^{-1}a)a^{-1} \tag{3.47}$$

В силу аксиом группы отсюда вытекают равенства

$$\begin{aligned} a^{-1}a = (a^{-1}a)e = (a^{-1}a)\left(a^{-1}\left(a^{-1}\right)^{-1}\right) = \\ = \left((a^{-1}a)a^{-1}\right)\left(a^{-1}\right)^{-1} = a^{-1}\left(a^{-1}\right)^{-1} = e \end{aligned} \tag{3.48}$$

Свойство 3.2. Для каждого элемента а группы элемента a^{-1} является единственным обратным элементом. Каждый элемент а группы имеет единственный правый и единственный левый обратный элемент, причем оба они совпадают с a^{-1}.

Свойство 3.3. Для любого элемента а группы $ea = a$, т. е. правая единица является также и левой единицей.

Доказательство. Из аксиом группы и свойства 3.1 следует, что

$$ea = (aa^{-1})a = a(a^{-1}a) = ae = a \tag{3.48}$$

т. е.

$$ea = ae = a \tag{3.49}$$

Свойство 3.4. Элемент e группы является единственным единичным элементом группы. Он же является единственным левым и единственным правым единичным элементом группы.

Свойство 3.5. Для любых элементов a, b группы каждое из уравнений $ax = b$ и $ya = b$ относительно переменных x и y имеет в группе единственное решение.

Доказательство. Элемент $a^{-1}b$ есть решение уравнения $ax = b$ так как $a(a^{-1}b) = (aa^{-1})b = eb = b$ С другой стороны, если c — произвольное решение уравнения $ax = b$, то $c = ec = \left(a^{-1}a\right)c = a^{-1}\left(ac\right) = a^{-1}b$. Следовательно, элемент $a^{-1}b$ является единственным решением первого уравнения. Аналогично доказывается, что элемент ba^{-1} является единственным решением второго уравнения.

Свойство 3.6 *(закон сокращения).* Для любых элементов a, b, c группы из $ac = bc$ следует $a = b$ и из $ca = cb$ следует $a = b$.

Доказательство. Если $ac = bc$, то a и b являются решениями уравнения $yc = bc$. По свойству 12.3 отсюда следует, что $a = b$. Аналогично доказывается, что из $ca = cb$ следует $a = b$.

Свойство 3.7. Для любых элементов a, b, c группы из $ab = a$ следует $b = e$ и из $ca = a$ следует $b = e$

Доказательство. Если $ab = a$, то $ab = ae$. По закону сокращения, из $ab = ae$ следует $b = e$. Аналогично, из $ca = a$ следует $ca = ea$ и c = e.

Свойство 3.8. В группе элемент a есть обратный к a^{-1}, т. е. $(a^{-1})^{-1} = a$.

Доказательство. По третьей аксиоме группы, $(a^{-1})(a^{-1})^{-1} = e$. По свойству 12.1, $a^{-1}a = e$. Таким образом, $a^{-1}(a^{-1})^{-1} = a^{-1}a$. По закону сокращения, отсюда следует равенство $(a^{-1})^{-1} = a$.

Свойство 3.9. Для любых элементов a, b группы из $ab = e$ следует, что $b = a^{-1}$ и $a = b^{-1}$. Это вытекает из определения обратного элемента и свойства 12.2.

3.2.2. Группы точек эллиптических кривых

Алгебраическая кривая порядка n определяющая подмножество точек афинной плоскости A^2 , для которой верно:

$$f(x, y) = 0. \tag{3.50}$$

где $f(x; y)$ – подмножество степени n с «к» из поля К.

Особые точки алгебраических кривых определяются точками: $(x_{0i}y_{0i})$, где $i = \overline{1,t}$, в каждой из которых:

$$\left.\frac{df(x,y)}{dx}\right|_{(x_{oi},y_{oi})}=0$$
$$\left.\frac{df(x,y)}{dy}\right|_{(x_{oi},y_{oi})}=0 \qquad (3.51)$$

Двойные точки алгебраических кривых определяются особыми точками, в которых не все части $f(x;y) \equiv 0$.

Требование для двойных точек алгебраических кривых определяется существованием особых точек, где $\left.\begin{matrix}\frac{d^j f}{dx^j}\\ \frac{d^j f}{dy^j}\end{matrix}\right|_{j=\overline{1,2}} \equiv 0$, но не все $\frac{d^3 f}{dx^3}$ и $\frac{d^3 f}{dy^3} = 0$

Родом алгебраической кривой P называют главную характеристику алгебраической кривой $f(x;y) = 0$ порядка n, вычисляемую как:

$$p=\frac{1}{2}(n-1)(n-2)-r, \quad где\ r: число \qquad (3.52)$$

Касп или **точка возврата** - это особая точка, в которой криволинейная линия разделяется на две (или более) ветви, имеющие в этой точке один и тот же направляющий вектор. То есть ветви в данной точке имеют общую касательную, и движение из них от этой точки изначально происходит в одном направлении.

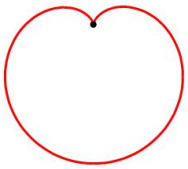


Рис. Касп, точка возврата

3.2.3. Эллиптические кривые и групповой закон на эллиптических кривых

Пусть K – поле; $char(K)$; эллиптических кривых над K (обозначим её E) есть кривая I рода в проективном пространстве P2 с подмножеством точек (x, y, z) ò K, которое удовлетворяет обобщённому условию Вейерштрасса.

$$E: Y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_5z^3, \qquad (3.53)$$

где $a_1 \ldots a_5 \in \bar{K}$, $\bar{K}$ – фиксированное алгебраическое замыкание K.

Пусть $char\, K > 3$ и уравнение записано аффинными координатами вместе с некоторой специальной точкой «O», которая определяется как «точка в ∞».

Тогда подмножество кривых есть подмножество значений $(x; y)$ элементов поля К, удовлетворяющих условию:

$$E : y^2 = x^3 + ax + b \tag{3.54}$$

Известно, что к эллиптической кривой применим групповой закон, определяющий аддитивное, подмножество абелевой группы. Необратимый элемент группы («0») – в данном случае есть точка в ∞, $0 = (\infty : \infty)$. Групповая операция – есть сумма 2-х точек: $P_1 = (x_1; y_1)$ $P_2 = (x_2; y_2)$, приводящая к получению результирующей точки: $P_3 = (x_3; y_3)$

Снижение осуществляется следующим образом:

Пусть λ определяется на основании выражений:

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & x_2 \neq x_1 \\ \dfrac{3x_1^2 + a}{2y_1}, & x_2 = x_1 \end{cases} \tag{3.55}$$

Тогда

$$\begin{aligned} x_3 &= \lambda - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{aligned} \tag{3.56}$$

Если точка P суммируется n раз, то такая сумма обозначается как:

$$p + p + \ldots + p = n * p \tag{3.57}$$

NB

Криптографическое значение этой записи состоит в том, что она определяет группу, в которой сравнительно легко вычислить $p = nQ$, однако это вычислительно трудно для понимания.

Групповой закон на эллиптических кривых

Мы можем определить группу для эллиптических кривых. А именно:

1. элементы группы являются точками эллиптической кривой;
2. единичный элемент — это бесконечно удалённая точка 0;
3. обратная величина точки P — это точка, симметричная относительно оси x;
4. сложение задаётся следующим правилом: сумма трёх ненулевых точек P, Q и R, лежащих на одной прямой, будет равна $P + Q + R = 0$.

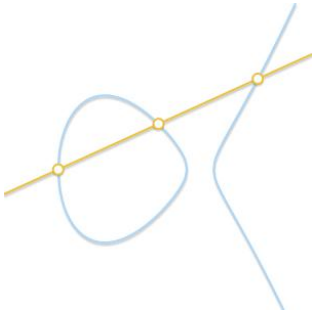


Рис. Сумма трех точек на одной прямой равна 0

Стоит отметить, что в последнем правиле нам нужны только три точки На одной прямой, и порядок расположения этих трех точек не важен. Это означает, что если три точки P, Q и R лежат на одной прямой, то $P + (Q + R) = Q + (P + R) = R + (P + Q) = \cdots = 0$. Таким образом, мы интуитивно доказали, что наш оператор + обладает свойствами ассоциативности и коммутативности: мы находимся в Абелевой группе

3.3. Введение в теорию чисел

3.3.1 Решение рекуррентных соотношений

Рекуррентное соотношение, в общем смысле, это некое равенство, связывающее некоторые функции в дискретные моменты отсчёта n. Во многих частных случаях такие соотношения представляются в виде разложения n-го члена последовательности исходной функции в виде композиции данной функции в какие-либо из предыдущих моментов времени, при этом задаётся начальное состояние данной функции в момент времени n = 0, 1, …

Задача решения рекуррентных соотношений заключается в представлении данного n-го состояния функции через переменную отсчета n и её состоянием в начальный момент времени n = 0, 1, …

В таком случае можно уверенно говорить о представимости любого члена искомого ряда через начальное состояние. Таким образом, мы получаем решение в виде связи состояния функции в n момент времени и в начальный момент времени.

Было предположено, что производящая функция $F_n(x)$ для $\left\{\binom{n}{k}\right\}_{k=0}^{n}$ имеет вид: $(1+x)^n$. Существует регулярный приём решения рекуррентных соотношений.) от обратного :

(*) Начальный момент - $\begin{bmatrix} n \\ 0 \end{bmatrix} = 1$

(*) Данное состояние величины в виде композиции предыдущих отсчётов дискретного состояния $\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k \end{bmatrix} + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}; k \geq 1$

(*) X на X^k и $\sum c$

Следовательно:

$$\begin{bmatrix} n \\ 0 \end{bmatrix} + \sum_{k \geq 1} \begin{bmatrix} n \\ k \end{bmatrix} x^k = 1 + \sum_{k \geq 1} \begin{bmatrix} n-1 \\ k \end{bmatrix} x^k + \sum_{k \geq 1} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} x^k$$

т.е.

$$F_n(x) = F_{n-1}(x) + xF_{n-1}(x)$$

$$F_n(x) = (1+x) + F_{n-1}(x)$$

$$\Rightarrow F_n(x) = (1+x)^n, (\textit{ибо } F_1(x) = 1+x)$$

Опишем теперь одно из важных применений рекуррентных функций – решение рекуррентных соотношений.

Есть: $\{q_n\}_{n \geq 0}$ - последовательность удовлетворяющих рекуррентных соотношений. Необходимо получить выражение для q_n, зависящее от n и шага (производящей функции).

1. Записать рекуррентное уравнение , выражающее q_n через другие элементы последовательности добавить к нему, если надо, уравнение для начального значения n.
2. Умножить обе части полученного уравнения на соответствующие Z^n и просуммировать по всем n. Снова получим: $\sum_{n \geq 0} q_n z^n$ - равна произведению функций $G(z)$. Правую часть следует преобразовать так, чтобы она превратилась в выражение, включающее $G(z)$
3. Решить полученные уравнения, получив для $G(z)$ выражение в замкнутом виде.
4. Разложить $G(z)$ в степенной ряд, получить «к» при «z», это и будет искомое для q_n.

3.3.2 Числа Каталана

Определение чисел Каталана:

$$C_n = \frac{1}{n+1} \begin{bmatrix} 2n \\ n \end{bmatrix} \tag{3.58}$$

разных по формулировке задач, сводящихся к всего 2-у нас – остальные в $(n+1)$.

Пример. $x_0, x_1, \ldots, x_n$ – переменные. Надо вычислить их произведение при помощи n умножений. Сколько существует способов расставить скобки в произведении чтобы порядок умножения был полностью определён?

$n = x_0 * (x_1 * x_2)$ способа 2

$n = (x_0 * x_1) * x_2$

$n = 35$ способа 3

т.е.

$$\left.\begin{array}{l} C_1 = 1 \\ C_0 = 0 \end{array}\right\} \text{ положим}$$

тогда:

$C_2 = 2$

$C_3 = 5$

$n \geq 2$ – одна операция вне скобок – последнее (о)

Если эта операция располагается между x_k и x_{k+1}, то можно $C_к$ способами расставить скобки в произведении : $x_0 \circ \ldots \circ x_k$ и C_{n-k-1} способами в произведении : $x_{k+1} \circ \ldots \circ x_n$

$$\Rightarrow C_n = C_0 C_{n-1} + C_1 C_{n-2} + \ldots + C_{n-1} C_0 \quad \text{если } n > 0$$

т.е.

$C_0 = 1$

$C_n = \sum C_k C_{n-k-1}$

Умножим каждый $!C_n^k$ на соответствующую степень z^n и просуммируем:

$$C(z) = \sum_n C_n Z^n = \sum_n \sum_k C_k C_{n-k-1} Z^n + 1 =$$

$$= \sum_k C_k Z^k \sum_n C_{n-k-1} Z^{n-k} + 1 = C(z) * z * C(z) + 1$$

отсюда следует

$$C(z) = \frac{1 \pm \sqrt{1-4z}}{2z} = \oplus, \textit{ следовательно } C(0) = \infty$$

Что противоречит действительности для $C(z) : C(0) = C_0 = 1$

$$C(z) = \frac{1 - \sqrt{1-4z}}{2z}$$

(Это согласуется и с $C(0) = C_0 = 1$). Остаётся вычислить «к» при Z^n в разложении $C(z)$.

По биномиальный:

$$\sqrt{1-4z} = \sum_{k\geq 0}\begin{bmatrix}2\\k\end{bmatrix}(-4z)^k = 1 + \sum_{k\geq 0}\frac{1}{2k}\binom{-\frac{1}{2}}{k-1}(-4z)^k$$

Ранее была определена производящая функция:

$$(1+z)^r = \sum_k \binom{r}{k} z^k \leftarrow \textit{для } r \in Z^+$$

Если r –∀ò IR:

$$F(z) = \frac{F(0)}{0!}z^0 + \frac{F'(0)}{1!}z^1 + \frac{F''(0)}{2!}z^2 + \ldots = \sum_{k\geq 0}\frac{F^k(0)}{k!}z^k$$

По Теореме Тейлора:

$$F^n(z) = [r]_k (1+z)^{r-k}$$

т.к.

$$\binom{r}{k} = (-1)^k \binom{k-2-1}{k}$$

формула верхнего обращения

$$\rightarrow \binom{-\frac{1}{2}}{n} = \left(-\frac{1}{4}\right)^n \binom{2n}{n}; n \in Z$$

Подстановки

$$\frac{1-\sqrt{1-4z}}{2z} = \sum_{k\geq 1}\frac{1}{k}\begin{bmatrix}-\frac{1}{2}\\k-1\end{bmatrix}(-4z)^{k-1} = \sum_{n\geq 0}\begin{bmatrix}-\frac{1}{2}\\0\end{bmatrix}\frac{(-4z)^n}{n+1} = \tag{3.59}$$

$$= \sum_{n\geq 0}\begin{bmatrix}2n\\n\end{bmatrix}\frac{z^n}{n+1} = \sum_{n\geq 0} C_n * z^n$$

$C_n =$ *числу Каталана* $\frac{1}{n+1}\binom{2n}{n}$

3.3.3 Пример на числа Каталана

Сколько последовательностей $< a_1; a_2; \ldots; a_{2n} >$, состоящих из n чисел $+1$ и n чисел -1, обладает свойством :

$$a_1 + a_2 + \ldots + a_n = 0$$

а все их частичные суммы:

$$a_1;\ a_1 + a_2;\ a_1 + a_2 + a_3; \ldots; \sum_{k=1}^{n} a_k$$

неотрицательны? (В точности C_n вариантов существует B_i между n-теми способами расстановки скобок).

3.3.4 История теории чисел

Теорема Ферма 1601-1665: письмо Декарта. Пометка (не располагает удовл. док.) в простых числах

$$2^{2n}+1$$

$n >= 5$ – Эйлер – составим

Теорема «Великая, Большая, Последняя»

$$\{x,y,z\} \neq 0 \in Z \mid x^n + y^n = z^n \quad для\ n > 2$$

доказано $n < 100000$ 10^{100000}

$$n = 2$$
$$\exists:\ 3,\ 4,\ 5 \quad n = 4$$

Теор Ферма – единственное док-во, доказанное до нас.

Арифметика Диофанта поля

«поля слишком малы, чтобы его уместить»

1980 г. – Диксон ≈ 300 работ $n > 4$ – нет элементарных

1908 Вальфскель 100 000 RDM - Геттингемское мат-общество

Теория алгебраических чисел

Теория $\frac{Ферматист}{Грюнерт}$

$$\{x,y,z\} \in Z \mid x^n + y^n = z^n$$

Существует если $\exists \rightarrow x > n,\ y > n,\ z > n$

Д : д

Пусть $z = x + a$; $a >= 1$ $\Rightarrow$

$$X^n + Y^n = X^n + nX^{n-1}a + \ldots + nXa^{n-1} + a^n$$
$$\Rightarrow Y^n > nX^{n-1}a > nX^{n-1}$$

Аналогично:

$$X^n > nY^{n-1} \Rightarrow \left(Y^n\right)^n > n^n X^{n(n-1)} > n^n n^{n-1}\left(Y^{n-1}\right)^{n-1}$$

т.е. $Y^{2n-1} > n^{2n-1}$, $Y > n$

по симметрии $X > n \Rightarrow X > n$

Что и требовалось доказать.

Элементарно нет для $n=3$ Эйлер числа вида

$a+b\sqrt{-3}$

(a,b) ò Z

Перенос некат утв. по Z. Простейшие формы делимости.

ГАУСС $n=5$ док-во

Дирихле, Лежандр 1828, Племель 1912 $n=7$

1833 ЛАМЕ, ЛЕБЕГ попытка $n>=3$

$$a_0+a_n\zeta+\ldots+a_n\zeta^{n-2} \qquad a:\in \mathbf{Z}(x)$$

$$\zeta=\sqrt[n]{1}=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$$

ЛИУВИЛЛЬ

¬ единственное разложение в П простых (неразложимых) чисел

КУММЕР

развитие идеи

высшие законы взаимодействия

добавил к (+) еще числа спец. вида.

Доказать

В области чисел

$a+b\sqrt{-5},$

a,bòZ

число 21

2-я способами разлагается в П простые множители

3.3.5 Теория чисел подмножеств (Ферма-теория)

Итак, возвращаясь, мы рассмотрели подмножество b теорему «Антиферма» (Грюперт):

$$\begin{array}{c|c} \exists\, 0\neq\{x^n,y^n,z^n\}\in Z & x^n+y^n=z^n\Rightarrow x>n \\ \in N & y>n,\ z>n \end{array} \qquad (3.60)$$

1768 г. Эйлер – оказались необходимыми соображения, использующие числа вида:

$$H=a+b\sqrt{-3},\ \{a,b\}\in Z \qquad (3.61)$$

Чуждые Ферма методы, их использовать он не мог заведомо.

Эйлер подгадал неверие подмножеств (в том числе использовал факты делимости Z для чисел вида (3.61). Арифметику чисел H – привел Гаусс. Для $n=5$ - Лежен Дирихле и Лежэндр, усовершенствовал Племель. Далее Ламе предложил для $n=7$, упрощено Лебегом (n·|| и метрики для подмножеств). Идёт весьма совершенственное развитие чисел вида H.

$$a_0 + a_1\zeta + \ldots + a_{n-1}\zeta^{n-1}; \quad a \in Z$$
$$\zeta = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right); \quad i = \overline{0, n-1} \tag{3.62}$$

ζ - первообразный корень n-ой степени из 1.

Лиувилль – промах подмножества Ламе в том, что числа вида (3.61), подобно Z, единственным образом разлагаются в П простых передложимых чисел. Далее – числа Куммера (1843) – по пути Ламе понимал, что неверная идея искать её доказательство не имеет смысла, а => по Куммеру добавит к числам вида (3.61) новые, которые назвал «идеальными» с целью восстановления подмножества «1» на кратные множители подмножеств в области чисел.

Было Д/З : Разложить 2-мя способами :

$$q = a + b\sqrt{-5}; \quad a, b \in Z$$
$$21 = 3 * 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

(q – являются числами вида ζ мн при к-либо «n» или как говорят «УЖО»).

Но к ним применима идея Куммера. К числам q добавляется идеалети чисел:

$$A, B, C, D \quad \left(4 + \sqrt{-5}\right)\left(4 - \sqrt{-5}\right)$$
$$ideal: \quad A, B, C, D \mid 3 = AB, 7 = CD, 1 + 2\sqrt{-5} = AC, 1 - 2\sqrt{-5} = BD$$

Единственное разложение на простые числа будет восстановлено.

Подобное предположение привело к усложнению, что уже Куммер доказал Теорему для показателей удовлетворяющих $n = L$, удовлетворяющим условию (A) и (B). О них ниже. Он считал их выполнимыми для ∀ простых чисел (но нет – «37» исключение). Результат Куммера заставляет желать лучшего, ибо не давно им 1 простого показателя L, для которого определяется теорема Ферма.

Далее, очень тонким и сложным образом Куммер добился сведения (B) к (A), которое означало чтобы $l \neq h$, h – витиеватое число: $h = h_1 h_2$ были найдены формулы для них и показаны, что $h \mid L \leftrightarrow$ надо $L \mid h_1$ (l-ый множитель) и показал, что это числа Бернулли, то есть L не делит числителей первых (L-3) членов ряда чисел Бернулли.

Это Q-числа

$$B_1 = \frac{1}{6}$$

$$B_2 = \frac{1}{30}$$

$$B_3 = 0\ldots$$

(показан вывод этих коэффициентов в курсах проф. Кузьмина)

Такие простые числа Куммер назвал регулярными. Условие Куммера проверяется для каждого L без особого труда, в том числе и для $L < 100$. Нерегулярные : 37, 59, 67. Совершенно не тривиальны. Нет t.

Считал что регулярных чисел ∞ много. До сих пор не доказал этот факт.

Однако, 1915 г. нашёл теорему о том, что имеется ∞ много нерегулярных простых чисел как это уживается? См. теорему множеств.

1851 г. Куммер: попытка доказать Теорему Ферма для нерегулярных Z.

1858 г. – доказал Теорему Ферма для нек. класса простых показателей L<TOa (с исправлением МЕРТЕНСА и Вандивера)

1858 г. Достижения Русских исследователей

Случай $L = 37$

Теорема Мириманова (жил в Швейцарии, родом из Переславля-Залесского, Дмитрий Семенович Мириманов)

1857 г. Французское АН – 3000 FR – Куммеру (даже не был среди претендентов).

Теорема Вандивера:

Теорема Ферма справедлива для L простого, если

h2 числа h ⁜ l

числители L-3 чисел Бернулли

$B_{2e}, B_{4e}, \ldots B_{2e(e-3)}$

Не делятся на L^3

Для современных ЭВМ проверить 2) труда не составляет.

? – не известно до сих пор такого L простого, для которого оно не выполнимо.

(<100000). Для них условие 2) Теорема Вандивера тоже выполнимо. Т.е. Теорема Ферма справедлива до <100000.

Уже Эйлеру было известно, что при исследовании

$$X^L + Y^L = Z^L;\ \text{L – простое } >= 3$$

Необходимо различать случаи когда ни одно из чисел X, Y, Z не делится на L, от случая, если какой-либо из них делится.

Говорят, что уже (**) не может быть удовлетворено не делящимися на L числами – I случай Теоремы Ферма, а если какой-либо них делится – II случай Теоремы Ферма.

Оказывается, что в отличие от общего случая Теоремы Ферма, Теорема Ферма I допускает для малых L элементарное доказательство – XIX Софи ЖЕРМЕН (1771 – 1831) , Iл женщина –математик нового времени (София Ковалевская, 1850-1891, №1 женщина-профессор в России и №1 в мире - женщина-профессор-математик). Никитский Сорока (Москва) знаменитый деревни за Петровскими Воротами.

Её теория: «и для простого L справедлива Теорема Ферма I, если $(2L+1)$ тоже является простым числом». Ну и ни к чему не привело это. **Теорема Ферма** – сплошные романы в письмах. Это в письме к Лежандру. (Как ведут себя студенты) – от публикация к на нее сослался + его следствие.

Теорема Лежандра: Теорема Ферма I справедлива для простого L , если хотя бы 1 из 5 чисел :

$$4e+1 \quad 8e+1 \quad 10e+1 \quad 14e+1 \quad 16e+1$$

является простым числом.

Тем самым Теорема Ферма I оказывается доказанной для всех простых показателей меньших <197.

$197 = ?$ не было ясно. Последнее качественное улучшение Теоремы Ферма в записях эл.методов - Вендт ввел $\forall m > = 1$

D_mòZ и использовать общую технику. ЖЕРМЕН, показал, что Теорема Ферма I справедлива для простого показателя L, если существует $m > = 1$, такое, что:

1. $P = 2_m L+1$, явл. простым числом ⁜ числа D_m
2. Числа $L^{2m} - 1$ не делятся на P
3. Число D_m допускает 3 равносильных определения.

$$D_m = (-1)^m \prod_{j=1}^{2m-1} \left[\left[1 + \zeta^j \right]^{2m} - 1 \right]$$

$$\zeta = \cos\left(\frac{\pi}{m}\right) + i \sin\left(\frac{\pi}{m}\right)$$

$$P_n = \det \begin{bmatrix} \binom{2m}{1} & \binom{2m}{2} & \cdots & \binom{2m}{2m-1} & \binom{2m}{2m} \\ \binom{2m}{2} & \binom{2m}{3} & \cdots & \binom{2m}{2m} & \binom{2m}{1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \binom{2m}{2m} & \binom{2m}{1} & \cdots & \binom{2m}{2m-2} & \binom{2m}{2m-1} \end{bmatrix} \tag{3.63}$$

где D_m := "результант", а p_1 и p_2:

$$p_1 = x^{2m} - 1$$

$$p_2 = (x+1)^{2m} - 1 \tag{3.64}$$

Не смотря на усилия ≈ 1000 математиков, им не удалось найти никаких других элементарных и вместе с тем достаточно общих подходов к доказательству Теоремы Ферма (хотя бы Теоремы Ферма I).

NB

Общность Теоремы Ферма до сих пор до конца не выяснена. (Подмножество L для студентов: ∃ ли ∞ число простых показателей L, к которым применимо?)

Неэлементарные методы

1-ый Куммер : 1818 г. – доказал, что Теорема Ферма I справедлива для простого показателя L, если на L не делится числитель хотя бы 1 из двух чисел Бернулли B_{L-3} и B_{L-5}.

1905: Миримов: «достаточно, чтобы L не делило числитель хотя бы 1 из 4-х чисел Бернулли

B_{L-3} , B_{L-5} , B_{L-7} , B_{L-9}.

Это доказывает теорему Ферма для $L < 257$

Развивая Виферих 1909.

Теорема: Теорема Ферма I справедлива для всех простых показателей L, для которых $2^{L-1} - 1 \neg | L^2$. Сенсация – для простых чисел 200183 он не даёт ответа лишь для 1093 и 3511.

Теорема Фробениуса. В теореме Вифериха основание 2 может быть заменено на 3, ибо теорема Ферма I оказывается справедлива для любого простого показателя L, для которого хотя бы 1 из числа $2^{L-1}-1$ или $3^{L-1}-1 \neg | L^2$.

Теорема Фуртвенглера 1912 г. (следует из подмножества ζ взаимности Эйзенштейна) – доказал Теорему в несколько строк – самая короткая диссертация на доктора наук.

Теория полей классов. 1941 г – доказал, что в критериях Вифериха основание 2 может быть заменено $\forall$ простым $P <= 3$. Следовательно теорема Ферма I справедлива для всех $L < 6*10^9$

Теорема Вандивера (II) 1934 г. Для простого показателя L справедлива теорема Ферма I, если $h_2 \neg | L$. Эта Теорема интересна тем, что неизвестно ни одного простого показателя L, который этому условию бы не удовлетворял.

Проведём до $L < 100000$.

3.3.6 Результант

Результант 2-х подмножеств P и Q с «к» и корнем над некоторым полем К, называется:

$$\begin{gathered} \operatorname{Re} s(P,Q) = \prod (x-y) \\ (x,y): P(x)=0, Q(y)=0 \\ \deg P(x) = n, \deg Q(x) = m; \\ p_n(x) = q_m(x) = 1 \end{gathered} \tag{3.65}$$

Это произведение полярных разностей между их корнями, которое берётся по всем корням с учётом их кратности.

Основные свойства:

1. $\operatorname{Res}(P,Q)=0 \leftrightarrow$ общий корень у P и Q.
2. Res – есть определитель подмножества Сильвестра.

$$A(x)=\sum_{i=0}^{n}a_i x^i,\quad B(x)=\sum_{i=0}^{m}b_i x^i$$

$$\dim S_{AO}=(n+m)*(n+m)$$

$$S_{AB}=\begin{bmatrix} a_n & a_{n-1} & a_{n-2} & \dots & \dots & a_0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & a_{n-2} & \dots & a_1 & a_0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & a_n & a_{n-1} & a_{n-2} & \dots & a_1 & a_0 \\ b_m & b_{m-1} & \dots & \dots & b_0 & 0 & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & \dots & \dots & 0 & b_m & \dots & b_1 & b_0 \end{bmatrix} \qquad (3.66)$$

3. Количество строк подмножества содержащих «к» элементов $a(x)$ = «m», а множества $в(x)$ = n

$$\operatorname{Re}s(A,B)=\det S_{AB}$$

$$A(x)=a_2x^2+a_1x+a_0$$

$$B(x)=b_3x^3+b_2x^2+b_1x+b_0$$

$$S_{AB}=\begin{bmatrix} a_2 & a_1 & a_0 & 0 & 0 \\ 0 & a_2 & a_1 & a_0 & 0 \\ 0 & 0 & a_2 & a_1 & a_0 \\ b_3 & b_2 & b_1 & b_0 & 0 \\ 0 & b_3 & b_2 & b_1 & b_0 \end{bmatrix} \qquad (3.67)$$

4. Дискриминант – это с точностью до знака, результант $P(x)$ и его $P'(x)$, поделённый на старый «к» многочлен, тем самым, дискриминант = 0 $\leftrightarrow$ (тогда и только тогда) когда у подмножества есть кратные корни.

5. $Res(P1, P2, Q) = Res(P1, Q) * Res(P2, Q)$

6. $Res(P, const) = const^{degP}$

7. $Res(A\,P(x)\,,\,B\,Q(x)\,) = A^{degQ}B^{degP}Res(P(x),Q(x))$

8. если $A \neq 0$, то

$deg(A\,P(x) + B\,Q(x)) = deg(C\,P(x) + D\,Q(x)) = n \quad 1 \rightarrow$

$Res(\,A\,P(x) + B\,Q(x)\,,\,C\,P(x) + D\,Q(x)\,) = (\,AD - BC\,)^n\,Res(\,P(x);Q(x))$

9. $Res\,(P,Q) = 0 \rightarrow deg\ gcd(P,Q) \quad 1$

т.е. результант = 0 $\leftrightarrow$ если НОД нетривиален

NB

Res вычисляем с помощью алгебры Евклида

10. для $P(x);Q(x)$ – многочленов существует $U(x);V(x)$

$$\deg U \Leftarrow \deg P - 1$$
$$\deg V \Leftarrow \deg Q - 1$$

такие, что

$$\mathrm{Re}\, s(P(x),Q(x)) = P(x)V(x) + Q(x)U(x)$$

Если $m = degU, n = degV$, то $u; v$ могут быть получены из представления результанта определителем в форме Сильвестра, в котором последний столбец заменён на

$$(x^m, \ldots, x, 1, 0, \ldots, 0)\ для\ U(x),\ u\ (0, \ldots, 0, x^n, \ldots, x, 1)\ для\ U(x)$$

3.3.7 Числа Бернулли

Первые числа ряда Бернулли представляются следующим образом:

$$B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_3 = 0, B_4 = -\frac{1}{30}, B_5 = 0, B_6 = \frac{1}{42}$$
$$B_7 = 0, B_8 = -\frac{1}{30}, B_9 = 0, B_{10} = \frac{5}{66}, B_{11} = 0 \qquad (3.68)$$

Яков Бернулли :

1. $B_i \in Q$ – выполнение суммирования последовательности натуральных чисел вида:

$$\sum_{n=0}^{N-1} n^k = \frac{1}{k+1} \sum_{s=0}^{k} \binom{k+1}{S} B_S N^{k+1-S} \qquad (3.69)$$

порождает биномиальное «к»

$$\frac{(k+1)!}{S!(k+1-S)!}$$

все B_i с нечётным $N = 0; B = 1/2$

2. Числа Бернулли (Б) являются значениями подмножества (Б) $B_n(x)$ при $x = 0 B_n = B_n(0)$

3. Числа подмножества (Р) выдаёт «к» разложений элементарных функций в степенной ряд :

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n}{(n)!} x^n; \quad |x| < 2\pi$$

$$x * ctg(x) = \sum_{n=0}^{\infty} (-1)^n * B_{2n} \frac{2^{2n}}{(2n)!} x^{2n}; |x| < 2\pi \tag{3.70}$$

$$tg(x) = \sum_{n=0}^{\infty} |B_{2n}| \frac{2^{2n}\left(2^{2n} - 1\right)}{(2n)!} x^{2n-1}; \quad |x| < \frac{\pi}{2}$$

4. Порядок роста чисел Бернулли

$$|B_n| \sim \frac{n}{(2\pi)^n} \quad \textit{при чётном } n \to \infty$$

3.3.8 Теорема Ферма для n = 4

Предисловие

Для любого натурального $n > 2$ уравнение:

$$x^n + y^n = z^n$$

не имеет решения в натуральных числах x, y, z.

Единственный случай, допускающий элементарное доказательство, использует формулы общего решения уравнения:

$$x^2 + y^2 = z^2 \tag{3.71}$$

Если примитивное решение $(x; y; z)$ решение (3.71), тогда и (x; y; z) также решение (3.71). С другой стороны для любых $(x; y; z)$ хотя бы один из x и y чётно. Если x и y нечётны, то $x^2 + y^2$ имеет вид $2_{\kappa+2}$ и следовательно не может быть равно квадрату числа z (ибо каждый z^2 имеет вид либо 4_k, либо 4_{k+1}).

Кроме того вместе с решением $(x; y; z)$, $(\pm x, \pm y, \pm z)$ также даёт решение.

NB

Нам достаточно найти лишь примитивное решение теоремы Ферма, состоящее из положительных чисел.

Лемма: Для любых взаимно простых Z+ m и n; $n < m$ разной чётности, формула:

$$\begin{aligned} x &= 2mn \\ y &= m^2 - n^2 \\ z &= m^2 + n^2 \end{aligned} \tag{3.72}$$

обеспечивает примитивное решение уравнения (3.71) с чётным x, состоящего из положительных целых чисел.

Обратно: Для любых состоящих из «+» чисел примитивные решения $(x; y; z)$ уравнения (3.71), для которого x чётно, выражается как (3.72), где $m,n \left| НОД(m,n) = 0 \right|$ разной чётности.

Доказательство:

$$(2mn)^2 + (m^2 - n^2)^2 \equiv (m^2 + n^2)^2$$

тогда числа (**) составляют решение, для которого x чётно. Если эти числа имеют общий множитель $\lambda \quad 2$, тогда λ будет делить и числа:

$$2m^2 = (m^2 + n^2) + (m^2 - n^2)$$
$$2n^2 = (m^2 + n^2) - (m^2 - n^2)$$

В таком случае $\lambda = 2$, ибо, по условию числа m и n – взаимно просты, но если $\lambda = 2 \Rightarrow y = m^2 - n^2$ четно и $\Rightarrow$ m^2 и n^2 одновременно или четно или нечетно что невозможно, ибо по условию m, n имеют разную чётность. Следовательно, решение (3.72) примитивно.

Обратно: (x, y, z) – произвольные из Z+ примитивные с $x = 2a$ – чётное, т.к. y и z нечётны то тогда $X + Y$, $X - Y$ – чётны.

Пусть:

$$X + Y = 2b$$
$$X - Y = 2c$$
$$(b,c) > 0$$

Каждый общий делитель λ чисел b и c делит $z = b + c$ и $y = b - c \rightarrow \lambda = \pm 1$, т.к. числа b и c взаимно простые. С другой стороны: $4a^2 = x^2 = z^2 - y^2 = 4bc$, т.е. $a^2 = bc$. Подмножество $\{a,b,c\}$ ò $Z+$, таких что:

$$ab = cn$$
$$НОД(a,b) = 1$$

Следовательно, $\exists x, y$ ò N, что $a = x^n$; $b = y^n$, и по этой лемме $\exists \{m,n\} > 0$, что $b = m^2$, $c = n^2$, следовательно $a^2 = m^2 n^2$ и тогда $a = mn$, и

$$x = 2a = 2mn$$
$$y = b - c = m^2 - n^2$$
$$z = b + c = m^2 + n^2$$

и т.д.

Теорема Ферма для n = 4

Уравнение

$$x^4 + y^4 = z^2 \tag{3.73}$$

не имеет решений в Z+

Доказательство. От обратного. Пусть ∃ такое решение уравнения (3.73). Предположим, что НОД $\begin{pmatrix} xy \\ xz \\ yz \end{pmatrix} = 0$, можем выбрать из них min. Ясно, что одно из (x, y, z) должно быть чётным.

Пусть х. т.к.

$$\left(x^2\right)^2 + \left(y^2\right)^2 = z^2$$

т.к.

$$НОД\left\{x^2, y^2, z^2\right\} = 0, \quad \left\{x^2, y^2, z^2\right\} \in Z^+$$

x^2 – чётно, тогда по лемме $\exists\, m, n$ - разной чётности, $\left|НОД(m, n) = 1\right|$ такие, что

$$x^2 = 2mn$$
$$y^2 = m^2 - n^2$$
$$z^2 = m^2 + n^2$$

Если $m = 2k$; $n = 2l + 1 \rightarrow y^2 = 4\left(k^2 - l^2 - l - 1\right) + 3$, что невозможно, ибо любой нечётный квадрат должен иметь вид $4к + 1$, следовательно m нечётно, а число n чётно. Пусть

$$n = 2q, тогда\ x_2 = 4mq\ и\ mq = \left(\frac{x_2}{2}\right)$$

$НОД(m; q) = 1$, следовательно $m = z_1^2$, где $\begin{pmatrix} z1 \\ t \end{pmatrix}$ò$Z+$

$$q = t^2$$

$НОД(z, t) = 1 \rightarrow y^2 = \left(z_1^2\right)^2 - \left(2t^2\right)^2$, т.е.

$$\left(2t^2\right)^2 + y^2 = \left(z_1^2\right)^2$$

т.к. $НОД(z, t) = 1$, следовательно опять применима лемма

$$\exists a, b \in Z^+, \quad a < b, разной\ чётности, НОД(a,b) = 1$$

что

$$2t^2 = 2ab$$

$$t^2 = ab$$

$$y^2 = a^2 - b^2$$

$$z_1^2 = a^2 + b^2$$

$НОД(a;b)=1 \rightarrow$ по лемме доп.

$$\exists\, x_1; y_1 \begin{vmatrix} a = x_1^2 \\ b = y_1^2 \end{vmatrix}$$

из следует, что

$$z_1^2 = x_1^4 + y_1^4$$

т.е. ($z_1 x_1 y_1$) – составляют примитивное решение (3.73) принадлежащее Z+, т.е. в силу выбора $(x\, y\, z)$ должно иметь место $z_1 \geq 2 \rightarrow z_1^{\,2} \geq z$ и неравенство $m \geq m^2 + n^2$ - абсурд.

Таким образом, предположение о существовании у (3.73) Z+ решений приводит к противоречию.

3.3.9 Китайская теорема об Остатках

$$\forall \{n_1, n_2, \ldots, n_k \geq 2\} \in Z$$
$$\forall i \neq j,\ НОД(n_i, n_j) = 1$$
$$\rightarrow \begin{cases} x = b_1 \{n_1\} \\ x = b_2 \{n_2\} \\ \ldots \\ x = b_k \{n_k\} \end{cases} \qquad (3.74)$$

существует решение и более того: $y = x\ \{N\}$, где $N = n_1 n_2 \ldots n_k$ тоже решение

Доказательство. Полагаем i=1,2,…,k

$$N_i = n_1 \cdot n_2 \cdot \ldots \cdot n_{i-1} \cdot n_{i+1} \cdot \ldots \cdot n_k = \frac{N}{n_i}$$

В силу попарной простоты $n_1 n_2 \ldots n_k$ число N_i взаимно простое с n_i, где $i = \overline{1;k}$. N_i обратимо по n_i, т.е. существует $M_i \in Z$, что $N_i * M_i = 1\{n_i\}$

Мы утверждаем что

$$x = b_1 M_1 N_1 + \ldots + b_k M_K N_K$$

также решение системы.

Произведём вычисление $\{n_i\}$. В этом случае все числа $b_l M_l N_l$ для $l \neq i$ удовлетворяют сравнению $b_l M_l N_l = 0\{n_i\}$ потому что тогда $N_i \vdots n_i$.

В то же t по нашему выбору выполнимо сравнение $M_i N_i = 1\{n_i\}$, а вместе с

$$b_i M_i N_i = b_i \{n_i\} \tag{3.75}$$

ним и сравнимы

следовательно, $x = b_i \{n_i\}$ для $\forall = \overline{1,\kappa}$, что и требовалось доказать.

Если $y = x\{N\} \rightarrow y = x + qN$ для $q \in Z$, т.к. $N = 0\{n_i\}$, то $y = x = b_i \{n_i\}$, что верно для $\forall i = \overline{1,k}$. Т.е. у также является решением (3.74). Пусть теперь $x, y - 2$ решение (3.74). Т.к. $x = y = b_i \{n_i\}$, что равносильно делимости $(x - y) \vdots n_i$, для $\forall i$ мы получим делимость $(x - y) \vdots \mathrm{N}$, ибо $N = \prod n_i$, а это означает, что $x = y\{N\}$, и т.д.

Пример.

$$\begin{cases} x = 5_{b_1} \{11\}^{n_1} \\ x = 4_{b_2} \{13\}^{n_2} \\ x = 3_{b3} \{24\}^{n_3} \end{cases}$$

$$b_1 = 5, b_2 = 4, b_3 = 3,$$
$$n_1 = 11, n_2 = 13, n_3 = 24;$$

Далее

$N = n_1 n_2 n_3 = 3432$

$N1 = n_2 n_3 = 312$

$N2 = n_1 n_2 = 264$

$N3 = n_1 n_3 = 143$

M1 , M2 , M3 - вычисляем по обобщённому алгоритму Евклида:

$312 = 11*28 + 4$

$\downarrow 11 = 4*2 + 3$

$4 = 3*1 + 1$

Далее

$\uparrow 1 = 4 - 3*1 = 4 - (11 - 4*2)*1 = 4*3 - 11*1$

$= (312 - 11*28)*3 - 11*1 = 312*3 - 11*85$

$\Rightarrow 312*3=1\{11\}$

$312^{-1}=3\{11\}$

$M_3=3$

$\downarrow 264=13*20+4$

$13=4*3+1$

$\rightarrow\uparrow 1=13-4*3=13*(264-13*20)3=-264*3+13*61$

$\rightarrow 264*10=1\{13\}$

$264^{-1}=10\{13\}$

$M_2=10$

$\downarrow 143=2*5+23$

$24=23*1+1$

$\rightarrow\uparrow\ 1=24-23*1=24-(143-24*5)1=24*5-143*1$

$\rightarrow\ 143*23=1\{24\}$

$143^{-1}=23\{24\}$

$M_3=23$

т.о. решением является

$x=5*312*3+4*264*10+3*143*23=4680+10560+9867=2510\ 7$

3.3.10 Поле Ке и кольцо De

Единственный известный в настоящее общий метод доказательства Теоремы Ферма – для $\forall e >= 3$ (к сожалению, пока успешно не для всех е), восходит к Куммеру и → на основные обобщения идей Эйлера. Основная роль в некотором поле Ке. Мы говорим о переходе Эйлера от Z к числам вида $a+в\sqrt{-3}$ для доказательства такого перехода необходимо построение арифметики чисел $a+в\sqrt{-3}$.

В частности подмножество булево:

взаимная простота чисел $a+в\sqrt{-3}$

проверить Теорему Ферма для показателя ʒ

(Если взаимно простые целые числа а и в обладают свойством, что $a^2+3в^2$ является кубом целого числа, то $\rightarrow s$ и $t\in Z$

$$a = s(s^2 - 9t^2)$$

$$b = 3t(s^2 - t^2)$$

Основная Теорема Ферма арифметика для чисел $a + в\sqrt{-3}$ не верим в существование «1» разложения на простые (неразложимые) множители.

$$4 = 2 * 2 = \left(1 + \sqrt{-3}\right)\left(1 - \sqrt{-3}\right)$$

НО(!) и 2 и $1 \pm \sqrt{-3}$ неразложимы !

Вопрос: Закономерно ли у Эйлера появление чисел вида $1 \pm \sqrt{-3}$?

Если вообще прибегать к каким-либо нецелым числам, то в I-ую очередь следует привлечь числа, участвующие в разложении левой части уравнения Ферма на линейные множители. Оно имеет вид:

$$x^3 + y^3 = (x + y)(x + \zeta y)(x + \overline{\zeta y})$$

$\{\xi, \overline{\xi}\} \in C$, является вместе с 1 корнем уравнения $x^3 = 1$, т.о. естественно рассмотреть решение $x^3 + y^3$ в числах вида:

$$a + b\zeta + c\overline{\zeta}, \{a, b, c\} \in Z \tag{3.76}$$

NB

Вместе с ʒ корнем (3.76) будет и ξ^2:

$$\left(\xi^2\right)^3 = \left(\xi^3\right)^2 = 1^2 = 1 \tag{3.77}$$

т.е. $\xi^2 = \overline{\xi}$ и (3.76) правильнее записать в виде

$$a + b\xi + c\xi^2$$

Более того, числа ʒ вместе с $\overline{\xi} = \xi^2$ являются корнем уравнения

$$\frac{x^3 - 1}{x - 1} = x^2 + x + 1 = 0$$

т.е. $\xi^2 = -1 - \xi$, и следовательно $\forall$ число (3.76) имеет вид

$$A + B\xi \tag{3.78}$$

где $A = a - c$, $B = в - c$. Множество чисел вида (3.78) $detD_3$. Сумма и разность чисел из D_3 является числом из D_3 , и произведение тоже. (появление после (*умножения) член ξ^2 может быть преобразован по $\xi^2 = -1 - \xi$)

$$\left(A + B\xi\right)\left(A_1 + B_1\xi\right) = (AA_1 - BB_1) + (AB_1 + BA_1 - BB)\xi,$$

т.е. D_3 – числовое кольцо для рассмотрения чисел (3.78), где $\{A, B\} \in Q$. Подмножество этих чисел отражается через K_3 . Ясно, что сумма, разность, умножение чисел из K_3 будет всё ещё внутри в K_3 .

Однако, теперь и частное любых двух чисел из K_3 будет числом из K_3.

$$\frac{C+D\xi}{A+B\xi}=\frac{\left(A+B\bar{\xi}\right)}{\left(A+B\bar{\xi}\right)}\frac{C+D\xi}{A+B\xi}=(A+B\xi\neq 0)$$

$$=\frac{\left(C+D\xi\right)\left(A+B\xi^2\right)}{A^2+AB(\xi+\bar{\xi})+B^2\xi\bar{\xi}}=$$

$$=\frac{CA+DA\xi+CB\xi^2+DB\xi^3}{A^2-AB+B^2}=$$

$$=\frac{CA+DA-CB}{A^2-AB+B^2}+\frac{DA-CB}{A^2-AB+B^2}$$

Следовательно K_3 является 3-х круговым полем (следует из задачи деления круга на 3 части – 3 корня). Числа D3 называются естественно целыми числами поля K_3. D_3 определено кольцом целых чисел поля K_3. Оно содержит все Z обычные при $B=0$.

NB

Запись чисел из K_3, K_3 в форме (3.78) единственна!

Действительно, если

$$A+B\xi=A_1+B_1\xi$$

$$B\neq B_1\rightarrow\xi=\frac{A-A_1}{B-B_1}$$

что не может быть, ибо ξ не принадлежит R (и тем более Q), и следовательно $B=B_1$ и следовательно $A=A_1$

$$\forall\alpha=A+B\xi\in K_3$$

$$N\alpha=\alpha\bar{\alpha}=A^2-AB+B^2=\frac{(2A-B)^2+3B^2}{4}$$

Это неотрицательное Q число определено нормой числа α.

$$\|\alpha\|=0\leftrightarrow\alpha=0$$

Замечательное свойство $\|\cdot\|$:

$$N(\alpha\beta)=N\alpha*N\beta;(\alpha,\beta)\in K_3$$

$$N(\alpha\beta)=\alpha\beta\overline{\alpha\beta}=\alpha\beta\bar{\alpha}\bar{\beta}=N\alpha*N\beta=$$

$$=(A^2-AB+B^2)(A_1^2-A_1B_1+B_1^2)$$

Числа из K_3 (и D_3) могут быть записаны в более явной форме. Заметим, что

$$x^2+x+1=0$$

имеет корни:

$$x_{1,2} = \frac{-1 \pm \sqrt{-3}}{2}$$

Пусть

$$\xi = \frac{-1 \pm \sqrt{-3}}{2}$$

следовательно: $A + B\xi = \frac{(2A - B) + B\sqrt{-3}}{2}$ таким образом числа из К3 имеют вид:

$$a + b\sqrt{-3}, \text{где } \{a,b\} \in Z$$

одинаковой чётности! При {p; q} чётных – получаем числа Эйлера $a + b\sqrt{-3}$, то есть ограничения только такими числами с общей точкой зрения имеем не оправдано.

Кольцо De

Известно понятие коммутативности, ассоциативности, и с единицей 1 кольца. Такие подмножества колец определяются целыми, если они не имеют делителей «0» - т.е. произведение любых двух его не равных нулю элементов не равно нулю. Каждое $\alpha \in Z$ мы будем отождествлять с элементом $a * 1$ где 1 – единичный элемент D. То есть кольцо целых рациональных чисел Z окажется подкольцом кольца D. Основное свойство целых колец в том, что в них (и только в них) справедливо правило сокращения:

т.е. если $\alpha\beta = \alpha\gamma, (\alpha \neq 0) \rightarrow \beta = \gamma$

Элемент е в De определяется обратимым элементом, если

$$ee^{-1} = 1$$

произведение ee и $e / e \equiv 1$

Пример: у целых и рациональных чисел две единицы - +1 и -1, а в кольце De - $n \in D \mid e^n = 1$. Таким образом получаем, что каждый корень из последнего соотношения будет единицей кольца.

Какие е в D_3? Пусть α - единица D_3. Тогда:

Следовательно если $N\alpha = 1$, $\alpha\alpha^{-1} = 1$

$$N\alpha * N\alpha^{-1} = N(\alpha\alpha^{-1}) = N1 = 1$$

$$N\alpha = A^2 - AB + B^2 = \frac{(2A - B)^2 + 3B^2}{4},$$

то $N\alpha = 1$ тогда и только тогда, когда либо $B = 0$ и $A = \pm 1$; $B = \pm 1$ и $(2A - B)^2 = 1$, т.е. $A = B = \pm 1$

или $A = 0;\ B = \pm 1$ тогда, кольцо D_3 имеет 6 едининчек

$$+1; +\xi; 1+\xi = -\xi^2; -1; -\xi; -1-\xi = \xi^2 \qquad (3.79)$$

Все они корни из «1» степени 6.

При этом каждая «1» являющаяся степенью 1

$$1+\xi = \frac{1+\sqrt{-3}}{2}$$

А именно :

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

Пусть $D^* = D \setminus \{0\}$

$\{\alpha; \beta\} \in D^*$ определена ассоциировано, если Э единица ξ, что $\beta = e\alpha$

NB

Отношение ассоциированное является отношением эквивалентности и следовательно подмножество D^* распадается на классы ассоциированных элементов.

Пусть $D' \delta D^*$ - подмножество $\neq 0$ элементов кольца D, на являющееся «1». Элемент $\alpha \in D'$ называется определённо разложимым, если $\exists\ \beta; \gamma \in D' \mid \alpha = \beta\gamma$. Неразложимый $\alpha' \in D'$ называется определённо простым.

Функция $\alpha \to \|\alpha\|$, определенная на $D*$ и принимающая значения на N определяется псевдонормой, если из того, что $\alpha \grave{o} D*$ делится на $\beta \in D*$ (т.е. $\alpha = \beta\gamma;\ \gamma\ \grave{o} D$) $\longrightarrow$ что $\|\alpha\| \geq \|\beta\|$.

Если γ – единица; то $\beta = \alpha\gamma^{-1}$, где $\gamma^{-1} \in D$ и потому $\|\beta\| > \|\alpha\|$. Тогда если α и β ассоциированы, то $\|\alpha\| = \|\beta\|$. Если обратное верно, т.е. если $\|\beta\| > \|\alpha\|$, когда α делится на β , но частное γ не является «1», то псевдонорма опред. строгой.

Пример: В D_3 строгая псевдо ||·|| является обычной ||·||.

3.3.11 Теория чисел. Кольца

Кольцо — множество R с двумя двоичными операциями сложения + и умножения·, такими что

относительно сложения R — коммутативная группа (которая называется аддитивной группой кольца);

умножение ассоциативно;

$$\begin{aligned} a(b+c) &= ab+ac; \\ (b+c)a &= ba+ca; \end{aligned} \tag{3.80}$$

(дистрибутивность умножения слева и справа относительно сложения).

Если кольцо имеет единичный элемент для умножения, то кольцо называется кольцом с единицей. Мы будем обозначать единицу через 1, несмотря на двусмысленность этого обозначения. Если умножение коммутативно, то такое кольцо называется коммутативным кольцом.

Замечание 3.1. В литературе встречается другое определение кольца, в котором опущена аксиома ассоциативности R^2.

В таких книгах кольца с ассоциативным умножением называются ассоциативными. Нам удобнее использовать более узкое понятие кольца.

Замечание 3.2. Когда рассматриваются кольца с единицей, почти всегда исключается вырожденный случай $0=1$. Далее всегда предполагается, что в кольцах с единицей $0 \neq 1$.

Обратного элемента по второй операции (умножению) в кольце может и не быть. Поэтому уравнение $ax = b$ может не иметь решений в кольце.

Классический пример кольца — это множество целых чисел с операциями сложения и умножения. Обозначается кольцо целых чисел через Z. Обратного элемента по умножению нет для всех целых чисел, за исключением ± 1. Другой важный пример кольца — кольцо многочленов — подробно рассматривается ниже. Из аксиом кольца следует довольно много тривиальных следствий. Приведем здесь только самые необходимые, и будем вводить остальные по мере надобности.

Утверждение 23.3. В любом кольце

$$a(b-c) = ab-ac$$

Это утверждение означает, что дистрибутивность выполняется и для вычитания (сложения с противоположным, т. е. обратным относительно сложения).

Доказательство.

$$a(b-c)+ac = a(b-c+c) = ab$$

Конечно, выполняется также и равенство

$$(b-c)a = ba - ca$$

Утверждение 23.4. В любом кольце $a \cdot 0 = 0$.

Доказательство.

$$a0 = a(b-b) = ab - ab = 0$$

Выполняется также и аналогичное равенство при умножении на 0 слева: $0 \cdot a = 0$

Для чисел и многочленов выполняется такое свойство: если произведение двух элементов равно нулю, то хотя бы один элемент равен нулю. В общем случае это свойство может не выполняться. Давайте рассмотрим некоторые примеры.

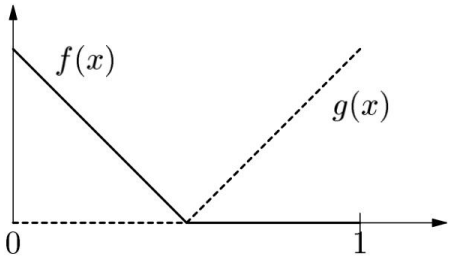
Пример 23.5. Множество целых чисел с операциями сложения и умножения по модулю 4. Более точно, мы рассматриваем операции на множестве вычетов по модулю 4, т. е. не различаем числа, разность которых делится на 4. Относительно этих операций множество из четырех различных вычетов по модулю 4, т.е. $\{0,1,2,3\}$, образует кольцо. И в этом кольце произведение двух не равных нулю элементов может быть нулевым: $2 \cdot 2 = 0$

Пример 23.6. Прямым обобщением предыдущего примера является кольцо вычетов по модулю n, где n — натуральное число. Элементами этого кольца, которое мы будем обозначать Zn, являются числа $0, 1, \ldots, n-1$. Сложение и умножение в этом кольце определяются как сложение и умножение по модулю n. Аналогично предыдущему примеру можно заметить, что если число $n = ab$ — составное, то $ab = 0$ в Zn. Оказывается, что если n — простое, то произведение ненулевых элементов в Zn обязательно отлично от 0. Доказательство этого утверждения будет приведено ниже.

Пример 23.7. Есть еще один важный пример — кольцо непре- рывных функций на отрезке $[0,1]$ с обычными операциями поточечного сложения и умножения функций:

$$(f+g)(x) = f(x) + g(x), (f * g)(x) = f(x)g(x)$$

Нулем этого кольца является функция, тождественно равная нулю. Рассмотрим две ненулевых функции f, g, графики которых изображены на рисунке. Очевидно, что произведение этих функций тождественно равно нулю.



Пример 23.8. По двум кольцам R1, R2 можно определить их прямую сумму $R1 \oplus R2$ аналогично прямому произведению групп и прямой сумме абелевых групп.

Кольцо $R1 \oplus R2$ состоит из всевозможных пар $(r1, r2)$, где $r1 \in R1,\ r2 \in R2$. Операции определяются так:

$$(r_1, r_2) + (r_1', r_2') = (r_1 + r_1', r_2 + r_2')$$
$$(r_1, r_2) * (r_1', r_2') = (r_1 * r_1', r_2 * r_2')$$

(для простоты обозначений мы используем одни и те же символы для операций в обоих кольцах).

Проверка аксиом кольца для прямой суммы колец выполняется механически. По сложению это группа, которая есть прямое произведение аддитивных групп колец $R1$ и $R2$. Ассоциативность умножения и дистрибутивность проверяются покомпонентно.

В прямой сумме колец несложно построить пару ненулевых элементов, произведение которых равно нулю.

Используем **утверждение 23.4**:

$$(a,0) * (0,b) = (a * 0, 0 * b) = (0, 0)$$

Ненулевые элементы кольца, произведение которых равно нулю, имеют специальное название — делители нуля. Технически бывает удобно различать левые и правые делители нуля. Элемент $a \in R$ называется правым (левым) делителем нуля, если для некоторого $b \in R$ выполняется $ba = 0\ (ab = 0)$.

Наличие делителей нуля в кольцах является крайне неприятным эффектом. Поэтому выделяется класс колец без делителей нуля. Коммутативные кольца без делителей нуля называются целостными кольцами (или областями целостности). Как правило, мы будем рассматривать целостные кольца, поскольку они дают важные для приложений примеры.

3.3.12 Модуль над кольцом

Одно из основных понятий в общей алгебре. Обобщение 2-х понятий – векторного пространства и абелевой группы.

Векторное пространство это модуль над полем абелевой группы, модуль над кольцом Z.

В векторном пространстве Подмножество скаляров образует поле и умножение на скаляр удовлетворяет нескольким аксиомам:

дистрибутивность умножения.

В модуле Подмножество многочленов требуется лишь, чтобы скаляры образовывали кольцо (ассоциативное, с «1»), аксиомы оставались теми же самыми. Значительная часть Теории модулей состоит из попыток обобщить на них известные свойства векторного пространства. Иногда для этого приходится ограничивать модуль над “хорошими” кольцам. Пример – кольцо главных идеалов.

Подмножество в целом устроено более сложно, чем векторные пространства.

NB

Не в каждом подмножестве может быть выбран базис.

И даже там, где этот возможно может быть несколько аддитивных групп с различным числом элементов (некоммутативное кольцо).

R подмножество - кольцо, пусть, далее коммут., с 1 R – подмножество def, если M – абелева подмножество групп с отражением умножения на элементы кольца R:

$$R \times M \to M(r,m) \to rm$$

$$\forall m \in M, \forall r_1, r_2 \in R: \quad (r_1 r_2)m = r_1(r_2 m)$$

$$\forall m \in M: 1m = m1 = m$$

$$\forall m_1, m_2 \in M, \forall r \in R: \quad r(m_1 + m_2) = rm_1 + rm_2$$

$$\forall m \in M; \forall r_1, r_2 \in R: (r_1 + r_2)m = r_1 m + r_2 m$$

(Если R - не коммутативно, то эти подмножества (r_1 и r_2) называются левыми.)

Правые подмножества

$$\forall m \in M; \forall r_1, r_2 \in R: \quad (r_1 r_2)m = r_1(r_2 m)$$

Что гораздо удобнее формулировать, записывая элементы кольца справа от элемента подмножества m.

$$\forall m \in M; \forall r_1, r_2 \in R: \quad m(r_1 r_2) = (mr_1)r_2$$

отсюда и терминология. Любое кольцо R может быть рассмотрено как подмножество над собственным (В некотором случае оно является правым Подмножеством над собой).

Подмножество подмножества M_R называется подмножеством подгрупп В подгруппе М, замкнутая относительно умножения на элементы из R, т.е. :

$$\forall b \in B; r \in R: \quad rb \in B$$

Если R рассматривать как левое подмножество над собой, то его подподмножества являются левыми идеалами; если кольцо рассматривать как правое подмножество, то правыми идеалами.

В комм. случае считается левый и правый идеалы идеально совпадают.

Пример:

1. любая абелева Подгруппа – подмножество над Z.
2. Любая ограниченная (т.е. $nA = 0$).
3. Подмножество над кольцом Zn классов вычетов по модулю n.
4. Линейное пространство над полем F является подмножеством над F.
5. Линейное пространство V - подмножества над кольцами всех своих линейных преобразований.
6. I – левый идеал кольцо R, $\rightarrow$ он будет левым Подмножеством над этим кольцом.

3.3.13 Коммутативный моноид

Задано некоторое подмножество D, в котором определено коммутативное и ассоциативное умножение, обладающее 1. Обычно элементы такого множества принято означать малыми готическими буквами (единица, в том числе обозначается e).

Говорят, что $\beta \in \delta$ делит элемент $c \in \delta$, если $\exists b \in \delta \,|\, c = b\beta$. Если элемент $b \neq e$ делится только на себя и на e, он называется простым.

Моноид D называется свободным (коммутативным) моноидом (или моноидом с однозначным разложением на простые множители), если каждый $\beta \in \delta$ может быть представлен в виде:

Моноид D называется свободным (коммутативным) моноидом (или моноидом с однозначным разложением на простые множители), если каждый $\beta \in \delta$ можно представить в виде:

$$\beta = r_1 \ldots r_p;\ p \geq 0$$

и такое разложение с точностью до порядка множителей «1» (при $p = 0$ произведение считается равным e).

NB

В свободном моноиде $\mathbb{ZZ}$ нет обратимых элементов («1»), кроме «настоящей» единицы e.

Пример:

Подмножество N по отношению к умножению. В свободном моноиде для любых элементов ∃! НОД и ∃! НОК. Если $НОД \equiv e$, то элементы называются взаимно простыми.

В произвольном сводном моноиде сохраняются известные свойства делимости в свободном моноиде N.

Пример:

1. Если $\alpha\beta \mid \vdots$ на C и α взаимно просто с $C \to \beta$ делится на C.
2. Если α и β взаимно просты и $\alpha\beta = C^2$, то $\exists\, \alpha_1 и\, \beta_1$, что $\alpha = \alpha_1^n$ и $\beta = \beta_1^n$ и т.д.

Для произвольного кольца D множество D* вех его $\neq 0$ элементов является, очевидно, моноидом. Пусть задано некоторое подмножество этого моноида в свободный моноид D. Обозначая образ элемента α ϵ D* символом (α), потребуем, чтобы для $\forall \alpha, \beta \in D^*$ было бы выполнено

$$(\alpha\beta) = (\alpha)(\beta)$$

т.е. подмножество атрибутов $\alpha \to (\alpha)$ было бы полиморфизмом моноидов. Тогда, если $\alpha \vdots \beta$ в δ, то $(\alpha) \vdots (\beta)$ в D. Потребуем, чтобы было верно и обратное.

Аксиома 1: Элемент $\alpha \in D^*$ тогда и только тогда $\vdots \beta \in D^*$, когда $(\alpha) \in D^*$ $\vdots$ $(\beta) \in D^*$. В частности отсюда следует, что $(\alpha) = (\beta)$ тогда и только тогда, когда элементы α и β ассоциированы.

NB

Единица кольца D характеризуется равенством $(e) = e$

Если элемент $\alpha \vdots (\alpha)$, то может быть рассмотрена совокупность всех $\alpha \in D^* \vdots \widetilde{\alpha} \in D$ + элемент $0 \in P$ (который мы таким образом определённо считаем делящимся на любой элемент $\alpha \in D$), совокупность, которая далее обозначается, как $[\alpha]$. Естественно требуется, чтобы сумма и разность

элементов кольца D, делящихся на α òD также делилась бы на α . Что формализуется в виде:

Аксиома 2:

Если

α, β ò$[\alpha]$

следовательно

$\alpha \pm \beta$ ò$[\alpha]$

Наконец потребуем, чтобы в D не было «лишних» элементов, т.е. $\forall 2$ элемента у D отличались по их свойствам делимости по отношению к элементам кольца D.

Аксиома 3:

Если

$[\alpha]=[\beta]$

следовательно

$\alpha = \beta$

и для $\forall\alpha$ подмножества $[\alpha]$ содержит $\neq 0$ элементы (стараюсь как могу объяснить просто, ибо:) все выше сказанное может быть сказано мехмат языком:

Мы имеем дело с моноидами, которые являются обобщением подмногообразий «1» алгебраического многообразия | соразмерности

(Алгебраическое локальное кольцо общей $(\cdot)\forall$ неприводимого замкнутого подмножества регулярно).

3.3.14 Применение теории чисел. Криптография. Шифрование. Дискретный логарифм.

Пусть $p \equiv 3\ \{n\}$ Если с ò$Z * p$ – квадратный вычет, из этого следует, что:

$$\sqrt{C} = C^{\frac{p+1}{4}}\ \{p\} \to \left(\frac{p+1}{4}\right) \tag{3.81}$$

Если $p \equiv 1\{n\}$, то корень тоже может быть вычислен за короткое время, но сложнее. t вычисляем $\sim O\left(lg_2^3 p\right)$.

Умея вычислять подмножество квадратных вычетов, можно найти каждое решение квадрата уравнения по модулю p вида:

$$ax^2 + bx + c = 0\ \{p\}$$

решение отыскивается по той же формуле, что и для обычного квадратного уравнения:

$$x \equiv \frac{-b + \sqrt{b^2 + 4ac}}{2a}\{p\}$$

NB

Однако для $\frac{1}{2a}\{p\}$ нужно найти некоторое расширение алгоритма Евклида, $a\sqrt{b^2 - 4ac}\{p\}$ – если он $\exists!$, то искать, используя (3.81).

Далее:

Пусть N – составное число, тогда: когда $\exists \sqrt{C_{\{p\}}}$ и каково время его вычисления?

Подход - факторизация N

Данный факт используется в криптосистемах, основанных на Факторизации Z, таких как RSA и Росбиен.

Пример:

Рассмотренное нами ранее, приведение к построению алгоритмов, выполняемых за короткое время.

По заданному составному N и $x \in Z_n$ найти $x^{-1}{}_{\{N\}}$ легко. По заданному простому числу p и полиному $f(x) \in Zp[x]$, найти $z \in Zp$ такое, что $f(x) \equiv 0\{p\}$, если оно существует, также легко причём время вычислений оценивается линейной функцией от deg f.

NB

Э большой набор вычислительно сложных задач теории чисел.

Выберем простое $p > 2$ и $g \in Z * p$ порядка q. Возьмем функцию $x \to g +$в Zp и рассмотрим обратную функцию D

$$\log_g(g^x) = x, \text{ где } x \in (0,\ldots,q^{-2}).$$

Эта функция называется функцией дискретно логарифмированной.

Пример:

$$\mathbb{Z}_{11}$$

$$D\ log_2(1)=0 \qquad D\ log_2(3)=8 \qquad D\ log_2(8)=3$$
$$D\ log_2(2)=1 \qquad D\ log_2(4)=2 \qquad D\ log_2(9)=6$$
$$D\ log_2(5)=4 \qquad D\ log_2(10)=5$$
$$D\ log_2(6)=5$$
$$Dlog_2(7)=7$$

Функция дискретного логарифма может быть обобщена.

Пусть G – конечная циклическая группа, а g – образуемый элемент G, т.е.:

$$G=\langle g\rangle=\{1, g, g^2,\ldots, g^{q-1}\}$$

q – порядок группы G.

Говорят, что заданное дискретное логарифмирование является вычислительно сложной в G, если для любого алгоритма A, выполнимого за полиномиальное время, вероятность $P_{(g\leftarrow G;x\leftarrow Zp)}[A(G,q,g,g^x)=x]$ составляет пренебрежимо малую величину.

Пример:

Группы, в которых задано дискретное логарифмирование являющееся вычислительно сложной, является группой Z*p, где p-большое простое число, а также группа точек эллиптической кривой над конечным полем.

Лучший из известных алгоритмов дискретного логарифмирования для группы $Z*p$ – обобщение так называемого алгоритма «решето числового поля». Его трудоемкость оценивается величиной $e^{O(\sqrt[3]{n})}$, где n – длина числа p в битах.

Вторая вычислительно сложная проблема – факторизация, разложение большого составного числа на простые сомножители.

Рассмотрим подмножество $Z_{(2)}(n) = \{N \mid N=pq\}$, где p, q – n битные простые числа. Задача нахождения p и q по заданному N в этом случае вычислительно сложная.

Проблема факторизации Z сформулирована Гауссом в 1806 году.

Лучший алгоритм - $e^{O(\sqrt[3]{n})}$ - для n – битных чисел.

Мировой рекорд – факторизация 768-битного модуля системы RSA (имеющий 232 десятичные цифры в записи числа).

Потребовалось ≈ 2х лет одновременной работы компьютерной сети США.

В ближайшее время станет возможным факторизация 1024-битных чисел – ее трудоемкость на 3 порядка выше.

Также по заданному полиному $f(x)$; $deg\, f(x) > 1$ и случайному числу N ò $Z_{(2)}(n)$ вычислительно трудно найти $x \in Zn$ такое, что $f(x) \equiv 0\{N\}$.

СПИСОК ЛИТЕРАТУРЫ

1. Ю.И.Журавлев, Ю.А.Флеров, О.С.Федько Дискретный анализ. Комбинаторика. Алгебра логики. Теория графов. -М.:МФТИ, 2012.

2. М. Холл Комбинаторика, -М: «МИР», Москва, 1970

3. А.И.Сирота, Ю.И.Худак Основы дискретной математики. -М: МИРЭА, 2010.

4. В.И. Кузьмин, А.Ф. Гадзаов Модели и методы научно-технического прогнозирования. -М: МИРЭА, 2016.

Сведения об авторах

Дзержинский Роман Игоревич, кандидат технических наук, заведующий кафедрой Прикладная математика, институт информационных технологий, МИРЭА - Российский технологический университет.

Юрченков Иван Александрович, ассистент кафедры Прикладная математика, институт информационных технологий, МИРЭА - Российский технологический университет.