В.С. Кугураков

Элементы общей алгебры, теории чисел и комбинаторики

Казань-2020

УДК 512.8+511.00
ББК 22.19
Г22

Печатается по рекомендации
Научно-образовательного математического центра
Приволжского федерального округа

Рецензент:
д-р физ.-мат наук, профессор А.Н. Абызов

Научный редактор:
д-р физ.-мат наук, профессор М.М. Арсланов

Кугураков В.С.

Учебник посвящен систематическому изложению математического аппарата, входящего в федеральный компонент дисциплины "Алгебра" по направлениям бакалавриата и магистратуры "Информационная безопасность" и "Прикладная математика и информатика". Рассматривается иерархия алгебраических структур – группоиды, полугруппы, моноиды, группы, кольца, тела и поля, элементы теории чисел и комбинаторики. Основное внимание уделено изучению строения конечных полей Галуа, которые находят широкое (прикладное) применение в теории кодирования, криптографии и других областях дискретной математики. В частности, рассмотрены методы вычисления корней многочленов над конечными полями и методы разложения многочленов на неприводимые сомножители. В доступной учебной литературе эти вопросы отражены еще весьма слабо.

Книга рассчитана на студентов и аспирантов, обучающихся по математическим специальностям, а также на преподавателей. Она может служить основой при разработке специальных курсов и выполнении курсовых проектов.

Учебное издание

Владимир Сергеевич Кугураков
Элементы общей алгебры, теории чисел и комбинаторики: Учебник.
– Казань, 2020. – 232 с.

ISBN

Оглавление

Введение

Эта книга возникла из специального курса лекций «Общая алгебра и теория чисел», читаемого студентам 3 курса, обучающихся по направлению «Прикладная математика и информатика», а также студентам 1-го года обучения по направлению магистратуры «Прикладная математика» и «Информационная безопасность» в Казанском (Приволжском) Федеральном Университете. По мере написания пособия курс оброс дополнительными материалами, хотя многое остаётся за бортом. Поскольку слушатели этого курса владеют, как правило, лишь основами линейной алгебры, то освоить курс в полном объёме физически трудно. Те же трудности возникают и у лектора ввиду скромного числа лекционных часов. Поэтому при первом чтении некоторые разделы можно пропустить. Они могут служить основой для самостоятельного изучения и выполнения курсовых работ.

Основная (практическая) цель курса – введение в элементарную теорию чисел (более точно: модулярную арифметику) и теорию конечных полей. Конечные поля начали изучать в начале XIX века. Заслуга в их изучении несомненно принадлежит К.Ф. Гауссу и Э. Галуа. Первоначально конечные поля находили применение только в алгебре и теории чисел. Но постепенно круг использования конечных полей существенно расширился. Они нашли широкое применение в теории колец и полей, теории групп, алгебраической геометрии, комбинаторном анализе, криптографических методах защиты информации, при построении генераторов псевдослучайных чисел, но особенно в теории кодов с исправлением ошибок. Не вдаваясь в описание содержания глав пособия (с этим можно познакомиться в оглавлении), отметим, что седьмая глава посвящена решению алгебраических уравнений от одного неизвестного в конечных полях. Соответствующий материал, по нашему мнению, весьма слабо отражен в учебной литературе и разбросан по журнальным статья. Мы восполняем этот пробел. Результаты этой главы, как и результаты некоторых других параграфов могут служить основой для курсовых работ.

О нумерации утверждений и формул. Утверждения – теоремы, леммы и следствия – имеют двойную нумерацию: вначале номер параграфа, затем номер утверждения. Формулы в каждом параграфа нумеруются с 1, но при ссылке из другого параграфа поступаем аналогично: вначале пишем номер параграфа, затем – номер формулы.

Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.

Бог создал целые числа, всё остальное — дело рук человека.

Леопольд Кронекер [1]

Глава I. Множества и отображения

§ 1. Множества

Понятие множества является основным в математике и логике.

Определение. Под *множеством* понимается любая совокупность объектов, называемых э*лементами* множества, обладающих общим для всех характеристическим свойством.

Замечание. Георг Кантор [2], создатель теории множеств, даёт такое определение: *«множество есть многое, мыслимое нами как единое»*. Эти определения не являются логически строгими, а всего лишь пояснениями, поскольку понятие множества принадлежит к числу первоначальных понятий и не может быть описано с помощью более общего родового понятия, в котором оно выступает в качестве подвида. Множества описываются только при помощи примеров.

Основным понятием в теории множеств является понятие *принадлежности* элемента множеству. Если объект x принадлежит множеству X, то пишут $x \in X$, в противном случае пишут $x \notin X$.

Множество можно описать путём перечисления его элементов либо задать правило (свойство) для определения того, принадлежит

---

[1] ***Леопольд Кронекер*** (7.12.1823 – 29.12.1891) – немецкий математик. Основные труды по алгебре и теории чисел, где он продолжил работы своего учителя Э. Куммера по теории квадратичных форм и теории групп. Большое значение имеют его исследования по арифметической теории алгебраических величин

[2] ***Георг Кантор*** (3.03.1845 – 6.01.1918) – немецкий математик, ученик Вейерштрасса. Наиболее известен как создатель теории множеств. Основатель и первый президент Германского математического общества, инициатор создания Международного конгресса математиков.

или нет данный объект рассматриваемому множеству. В первом случае множество обозначается в виде заключённого в фигурные скобки списка элементов. Например, $\{1,3,5\}$. Если множество A задаётся свойствами $P_1,\ldots, P_n$ его элементов, то пишут

$$A = \{a \mid P_1,\ldots, P_n\}$$

и говорят, что A есть множество всех элементов, обладающих свойствами $P_1,\ldots, P_n$.

Пусть A, B – множества. Говорят, что A – *подмножество* множества B (или A содержится в B) и пишут $A \subset B$, если каждый элемент множества A является в то же время элементом множества B. Если $A \subset B$ и $B \subset A$, то говорят, что множества A и B равны (или совпадают) и пишут $A = B$. *Пустое* множество $\emptyset$ не содержит элементов и, по определению, является подмножеством любого множества. Если $A \neq \emptyset$, $A \subset B$, и $A \neq B$, то A – *собственное* подмножество в B.

Операции *пересечения*, *объединения* и *разности* множеств A и B определяются следующим образом:

$A \cap B = \{x \mid x \in A \text{ и } x \in B\}$,

$A \cup B = \{x \mid x \in A \text{ или } x \in B\}$,

$A \setminus B = \{x \mid x \in A \text{ и } x \notin B\}$.

Если пересечение $A \cap B$ – пустое множество, то говорят, что A и B *непересекающиеся* множества. Операции пересечения и объединения удовлетворяют следующим тождествам:

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

$A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.

Декартовым произведением множеств A и B называется множество $A \times B = \{(a,b) \mid a \in A, b \in B\}$, где пары (a,b) являются упорядоченными, т.е. $(a_1,b_1) = (a_2,b_2)$ тогда и только тогда, когда $a_1 = a_2$ и $b_1 = b_2$. Аналогично можно определить декартово произведение $A_1 \times \ldots \times A_n$ множеств $A_1,\ldots, A_n$. Если $A_1 = \cdots = A_n = A$, то вместо $A \times \ldots \times A$ (n сомножителей) пишут сокращённо A^n и говорят об n -ой степени множества A. Элементами множества A^n являются всевозможные упорядоченные наборы $(a_1,\ldots,a_n)$ длины n, где $a_i \in A$. Укажем на следующее различие между $A \times B$ и $A \cup B$ для *конечных* множеств, т.е. содержащих конечное число элементов:

$$|A \times B| = |A| \cdot |B|, \quad |A \cup B| = |A| + |B| - |A \cap B|,$$

где $|S|$ – число элементов множества S.

§ 2. Отображения

Понятие отображения – одно из центральных в математике.

Определение. *Отображение* (или *функция*) f – это закон (правило), по которому каждому элементу некоторого множества X ставится в соответствие вполне определённый элемент заданного множества Y (при этом множества X и Y могут совпадать). Это соответствие между элементами $x \in X$ и $y \in Y$ записывается как $y = f(x)$. Пишут также $f: X \longrightarrow Y$ или $X \overset{f}{\to} Y$ и говорят, что отображение f *действует* из X в Y. Множество X называется *областью определения* отображения f, а множество $\{f(x) \mid x \in X\}$ всех элементов $f(x)$ называется *областью значений*, или *образом* отображения f, и обозначается через $Im\ f$ (от $image$ – англ.) или $f(X)$.

Пусть $f: X \to Y$. Множество $f^{-1}(y) = \{x \in X \mid f(x) = y\}$ называется *прообразом* элемента $y \in Y$. Более общо, для $Y_0 \subset Y$ положим

$$f^{-1}(Y_0) = \{x \in X \mid f(x) \in Y_0\} = \bigcup_{y \in Y_0} f^{-1}(y).$$

Если $y \in Y \setminus Im\ f$, то $f^{-1}(y) = \emptyset$. Множество $f^{-1}(Y)$ называется *полным прообразом* множества Y.

Отображение $f: X \longrightarrow Y$ называется: *сюръективным*, или *отображением на*, если $Im\ f = Y$; *инъективным*, если $x_1 \neq x_2 \Longrightarrow f(x_1) \neq f(x_2)$ для любых $x_1, x_2 \in X$. Отображение, являющееся одновременно сюръективным и инъективным, называется *биективным*, или *взаимно однозначным*.

Равенство $f = g$ отображений f и g означает, что их соответствующие области совпадают: $X \overset{f}{\to} Y$, $X \overset{g}{\to} Y$ и $f(x) = g(x)$ для любого $x \in X$. Сопоставление элементу (аргументу) $x \in X$ значения $f(x) \in Y$ принято изображать ограниченной стрелкой: $x \longmapsto f(x)$.

Отображение $f: X \longrightarrow X$ обычно называют *преобразованием* множества X.

Отображение $e_X: X \longrightarrow X$ такое, что $e_X(x) = x$ для любого $x \in X$, называется *единичным*, или *тождественным*.

Произведением (ещё говорят *суперпозицией* или *композицией*) отображений $g: X \to Y$, $f: Y \longrightarrow Z$ называется отображение

$$f \circ g: X \longrightarrow Z,$$

определяемое условием $(f \circ g)(x) = f(g(x)), \quad \forall x \in X$.

Это наглядно изображается треугольной диаграммой на рис. 1. Эту диаграмму называют *коммутативной*, имея в виду, что переход от X к Z может быть осуществлён либо напрямую с использованием $f \circ g$, либо через Y с использованием g, а затем f.

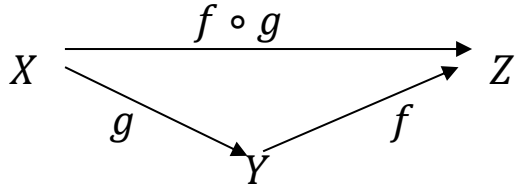

Рис. 1. Коммутативная диаграмма

Далее вместо $f \circ g$ будем просто писать fg.

2.1. ***Теорема.*** *Композиция отображений ассоциативна*: *если* $h: X \longrightarrow Y$, $g: Y \longrightarrow Z$, $f: Z \longrightarrow W$ *– три отображения, то* $f(gh) = (fg)h$.

Доказательство. Для произвольного $x \in X$ имеем

$$\big(f(gh)\big)(x) = f((gh)(x)) = f\Big(g\big(h(x)\big)\Big) = (fg)\big(h(x)\big) = ((fg)h)(x).$$

□[3]

Композиция отображений, вообще говоря, не коммутативна.

Некоторые отображения имеют *обратные*. Пусть $f: X \longrightarrow Y$, $g: Y \longrightarrow X$ – некоторые отображения. Если $fg = e_Y$, то f называется *левым обратным* к g, а g – *правым обратным* к f. Если

$$fg = e_Y, \quad gf = e_X, \tag{1}$$

то g называется *двусторонним обратным* (или просто *обратным*) *отображением для* f или *к* f (а f – обратным отображением для g) и обозначается через f^{-1}. Таким образом, $f(x) = y \Leftrightarrow f^{-1}(y) = x$.

2.2. ***Теорема.*** *Если двустороннее обратное отображение к* f *существует, то оно определено однозначно.*

Доказательство. Допустим, что существует ещё одно отображение $g': Y \longrightarrow X$, для которого $fg' = e_Y$, $g'f = e_X$. Тогда $g' = e_X g' = gfg' = g(fg') = ge_Y = g$. Другими словами, обратное отображение, если оно существует, определено однозначно. □

2.3. ***Лемма.*** *Если* $f: X \longrightarrow Y$, $g: Y \longrightarrow X$ – *любые отображения, для которых* $gf = e_X$, *то* f *инъективно, а* g *сюръективно.*

---

[3] Здесь и далее знак □ обозначает окончание доказательства.

Доказательство. Пусть $x_1, x_2 \in X$ и $f(x_1) = f(x_2)$. Тогда $x_1 = e_X(x_1) = (gf)(x_1) = g(f(x_1)) = g(f(x_2)) = (gf)(x_2) = e_X(x_2) = x_2$.

Значит, f инъективно. Далее, для любого $x \in X$ имеем $x = e_X(x) = (gf)(x) = g(f(x))$. Но это означает, что g сюръективно. □

2.4. ***Теорема.*** *Отображение $f: X \longrightarrow Y$ тогда и только тогда имеет обратное, когда оно взаимно однозначно* (*биективно*).

Доказательство. Предположим вначале, что f обладает обратным $g = f^{-1}$. Из равенств (1) и леммы 2.3 вытекает как сюръективность, так и инъективность f. Значит, f биективно. Обратно, пусть f биективно. Тогда для любого $y \in Y$ найдётся единственный элемент $x \in X$ такой, что $f(x) = y$. Полагая $g(y) = x$, определим отображение $g: Y \longrightarrow X$, обладающее свойствами (1). Значит, $f^{-1} = g$. □

2.5. ***Теорема.*** *Если отображение $f: X \longrightarrow Y$ биективно, то f^{-1} также биективно, причём*

$$(f^{-1})^{-1} = f. \qquad (2)$$

Если отображения $f: X \longrightarrow Y$, $h: Y \longrightarrow X$ биективны, то их композиция $hf-$ также биективное отображение, причём

$$(hf)^{-1} = f^{-1}h^{-1}. \qquad (3)$$

Доказательство. По предыдущей теореме из биективности f вытекает существование f^{-1}, что равносильно биективности f^{-1}. Из условий (1), которые переписываются как $fg = e_Y$, $gf = e_X$, вытекает равенство (2). Далее, по условию и предыдущей теореме существуют отображения $f^{-1}: Y \longrightarrow X$, $h^{-1}: Z \longrightarrow Y$ и их композиция $f^{-1}h^{-1}: Z \longrightarrow X$. Тогда из равенств

$$(hf)\,(f^{-1}h^{-1}) = ((hf)f^{-1})h^{-1} = (h(ff^{-1}))h^{-1} = hh^{-1} = e_Y,$$

$$(f^{-1}h^{-1})\,(hf) = f^{-1}(h^{-1}(hf)) = f^{-1}((h^{-1}h)f) = f^{-1}f = e_X$$

вытекает равенство (3). □

2.6. ***Теорема.*** *Если $X-$ конечное множество и отображение $f: X \longrightarrow X$ инъективно или сюръективно, то оно биективно.*

Доказательство. Если f инъективно, то нужно показать, что f сюръективно, т.е. для каждого $x \in X$ найдётся $x' \in X$ такой, что $f(x') = x$. Положим $f^0(x) = x$; $f^k(x) = f(f^{k-1}(x))$, $k = 1, 2, 3, \ldots$ В силу конечности X в последовательности $f^k(x)$, $k = 0, 1, 2, \ldots$ будут повторения. Пусть $f^m(x) = f^n(x)$, $m > n$. Тогда из этого равенства и инъективности f следует равенство $f^{m-1}(x) = f^{n-1}(x)$. Повторив достаточное число раз сокращение f, получим $f^{m-n}(x) = x$, откуда следует, что $f(x') = x$ при $x' = f^{m-n-1}(x)$.

Обратно, если f сюръективно, то нужно показать, что f инъективно. Если допустить, что $f(x_1) = f(x_2)$ при $x_1 \neq x_2$, то число элементов в $Im\ f$ будет меньше, чем в X, что противоречит предположению о сюръективности f. Значит, f инъективно. □

Понятие мощности. Каждому множеству X поставим в соответствие объект $|X|$, называемый *мощностью* множества X.

Множества X и Y имеют одинаковую мощность тогда и только тогда, когда существует биективное отображение $f: X \longrightarrow Y$. В этом случае пишут $|X| = |Y|$. В частности, пустому множеству $\emptyset$ поставим в соответствие в качестве мощности число 0, а множеству $\{x_1,\ldots,x_n\}$, состоящему из n элементов ($n = 1,2,\ldots$), − число n. Запись $|X| < \infty$ означает, что $X -$ конечное множество. Мощности называют также *кардинальными числами*, или просто *кардиналами.* Мощность множества $\mathbb{N}$ всех натуральных чисел принято обозначать $\aleph_0$ (алеф-нуль), а мощность множества $\mathbb{R}$ всех действительных чисел $-\ \aleph$ (алеф). Множества мощности $\aleph_0$ называются с*чётными.* Мощность $\aleph$ называется также мощностью *континуума*.

§ 3. Бинарные отношения

Для любых двух множеств X и Y любое подмножество $\rho \subset X \times Y$ называется *бинарным отношением* между X и Y (или просто на X, если $Y = X$). Для упорядоченной пары $(x,y) \in \rho$ используют обозначение $x\rho y$ и говорят, что элемент x *находится в отношении* ρ к элементу y. Будем писать (X, ρ), желая подчеркнуть, что на множестве X задано бинарное отношение ρ.

Каждому отображению $f: X \longrightarrow Y$ сопоставляется подмножество $\Gamma(f) = \{(x,y) \mid x \in X, y = f(x)\} \subset X \times Y$, называемое *графиком* отображения. График $\Gamma(f)$, очевидно, является отношением между X и Y, но, заметим, не всякое отношение может служить графиком некоторого отображения. Необходимое и достаточное условие заключается в том, чтобы каждому $x \in X$ соответствовал ровно один элемент $y \in Y$ с $x\rho y$. Задание X, Y и $\Gamma(f)$ однозначно восстанавливает отображение f.

§ 4. Отношение эквивалентности

Определение. Бинарное отношение $\sim$ на X называется отношением *эквивалентности*, если для всех $x, y, z \in X$ выполнены следующие условия:

(1) $x \sim x$ (рефлексивность);

(2) $x \sim y \Longrightarrow y \sim x$ (симметричность);

(3) $x \sim y$ и $y \sim z \Longrightarrow x \sim z$ (транзитивность).

Запись $x \nsim y$ означает отрицание эквивалентности.

Подмножество $[x] = \{y \in X \mid y \sim x\}$ всех элементов $y \in X$, эквивалентных данному x, называется *классом эквивалентности* (иногда *смежным классом*), содержащим элемент x.

Ввиду $x \sim x$ элемент x принадлежит классу $[x]$. Любой элемент $y \in [x]$ называется *представителем* класса $[x]$.

4.1. ***Теорема.*** *Множество классов эквивалентности по отношению $\sim$ является разбиением множества X на непересекающиеся подмножества. Это разбиение называется фактормножеством множества X по отношению эквивалентности $\sim$ и обозначается через $X/\sim$. Обратно, если имеется некоторое разбиение $\rho(X)$ множества X на непересекающиеся подмножества K_x, то K_x будут классами эквивалентности по некоторому отношению эквивалентности $\sim$.*

Доказательство. Доказать самостоятельно (см. [16], с. 48-49).

Другой вид бинарных отношений (отношения частичного порядка) будет рассмотрен в § 28.

§ 5. Факторизация отображений

Сюръективное отображение $\pi: x \mapsto \pi(x) = [x]$ множества X на фактормножество $X/\sim$, при котором каждому элементу x из X ставится в соответствие класс эквивалентности, содержащий этот элемент, называется *естественным* отображением (или *канонической проекцией*) множества X на фактормножество $X/\sim$.

Пусть X, Y – два множества и $f: X \longrightarrow Y$ – отображение. Бинарное отношение ρ_f, определяемое как $x \rho_f x' \Leftrightarrow f(x) = f(x')$ для любых $x, x' \in X$, очевидно, рефлексивно, симметрично и транзитивно, и, следовательно, является отношением эквивалентности на X.

Классы эквивалентности по данному отношению имеют вид: $[x] = \{x' \mid f(x') = f(x)\}$.

Отображение f индуцирует отображение $\varphi: X / \rho_f \longrightarrow Y$, определяемое правилом $\varphi([x]) = f(x)$, или, что то же самое, $\varphi\pi(x) = f(x)$, где $\pi -$ естественное отображение X на фактормножество X / ρ_f. Так как $[x] = [x'] \Leftrightarrow f(x) = f(x')$, то определение φ не зависит от выбора представителя x класса $[x]$, т.е. φ определено корректно. Отображение φ инъективно. Это следует из того, что $\varphi([x]) = \varphi([x']) \Leftrightarrow f(x) = f(x') \Leftrightarrow x = x'$.

Представление f в виде $f = \varphi \circ \pi$ задаёт *факторизацию* (разложение) отображения f в произведение сюръективного отображения π и инъективного отображения φ. Биективность f равносильна сюръективности φ. Если $\psi: {}^{X}/_{\rho_f} \longrightarrow Y -$ ещё одно отображение, для которого выполнено соотношение $\psi \circ \pi = f$, то из $\psi([x]) = \psi(\pi(x)) = f(x) = \varphi([x])$ следует, что на самом деле $\psi = \varphi$. Коммутативная диаграмма на рис. 2 даёт наглядное описание факторизации отображения $f = \varphi\pi$:

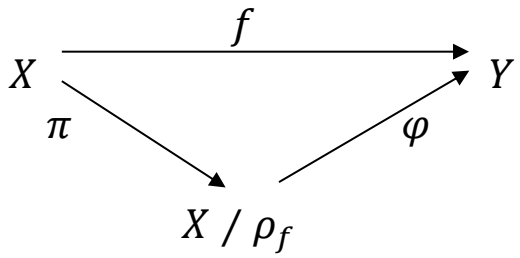

Рис. 2. Факторизация отображения f.

Глава II. Элементы теории чисел

Теория чисел занимается изучением свойств натуральных чисел. В данном разделе рассматриваются некоторые понятия и результаты классической теории чисел на основе арифметических свойств делимости и простых комбинаторных соображений без привлечения специальных понятий геометрии, алгебры и анализа, иррациональных и комплексных чисел.

Замечание. Традиционно в теории чисел неэлементарными считаются доказательства, в которых используются мнимые числа. Геометрические, алгебраические, аналитические, вероятностные методы в теории чисел – предмет более продвинутого изучения. □

Далее используются обозначения:

$\mathbb{N} = \{1, 2, 3, \ldots\}$ – множество натуральных чисел;

$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$ – множество целых чисел.

§ 6. Теория делимости в $\mathbb{Z}$

Число $r \in \mathbb{Z}$ называется *делителем* числа $n \in \mathbb{Z}$, если $n = rs$ для некоторого $s \in \mathbb{Z}$. В свою очередь n называется *кратным* числа r. Факт делимости обозначается как $r \mid n$ (читается: r *делит* n, или n *делится на* r), а отрицание делимости как $r \nmid n$ (читается: r *не делит* n, или n *не делится на* r). Отношение делимости транзитивно: если $a \mid b$ и $b \mid c$, то $a \mid c$. Отметим также: если $c = a + b$, $d \mid a$ и $d \mid c$, то $d \mid b$.

Натуральное число $p > 1$ называется *простым*, если все его натуральные делители исчерпываются числами 1 и p. Натуральное число $q > 1$, не являющееся простым, называется *составным*. Число 1 играет особую роль, его обычно не относят ни к простым, ни к составным. Такое соглашение полезно при формулировке большинства теоретико-числовых результатов.

6.1. ***Теорема*** Евклида [4]. *Множество* $\mathbb{P}$ *простых чисел бесконечно.*

Доказательство (от противного). Допустим, что множество $\mathbb{P}$ конечно и состоит из чисел $p_1, p_2, \ldots, p_k$. Тогда число $q = p_1 p_2 \ldots p_k + 1$ является составным и представимо в виде $q = np_i$ для некоторых $p_i \in \mathbb{P}$ и $n \in \mathbb{N}$, и, следовательно,

$$(n - p_1 \ldots p_{i-1} p_{i+1} \ldots p_k)\, p_i = 1.$$

Последнее равенство, однако, невозможно, так как делителями единицы в $\mathbb{Z}$ являются лишь 1 и -1. Значит, $\mathbb{P}$ не может быть конечным множеством. □

6.2. ***Теорема*** (О делении в $\mathbb{Z}$ с остатком). *Для любых* $a \in \mathbb{Z}$ *и* $b \in \mathbb{N}$ *существуют единственные* $q, r \in \mathbb{Z}$, *такие, что* $a = bq + r$, $0 \le r < b$. *Числа* q и r *называют соответственно частным* и *остатком от деления* a *на* b.

Доказательство. Рассмотрим множество чисел $S = \{a - bs \mid s \in Z, a - bs \ge 0\}$.

Так как $c = a - b(-a^2) \ge 0$, и $c \in S$, то $S \ne \emptyset$ (S не пусто). Пусть $r = a - bq$ − наименьшее число в S. По условию, $r \ge 0$. Если допустить, что $r \ge b$, то $a - b(q + 1) = r - b \in S$, а это противоречит выбору числа r. Значит, $r < b$. Докажем, что числа q и r могут быть выбраны единственным способом. Допустим, что существуют q_1, r_1 такие, что $a = bq_1 + r_1$, $0 \le r_1 < b$. Тогда $0 = b(q - q_1) + (r - r_1)$. Для определённости, считаем, что $r \ge r_1$. Тогда

$$b \mid (r - r_1) \Longrightarrow r = r_1 \text{ и } 0 = b(q - q_1) \Longrightarrow q = q_1. \quad \square$$

Для чисел $a \in \mathbb{Z}$ и $b \in \mathbb{N}$ введём операции div и mod, полагая $a \operatorname{div} b = q$, $a \bmod b = r$, где q и r − соответственно частное и остаток от деления a на b.

Пусть числа $a, b \in \mathbb{Z}$ не равны нулю одновременно. Наибольшее $d \in \mathbb{Z}$ такое, что $d \mid a$ и $d \mid b$, называется *наибольшим общим делите-*

---

[4] ***Евклид или Эвклид*** − выдающийся древнегреческий математик, автор первого из дошедших до нашего времени теоретических трактатов по математике. Биографические сведения о нем весьма скудны. Его научная деятельность протекала в Александрии в III в. до н. э.

лем чисел a и b и обозначается символом (a, b) (или как НОД (a, b), если возникает коллизия с обозначениями векторов).

Алгоритм Евклида вычисления $d =$ НОД (a, b) основан на использовании следующих свойств:

1) $(a,0) = |\, a \,|$;

2) $(a,b) = (b,a)$;

3) $a = bq + r \Longrightarrow (a,b) = (r,b)$

и осуществляется по схеме:

$a := abs(a);\ b := abs(b);$
$while\ (a\ > 0)\&(b\ > 0)\ do$
$\{if\ a > b\ then\ a \coloneqq a \bmod b\ else\ b := b \bmod a\};$
НОД $\coloneqq a + b.$

Этот алгоритм затрачивает $O(log_2(|\, a \,| + |\, b \,|))$ времени (по числу арифметических операций). Анализ этого и других алгоритмов вычисления НОД см. у Д. Кнута [5] ([14], Т. 2).

Если $(a,b) = 1$, то числа a и b называют *взаимно простыми*.

6.3. ***Теорема.*** *Пусть* $a, b \in \mathbb{Z}$, $ab \neq 0$. *Тогда существуют* $u, v \in \mathbb{Z}$ *такие, что* $(a,b) = au + bv$ для некоторых $u, v \in \mathbb{Z}$; *в частности, если* a *и* b *взаимно просты, то* $au + bv = 1$.

Доказательство. Положим $J = \{au + bv \mid u, v \in \mathbb{Z}\}$. Выберем в J наименьшее положительное число $d = au_0 + bv_0$. Запишем число a в виде $a = dq + r$, где $0 \leq r < d$. Имеем $r = a - dq = a(1 - u_0 q) - b(v_0 q) \in J$. Поскольку $r < d$, то $r = 0$ (по условию выбора d), и, следовательно, $d \mid a$. Аналогично получаем, что $d \mid b$. Пусть d_1 – любой общий делитель чисел a и b. Тогда $d_1 \mid a,\ d_1 \mid b \Longrightarrow d_1 \mid (au_0 +$

---

[5] ***Дональд Кнут*** **(**род. 10.01.1938**)** – выдающийся математик и программист. Его работы относятся к алгебре, теории чисел и комбинаторике. В начале 1960-х годов увлекся программированием. Эти работы принесли ему мировую известность. Уникальное явление – серия его книг под названием “Искусство программирования для ЭВМ”. Еще одно выдающееся достижение – издательские системы TEX и METAFONT, позволившие создавать математические тексты на высоком полиграфическом уровне.

$bv_0) \Longrightarrow d_1 \mid d$, откуда следует, что число d обладает свойствами НОД (a, b). □

Наибольший общий делитель чисел $a_1, a_2, \ldots, a_n$ может быть вычислен по схеме:

НОД $(a_1, a_2, \ldots, a_n)$ = НОД (НОД $(a_1, a_2), a_3, \ldots, a_n)$.

6.4. ***Лемма.*** *Пусть $a, b \in \mathbb{Z}$, p – простое число. Тогда, если $p \mid ab$, то либо $p \mid a$, либо $p \mid b$ (либо и то, и другое).*

Доказательство. Допустим, что $p \nmid a$. Тогда $(a,b) = 1$ и $au + pv = 1$ для некоторых $u, v \in \mathbb{Z}$. Умножая обе части последнего равенства на b, получим $aub + pvb = b$.

Так как $p \mid (aub + pvb)$, то $p \mid b$. □

6.5. ***Теорема*** (Основная теорема арифметики). *Всякое натуральное число $n > 1$ разлагается в произведение простых чисел, причем единственным способом, если не учитывать порядок сомножителей.*

Доказательство. Факт представления числа n в виде произведения простых сомножителей очевиден. Докажем единственность такого представления. Пусть $p_1 p_2 \ldots p_s = q_1 q_2 \ldots q_t$ – два разложения числа n на простые сомножители p_i, q_j. Тогда из предыдущей леммы следует, что p_1 делит одно из чисел $q_1, q_2, \ldots, q_t$. Пусть, для определённости $p_1 \mid q_1$. Поскольку q_1 – простое число, то $q_1 = p_1$. Переходя к равенству $p_2 \ldots p_s = q_2 \ldots q_t$, получаем аналогично, что $q_2 = p_2$, и так далее. □

В разложении числа на простые множители некоторые из них могут повторяться. Собирая одинаковые множители, получим $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, где $p_1 < p_2 < \cdots < p_k$ – различные простые числа, $\alpha_i \in \mathbb{N}$, $i = 1,\ldots,k$. Такое представление называется *каноническим разложением* числа на простые множители.

Пример. $1176 = 2^3 3^1 7^2$.

Замечание. Доказать теорему 6.5, опираясь только на мультипликативные свойства (т.е. свойства умножения и деления) целых чисел невозможно. Необходимо привлечение аддитивных свойств (т.е. свойств сложения). Это можно проиллюстрировать на примере множества $S = \{2,4,6,\ldots\}$ чётных чисел. Оно замкнуто относительно умножения: $a, b \in S \Longrightarrow ab \in S$. Всякое число $n \in S$ представимо в виде произведения чисел $q_1, \ldots, q_t$, каждое из которых неразложимо в S. Такие числа q_i назовём S- *простыми*. К ним относятся 2,6,10, 16,…, т.е. числа вида $2(2s + 1)$. Очевидно, что первая часть Основной теоремы выполняется. Однако, вторая часть (об однозначности

разложения) для S неверна, поскольку некоторые числа из S имеют более одного разложения в произведение S-простых чисел. Например, $180 = 6 \cdot 30 = 18 \cdot 10$, где ни одно из чисел 6,30,18,10 не разлагается в произведение только чётных чисел, т.е. эти числа являются S-простыми.

Такими же свойствами обладают множества $S = \{3k + 1 \mid k = 1,2,3,\ldots\}$, и др. (См. Радемахер и Теплиц [37], С. 249. Прим. 39.) □

Наименьшее общее кратное чисел $a, b \in \mathbb{Z}$, $ab \neq 0$, определяется как наименьшее число $k \in \mathbb{N}$ такое, что $a \mid k$ и $b \mid k$, и обозначается символом $[a,b]$ (или НОК $[a,b]$).

6.6. ***Теорема.*** *Пусть* $a, b \in \mathbb{N}$. *Тогда* $(a,b)[a, b] = ab$.

Доказательство. Пусть $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ и $b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$ – канонические разложения чисел a и b, $\gamma_i = min\{\alpha_i,\beta_i\}$, $\delta_i = max\{\alpha_i,\beta_i\}$, $i = 1,\ldots,k$. Тогда

$$(a,b) = \prod_{i=1}^{k} p_i^{\gamma_i},\ \ [a,b] = \prod_{i=1}^{k} p_i^{\delta_i} \implies (a,b)[a,b] = \prod_{i=1}^{k} p_i^{\gamma_i+\delta_i} = \prod_{i=1}^{k} p_i^{\alpha_i+\beta_i} = ab. \ \square$$

§ 7. Сравнения по модулю n

Пусть $n \in \mathbb{N}$. Числа $a, b \in \mathbb{Z}$ называются *сравнимыми по модулю* n, если при делении на n они дают одинаковые остатки. При этом пишут

$$a \equiv b \ (mod\ n). \qquad (1)$$

Запись $a \not\equiv b \ (mod\ n)$ означает, что для чисел a и b сравнение (1) не имеет места.

Отметим следующие свойства сравнений:

$a \equiv b \ (mod\ n) \Leftrightarrow n \mid a - b$; (2)

$a \equiv a \ (mod\ n)$; (3)

$a \equiv b \ (mod\ n) \Rightarrow b \equiv a \ (mod\ n)$ (4)

$a \equiv b \ (mod\ n)$ и $b \equiv c \ (mod\ n) \Rightarrow a \equiv c \ (mod\ n)$ (5)

(свойства $(2) - (4)$ означают, что отношение сравнимости рефлексивно, симметрично и транзитивно, т.е. является отношением эквивалентности на множестве $\mathbb{Z}$);

$a \equiv b \ (mod\ n)$ и $c \equiv d \ (mod\ n) \Rightarrow a \circ c \equiv b \circ d \ (mod\ n)$, (6)

где символ $\circ$ может быть заменён на любой из символов: $+$ (сложение), $-$ (вычитание) или $\cdot$ (умножение), но на один и тот же в обеих частях сравнения, так что сравнения можно почленно складывать, вычитать и перемножать);

$a \equiv b\ (mod\ n) \Longrightarrow a^m \equiv b^m\ (mod\ n), m \in \mathbb{N};$ (7)

если $f(x)$ – многочлен с целочисленными коэффициентами, то (8)

$a \equiv b\ (mod\ n) \Longrightarrow f(a) \equiv f(b)\ (mod\ n);$

$a \equiv b\ (mod\ mn) \Longrightarrow a \equiv b\ (mod\ n);$ (9)

если $d \mid a, d \mid b, a \equiv a_1 d, b = b_1 d, (d, n) = 1$, то (10)

$a \equiv b\ (mod\ n) \Longrightarrow\ a_1 \equiv b_1 (mod\ n),$

т.е. обе части сравнения можно разделить на любой общий делитель при условии, что этот делитель взаимно прост с модулем;

$ad \equiv bd\ (mod\ nd) \Longrightarrow b \equiv a\ (mod\ n),$ (11)

т.е. обе части сравнения и модуль можно разделить на любой их общий делитель;

$a \equiv b\ (mod\ m)$ и $a \equiv b\ (mod\ n) \Longrightarrow a \equiv b\ (mod\ k)$, где (12)

$k =$ НОК $[m, n]$;

$d|a, d|n,$ и $a \equiv b\ (mod\ n) \Longrightarrow d|b;$ (13)

$a \equiv b\ (mod\ n) \Longrightarrow$ НОД $(a,n) =$ НОД (b,n). (14)

§ 8. Полная система вычетов по модулю n

Пусть $n \in \mathbb{N}$ – фиксированное число. Для произвольного $a \in \mathbb{Z}$ определим класс чисел K_a, включая в него все числа, сравнимые с a по модулю n:

$$K_a = \{x \in \mathbb{Z} \mid x \equiv a\ (mod\ n)\}.$$

Нетрудно установить, что $K_a = K_b \Leftrightarrow a \equiv b\ (\mathrm{mod}\, n)$, $K_a \cap K_b = \emptyset \Leftrightarrow a \not\equiv b\ (\mathrm{mod}\, n)$. Другими словами, классы $K_0, K_1, \ldots, K_{n-1}$ попарно не пересекаются, и любой класс K_a совпадает с одним из них. Следовательно, имеет место следующее разбиение $\mathbb{Z}$ на непересекающиеся классы: $\mathbb{Z} = K_0 \cup K_1 \cup \ldots \cup K_{n-1}$. Каждое число из класса K_a называется *вычетом по модулю* n по отношению ко всем числам того же класса. Взяв по одному вычету из каждого класса, получим систему вычетов, которую называют *полной системой вычетов по модулю* n. В частности, множество $\mathbb{N}_n = \{0,1,\ldots, n-1\}$ образует полную систему *наименьших неотрицательных вычетов по модулю* n. В полной системе вычетов по модулю n любые два вычета попарно несравнимы по модулю n. Если a и b принадлежат одному и тому же классу вычетов по модулю n, то НОД (a, n) = НОД (b, n).

8.1. ***Теорема***. *Пусть* $a,\ b \in \mathbb{Z}$ *и* $n \in \mathbb{N}$ – *любые числа*, НОД $(a, n) = 1$. *Тогда, если* x *пробегает полную систему вычетов по моду-*

лю n, то $ax + b$ также пробегает полную систему вычетов по модулю n.

Доказательство. Если $ax_1 + b \equiv ax_2 + b \ (mod\ n)$, то из свойств сравнений следует, что $x_1 \equiv x_2 \ (mod\ n)$. Поэтому, если $x_1 \not\equiv x_2 \ (mod\ n)$, то $ax_1 + b \not\equiv ax_2 + b \ (\mathrm{mod}\ n)$. □

§ 9. Приведённая система вычетов по модулю n

В разбиении $\mathbb{Z}$ на классы $K_0, K_1, \ldots, K_{n-1}$ удалим те классы K_a, для которых НОД $(a, n) > 1$. Из оставшихся классов (для них НОД $(a, n) = 1$) возьмём по одному вычету. В результате получим систему вычетов, которую называют *приведённой системой вычетов по модулю n*. Как и для полной системы вычетов, выбор приведённой системы вычетов не однозначен.

9.1. ***Теорема***. *Пусть* НОД $(a, n) = 1$. *Тогда, если x пробегает приведённую систему вычетов по модулю n, то ax также пробегает приведённую систему вычетов по модулю n.*

Доказательство. Учитывая, что НОД $(ax, n) = 1$, имеем $ax_1 \equiv ax_2 \ (mod\ n) \Longrightarrow x_1 \equiv x_2 \ (mod\ n)$. Поэтому $x_1 \not\equiv x_2 \ (mod\ n) \Longrightarrow ax_1 \not\equiv ax_2 \ (mod\ n)$. □

§ 10. Функция Эйлера. Теоремы Эйлера, Ферма и др.

Функция Эйлера [6] $\varphi(n)$ определяется как количество чисел среди $1, 2, \ldots, n$, взаимно простых с n. Любая приведённая система вычетов по модулю n содержит $\varphi(n)$ вычетов**.** Первые 13 значений $\varphi(n)$:

n	1	2	3	4	5	6	7	8	9	10	11	12	13
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12

[6] ***Леонард Эйлер*** (15.04.1707 − 7.09.1783) − швейцарский, немецкий и российский математик и механик, внёсший фундаментальный вклад в развитие этих наук, а также ряда прикладных наук. Академик Петербургской и других академий наук. Полжизни провёл в России. Первые русские академики математики и астрономы − были его учениками.

Далее будет установлена формула для этой функции.

10.1. ***Теорема.*** *Пусть* $p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$ *– каноническое разложение натурального числа* n. *Тогда*

$$\varphi(n) = p_1^{\alpha_1-1}p_2^{\alpha_2-1}\dots p_k^{\alpha_k-1}(p_1-1)(p_2-1)\dots(p_k-1).$$

Утверждение теоремы вытекает из приводимых ниже лемм 10.2, 10.3.

10.2. ***Лемма.*** *Пусть* p *– простое число,* $\alpha \in \mathbb{N}$.

Тогда $\varphi(n) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$.

Доказательство. Среди $0,1,\dots,p^\alpha - 1$ имеется в точности $p^{\alpha-1}$ чисел, кратных p. Остальные числа взаимно просты с p и, следовательно, с p^α. □

10.3. ***Лемма***. *Если* НОД $(a,b) = 1$, *то* $\varphi(ab) = \varphi(a)\varphi(b)$.

Доказательство. Для $ab = 1$ утверждение леммы очевидно. Пусть $ab > 1$. Рассмотрим множество $\mathbb{N}_{ab} = \{0,1, \dots, ab-1\}$. Его можно представить как объединение $S = S_0 \cup S_1 \cup \dots \cup S_{b-1}$ попарно не пересекающихся подмножеств

$$S_r = \{r, b+r, 2b+r, \dots, (a-1)b+r\},\ r = 0, 1, \dots, b-1.$$

Удалим из S подмножества S_r, для которых НОД $(r,b) > 1$. В результате в S останется $\varphi(b)$ подмножеств S_r. Каждое из них содержит только числа из $\mathbb{N}_{ab}$, взаимно простые с b. Далее, любое из подмножеств S_r представляет собой полную систему вычетов по модулю a. В каждом из них содержится в точности $\varphi(a)$ чисел, взаимно простых с a. Эти числа оставим, а остальные удалим из S. В результате в S останутся те и только те числа из $\mathbb{N}_{ab}$, которые взаимно просты как с числом a, так и с числом b, и, следовательно, с ab. Всего же во множестве S, после всех удалений, останется $\varphi(a)\varphi(b)$ чисел. С другой стороны, в исходном множестве $S = \mathbb{N}_{ab}$ содержится $\varphi(ab)$ чисел, взаимно простых с ab. Значит, $\varphi(ab) = \varphi(a)\varphi(b)$. □

10.4. ***Теорема*** Эйлера.

$$\text{НОД}\ (a, n) = 1 \Longrightarrow\ a^{\varphi(n)} \equiv 1 (mod\ n). \qquad (1)$$

Доказательство. Пусть числа $r_1, r_2, \dots, r_k$, где $k = \varphi(n)$, образуют приведённую систему вычетов по модулю n. Тогда согласно теореме 8.1 числа $ar_1, ar_2, \dots, ar_k$ также образуют приведённую систему вычетов по модулю n. Поэтому всякое число ar_j сравнимо по модулю n с некоторым числом r_i, и обратно. Следовательно, имеет место система сравнений

$$ar_1 \equiv r_{i_1} (mod\ n),$$

$ar_2 \equiv r_{i_2}(mod\ n)$,

…

$ar_k \equiv r_{i_k}(mod\ n)$,

где $i_1, i_2, \ldots, i_k$ − некоторая перестановка индексов $1, 2, \ldots, k$.

Перемножая левые и правые части этих сравнений, получаем

$$(ar_1)(ar_2)\ldots(ar_k) = a^k r_1 r_2 \ldots r_k \equiv r_1 r_2 \ldots r_k (mod\ n).$$

Так как НОД $(r_1 r_2 \ldots r_k, n) = 1$, то левую и правую части последнего сравнения можно сократить на $r_1 r_2 \ldots r_k$.

В результате получим (1). □

10.5. ***Следствие*** (Малая теорема Ферма [7]). *Если p − простое число и $p \nmid a$*, то $a^{p-1} \equiv 1(mod\ p)$.

Доказательство. Достаточно учесть, что $\varphi(p) = p - 1$, и применить теорему 10.4. □

10.6. ***Следствие.*** *Если p − простое число, то*

$$a^{p^m} \equiv a\ (mod\ p)\ \textit{для любых}\ a \in \mathbb{Z}, m \in \mathbb{N}.$$

Доказательство. Если $p \nmid a$, то $a^{p-1} \equiv 1(mod\ p) \Longrightarrow a^p \equiv a\ (mod\ p)$. Если $p \mid a$, то последнее сравнение заведомо выполняется. Но тогда

$$a^{p^m} \equiv a^{p^m - 1} \equiv \cdots \equiv a^{p^2} \equiv a^p \equiv a\ (mod\ p).$$ □

Теорема Эйлера допускает следующее обобщение:

10.7. ***Теорема*** Кармайкла [8]. *Для любых взаимно простых чисел $a \in \mathbb{Z}$ и $n \in \mathbb{N}$*

$$a^{\lambda(n)} \equiv\ 1\ (mod\ n), \qquad (2)$$

где $\lambda(n)$ − функция Кармайкла, определяемая следующим образом:

$\lambda(2) = 1, \lambda(4) = 2;\ \lambda(2^\alpha) = 2^{\alpha-2}$, *если* $\alpha \geq 3$;

$\lambda(p^\alpha) = \varphi(p^\alpha) = p^\alpha(p-1)$, *если p − нечетное простое число*;

---

[7] ***Пьер Ферма*** (17.08.1601 − 12.01.1665) − французский математик-самоучка, один из создателей аналитической геометрии, математического анализа, теории вероятностей и теории чисел. Наиболее известен формулировкой Великой теоремы Ферма,

[8] ***Роберт Дэниэл Кармайкл*** (1.03.1879 − 2.05.1967) − американский математик. Известен своими исследованиями составных чисел, похожих на простые числа, как в Малой теореме Ферма.

$\lambda(n) = \text{НОК}\,[\lambda(p_1^{\alpha_1}),\ldots,\lambda(p_k^{\alpha_k})]$, *если* $p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$ *– каноническое разложение числа* n.

Доказательство теоремы см. в § 23. □

Замечание. Для чисел n вида 2, 4, p^α или $2p^\alpha$, где p – простое число, $\alpha \in \mathbb{N}$, имеет место равенство $\lambda(n) = \varphi(n)$. Во всех остальных случаях $\lambda(n)$ – собственный делитель числа $\varphi(n)$ и для них соотношение (2) уточняет теорему Эйлера**.** □

Следующее утверждение является обращением теоремы Ферма:

10.8. ***Теорема*** Люка [9] (1876). *Натуральное число* n *является простым тогда и только тогда, когда существует число* b *такое, что* $b^{n-1} \equiv 1\ (mod\ n)$, *но* $b^{(n-1)/q} \not\equiv 1\ (mod\ n)$ *для любого простого делителя* q *числа* $n-1$.

Доказательство см. в § 49. □

Из Малой теоремы Ферма следует, что если НОД $(b,n) = 1$ и $b^{n-1} \not\equiv 1(mod\ n)$, то n – заведомо составное число. Вместе с тем существуют составные числа n, для которых $b^{n-1} \equiv 1\ (mod\ n)$.

Такие (составные) числа называют b*-псевдопростыми*.

10.9. ***Теорема*** Чиполлы [10] (1904)**.** *Существует бесконечно много* b*-псевдопростых составных чисел*.

Доказательство. Положим $n = \frac{b^{2p}-1}{b^2-1}$, где p – нечетное простое число, взаимно простое с b^2-1, и отметим, что n – целое составное число, так как $n = \frac{b^p-1}{b-1}\cdot\frac{b^p+1}{b+1}$, а

$$\frac{b^p-1}{b-1} = b^{p-1} + b^{p-2} + \cdots + b^1 + 1,$$

$$\frac{b^p+1}{b+1} = (b^{p-1} - b^{p-2}) + (b^{p-3} - b^{p-4}) + \cdots + (b^2 - b^1) + 1$$

– целые числа. Имеем

$$n - 1 = \frac{b^{2p}-1}{b^2-1} - 1 = \frac{b^{2p}-b^2}{b^2-1} = 2cd,$$

---

[9] ***Франсуа Эдуард Анаотоль Люка*** (4.04.1842 – 8.10.1891) – французский математик, профессор. Важнейшие его работы относятся к теории чисел.

[10] ***Микеле Чиполла*** (28.10.1880 – 7.09.1947) — итальянский математик, специализировавшийся в области теории чисел.

где

$$c = \frac{b^2(b^{p-1}+1)}{2}, d = \frac{b^{p-1}-1}{b^2-1}.$$

Допустим, что НОД $(b,\ p) = 1$. Тогда $b^{p-1} \equiv 1(mod\ p)$. Поскольку $p \nmid (b^2-1)$, то $p \mid (b^{2p}-1)$ и $p|d$. Если же НОД $(b,\ p) \neq 1$, то $p|b$ и $p|c$. В любом случае $2p|n-1$, и $n\,|(b^{2p}-1) \Longrightarrow b^{2p} \equiv 1(mod\ n) \Longrightarrow b^{n-1} = b^{2p\frac{n-1}{2p}} \equiv 1(mod\ n)$. □

Пример. Для $b = 2$ и $p = 5$ получим $n = 341 = 11 \cdot 31$ и $2^{340} \equiv 1(\mathrm{mod}\ 341)$.

Замечание. Число n может быть b-псевдопростым для некоторого b, но не быть таковым при другом b. Однако существуют составные числа, которые являются псевдопростыми при любом b, взаимно простым с n. Такие числа называют *числами Кармайкла*, или *абсолютно псевдопростыми*. Известно (1994), что множество чисел Кармайкла бесконечно. Первое такое число равно $561 = 3 \cdot 11 \cdot 17$. □

Приведём одно утверждение, используемое в криптографии (в алгоритме RSA):

10.10. ***Теорема.*** *Пусть $p,\ q$ – различные простые числа, $n = pq$, $e \in \mathbb{N}$ – любое число, взаимно простое с $\varphi(n) = (p-1)(\,q-1)$.*

Тогда отображение

$$f\colon x \longrightarrow x^e\ mod\ n$$

является взаимно однозначным на множестве $\mathbb{N}_n = \{0, 1, \dots, n-1\}$, причем обратным к нему является отображение

$$f^{-1}\colon x \longmapsto x^t\ mod\ n,$$

где $t = e^{\varphi(\varphi(n))-1}\ mod\ \varphi(n)$ – число, удовлетворяющее сравнению $et \equiv 1\ (mod\ \varphi(n))$.

Доказательство. Достаточно показать, что $x^{et}\ mod\ n = x$ для любого $x \in \mathbb{N}_n$, рассматривая случаи: 1) $p \nmid x$ и $q \nmid x$; 2) $p \mid x$, т.е. $x = bp$ для некоторого b, взаимно простого с q; 3) $q \mid x$. (Третий случай аналогичен предыдущему, поэтому не рассматривается.) Отметим, что $et \equiv 1 + a\varphi(n)$ для некоторого $a \in \mathbb{N}$.

В первом случае имеем:

$$x^{et} = x^{1+a\varphi(n)} = x \cdot (x^a)^{\varphi(n)} \equiv x\ (mod\ n),$$

а во втором случае имеем:

$$x^{et} = (bp)^{1+a\varphi(n)} = bp\left((bp)^{a(p-1)}\right)^{q-1} = bp(1 + cq) = x + bcn \equiv x\ (mod\ n),$$

где c – некоторое целое. □

§ 11. Мультипликативно обратные элементы по модулю n

Число x называется *мультипликативным обратным к a по модулю n*, если $ax \equiv 1\ (mod\ n)$. Очевидно, что x существует тогда и только тогда, когда НОД $(a, n) = 1$. В этом случае в качестве x можно взять любое число, сравнимое с $a^{\varphi(n)-1}$ по модулю n, что непосредственно вытекает из теоремы Эйлера. В интервале $[1, n-1]$ содержится в точности одно такое x (действительно, $ax_1 \equiv ax_2(mod\ n) \Longrightarrow x_1 \equiv x_2(mod\ n)$); соответствующее x обозначим через $a^{-1} mod\ n$.

Другой способ вычисления $a^{-1} mod\ n$ (без привлечения функции $\varphi(n)$) основан на использовании расширенного алгоритма Евклида, в котором наряду с вычислением НОД (a, n) также вычисляются числа x и y такие, что $ax + ny = d$. Следующий алгоритм возвращает значение $d = (a, n)$ и значение x, удовлетворяющее сравнению $ax \equiv d\ (mod\ n)$ (поэтому, если $d = 1$, то $x = a^{-1}\ (mod\ n)$):

$(d, m, y, x) := (a, n, 0, 1)$;
$r := m\ mod\ d$;
while $r > 0$ ***do*** {
  $q := m\ div\ d$;
  $z := (y + (n - ((q \cdot x)\ mod\ n)))\ mod\ n$;
  $(m, d) := (d, r)$; $(y, x) := (x, z)$;
  $r := m\ mod\ d$
}.

§ 12. Китайская теорема об остатках

12.1. ***Теорема.*** *Пусть $m_1, \ldots, m_k \in \mathbb{N}$ – любые попарно взаимно простые числа; b, $a_1, \ldots, a_k \in \mathbb{Z}$ – любые числа; $M = m_1 \ldots m_k$. Тогда в интервале $[b,\ b + M - 1]$ содержится число x, удовлетворяющее сравнениям*

$$\begin{cases} x \equiv a_1(mod\ m_1), \\ \ldots \\ x \equiv a_k(mod\ m_k), \end{cases} \qquad (1)$$

причём единственное.

Доказательство. Построим искомое x. Положим

$$M_s = \frac{M}{m_s} = m_1 \dots m_{s-1} m_{s+1} \dots m_k, \quad N_s = M_s^{-1} \, mod \, m_s$$

(число N_s существует, поскольку НОД $(M_s, m_s) = 1$), $s = 1,\dots,k$. Далее полагаем $x_1 = a_1 N_1 M_1 + a_2 N_2 M_2 + \dots + a_k N_k M_k$. Нетрудно проверить, что число x_1 удовлетворяет системе сравнений (1), поскольку $N_i M_i \equiv 1 (mod \, m_i)$ и $N_j M_j \equiv 0 \, (mod \, m_i)$ при $0 \le j \le k$, $j \ne i$. Если $x_1 \equiv x_2 (mod \, M)$ и x_1 удовлетворяет (1), то и x_2 удовлетворяет (1). Отсюда следует, что любое число $x = x_1 + cM$, где $c \in \mathbb{Z}$, удовлетворяет (1). Одно из таких чисел попадает в интервал $[b, \, b + M - 1]$. Допустим на минутку, что в этом интервале содержатся два числа: x и y, удовлетворяющие (1). Пусть, для определённости, $x > y$. Поскольку число $z = x - y$ удовлетворяет системе сравнений

$$\begin{cases} z \equiv 0 \, (\mathrm{mod} \, m_1), \\ \dots \\ z \equiv 0 \, (\mathrm{mod} \, m_k), \end{cases}$$

то z делится без остатка на $m_1,\dots, m_k$, и, следовательно, на M. Так как $z < M$, то $z = 0$ и $x = y$. Значит, в указанном интервале содержится в точности одно число, удовлетворяющее системе сравнений (1). □

§ 13. Функция Мёбиуса. Формула обращения Мёбиуса

Функция *Мёбиуса* [11] $\mu(n)$ натурального аргумента n определяется следующим образом:

$\mu(1) = 1$,

$\mu(n) = (-1)^k$, если n – произведение k различных простых чисел,

$\mu(n) = 0$, если n делится на квадрат простого числа.

---

[11] ***Август Фердинанд Мёбиус*** (17.11.1790 – 26.09.1868) – немецкий математик, механик и астроном-теоретик. В 1858 году установил (почти одновременно с И. Б. Листингом) существование односторонних поверхностей и в связи с этим стал знаменит как изобретатель листа Мёбиуса. В теории чисел его именем названы ряд Мёбиуса, функция Мёбиуса $\mu(n)$ и формулы обращения Мёбиуса.

Первые 13 значений $\mu(n)$:

n	1	2	3	4	5	6	7	8	9	10	11	12	13
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0	-1

Далее символ $\sum_{d\,|\,n}$ означает, что суммирование распространяется на все натуральные делители d числа n.

13.1. ***Лемма.***

$$\sum_{d\,|\,n}\mu(d)=\begin{cases}1, \text{если } n=1,\\ 0, \text{если } n>1.\end{cases}$$

Доказательство. Для $n=1$ утверждение очевидно. Пусть $n>1$ и $p_1^{\alpha_1}\dots p_s^{\alpha_s}$ – каноническое разложение числа n. Тогда, учитывая, что делители n имеют вид $p_1^{\beta_1}\dots p_s^{\beta_s}$, где $\beta_i=0,1,\dots,\alpha_i;\ 1\le i\le s$, получаем

$$\sum_{\beta_1=0}^{\alpha_1}\dots\sum_{\beta_s=0}^{\alpha_s}\mu\left(p_1^{\beta_1}\dots p_s^{\beta_s}\right)=\sum_{\beta_1=0}^{\alpha_1}\dots\sum_{\beta_s=0}^{\alpha_s}\mu\left(p_1^{\beta_1}\right)\dots\mu\left(p_s^{\beta_s}\right)=$$

$$=\sum_{\beta_1=0}^{\alpha_1}\mu\left(p_1^{\beta_1}\right)\dots\sum_{\beta_s=0}^{\alpha_s}\mu\left(p_s^{\beta_s}\right)=0,$$

поскольку при $\alpha>0$

$$\sum_{\beta=0}^{\alpha}\mu\left(p^{\beta}\right)=\mu(1)+\mu(p)+\sum_{\beta=2}^{\alpha}\mu\left(p^{\beta}\right)=1+(-1)+0=0.\ \square$$

13.2. ***Теорема*** (Аддитивная формула обращения Мёбиуса). *Пусть $f(n)$ и $g(n)$ – функции натурального аргумента n. Тогда, если*

$$f(n)=\sum_{d\,|\,n}g(d)\ \text{для всех}\ n\in\mathbb{N},$$

то

$$g(n)=\sum_{d\,|\,n}\mu(d)\,f\left(\frac{n}{d}\right)\ \text{для всех}\ n\in\mathbb{N}.$$

Доказательство. Имеем

$$f\left(\frac{n}{d}\right)=\sum_{d'\,|\,\frac{n}{d}}g(d'),$$

$$\sum_{d\,|\,n}\mu(d)f\left(\frac{n}{d}\right)=\sum_{d\,|\,n}\mu(d)\sum_{d'|\frac{n}{d}}g(d')=\sum_{d\,|\,n}\sum_{d'|\frac{n}{d}}\mu(d)g(d').$$

Пусть $n=dd'n_1$. Тогда d при фиксированном d' пробегает все значения делителей числа $\frac{n}{d'}$. Это означает, что символы суммирования в последней двойной сумме можно поменять местами, т.е.

$$\sum_{d\,|\,n}\sum_{d'|\frac{n}{d}}\mu(d)g(d')=\sum_{d'|\,n}\sum_{d\,|\,\frac{n}{d'}}\mu(d)g(d').$$

Теперь, учитывая, что

$$\sum_{d\,|\,\frac{n}{d'}}\mu(d)=0\ \text{ для } d'\neq n,$$

получаем

$$\sum_{d'|\,n}\sum_{d\,|\,\frac{n}{d'}}\mu(d)g(d')\ =\sum_{d'|\,n}g(d')\sum_{d\,|\,\frac{n}{d'}}\mu(d)=g(n).\ \square$$

Имеется другая форма доказанной теоремы:

13.3. ***Теорема*** (Мультипликативная формула обращения Мёбиуса). *Пусть*

$$f(n)=\prod_{d\,|\,n}g(d)\ \text{ для всех } n\in\mathbb{N},$$

где символ $\prod_{d\,|\,n}$ *обозначает произведение, распространенное на все натуральные делители* d *числа* n. *Тогда*

$$g(n)=\prod_{d\,|\,n}f\left(\frac{n}{d}\right)^{\mu(d)}\ \text{ для всех } n\in\mathbb{N}.$$

Доказательство:

$$f\ \left(\frac{n}{d}\right)=\prod_{d'|\frac{n}{d}}g(d'),$$

$$\prod_{d\,|\,n}f\left(\frac{n}{d}\right)^{\mu(d)}=\prod_{d\,|\,n}\prod_{d'|\frac{n}{d}}g(d')^{\mu(d)}=\prod_{d'\,|\,n}\prod_{d\,|\,\frac{n}{d'}}g(d')^{\mu(d)}$$

$$=\prod_{d'|\,n}g(d')^{\sum_{d\,|\,\frac{n}{d'}}\mu(d)}=\ g(n)\ .\ \square$$

Обращение Мёбиуса может быть использовано, например, при решении следующей задачи.

Задача о числе циклических кольцевых последовательностей.

Будем рассматривать r-ичные последовательности $a_0a_1 \dots a_{n-1}$ длины n с компонентами $a_i \in R = \{0.1, \dots, r-1\}$, $r \geq 2$. Последовательности $a_0a_1 \dots a_{n-1}$ и $b_0b_1 \dots b_{n-1}$ называются *эквивалентными*, если из последовательности $b_0b_1 \dots b_{n-1}$ путём её циклического сдвига можно получить последовательность $a_0a_1 \dots a_{n-1}$. Линейные последовательности

$$a_0a_1 \dots a_{n-1},\ a_1a_2 \dots a_{n-1}a_0,\ \dots,\ a_{n-1}a_0a_1 \dots a_{n-2}$$

определяют одну и туже кольцевую последовательность $a_0a_1 \dots a_{n-1}$. Требуется установить, сколько существует попарно неэквивалентных последовательностей длины n с компонентами из R.

Пример. Среди двоичных последовательностей длины 4 последовательности

$$0000 \quad 0001 \quad 0011 \quad 0101 \quad 0111 \quad 1111$$

образуют максимальное множество из 6 попарно неэквивалентных последовательностей**.**

Периодом последовательности $a_0a_1 \dots a_{n-1}$ называется наименьшее число $d \in \mathbb{N}$ такое, что $a_0a_1 \dots a_{n-1} = a_da_{d+1} \dots a_{n-1}a_0 \dots a_{d-1}$, т.е. $a_i = a_{(i+d) mod\, n}$, $i = 0,1,\dots,\ n-1$. Период последовательности длины n является делителем числа n. Всякая последовательность периода d состоит из n/d одинаковых частей. Из каждой кольцевой последовательности периода d, разрывая её в d последовательных местах, можно получить d различных линейных последовательностей. Всего имеется r^n линейных последовательностей длины n. Поэтому

$$r^n = \sum_{d|n} dM_d,$$

где M_d – число кольцевых последовательностей периода d.

Применяя теорему об обращении Мёбиуса, получаем

$$nM_n = \sum_{d|n} \mu(d) r^{n/d},$$

и, следовательно,

$$M_n = \frac{1}{n} \sum_{d|n} \mu(d) r^{n/d}.$$

Тогда общее число r-ичных кольцевых последовательностей длины n задаётся формулой

$$K_n = \sum_{d|n} M_d = \sum_{d|n} \frac{1}{d} \sum_{k|d} \mu(k) r^{d/k}. \ \square$$

Другой подход к решению этой задачи и её обобщений рассмотрен в § 29.

§ 14. Сравнения для чисел сочетаний

Пусть p – простое число, $\binom{p}{k}$ – число сочетаний из p элементов k.

14.1. ***Лемма.***

$$\binom{p}{k} \equiv 0 \ (mod\ p) \text{ для всех } 0 \le k < p.$$

Доказательство. При $0 \le k < p$ числитель в формуле

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!}$$

кратен p, а знаменатель не делится на p. Значит, $\binom{p}{k}$ кратно p. $\square$

14.2. ***Следствие.*** $(1+x)^p \equiv 1 + x^p \ (mod\ p)$.

Доказательство.

$$(1+x)^p = \sum_{k=0}^{p} \binom{n}{k} x^k = 1 + \sum_{k=1}^{p-1} \binom{n}{k} x^k + x^p \equiv 1 + x^p \ (mod\ p). \ \square$$

14.3. ***Лемма.*** *Пусть a, b, r, s – неотрицательные целые числа, причем $0 \le r, s < p$. Тогда*

$$\binom{ap+r}{bp+s} \equiv \binom{a}{b}\binom{r}{s} \ (mod\ p).$$

Доказательство. Имеем

$$(1+x)^{ap+r} = \sum_{m=0}^{ap+r} \binom{ap+r}{m} x^m$$

$$= \sum_{i=0}^{a-1} \sum_{j=0}^{p-1} \binom{ap+r}{ip+j} x^{ip+j} + \sum_{j=0}^{r} \binom{ap+r}{ap+j} x^{ap+j}.$$

С другой стороны,

$$(1+x)^{ap+r} = (1+x)^{ap}(1+x)^r = (1+x^p)^a (1+x)^r$$

$$= \sum_{i=0}^{p-1} \sum_{i=0}^{a} \binom{a}{i} x^{ip} \sum_{j=0}^{r} \binom{r}{j} x^j = \sum_{i=0}^{a-1} \sum_{j=0}^{p-1} \binom{a}{i}\binom{r}{j} x^{ip+j} + \sum_{j=0}^{r} \binom{r}{j} x^{ap+j}.$$

Сравнивая коэффициенты при одинаковых степенях x, получаем требуемый результат. $\square$

Пусть

$$k = k_m p^m + \cdots + k_1 p^1 + k_0,\ 0 \le k_i < p; \quad (1)$$

$$n = n_m p^m + \cdots + n_1 p^1 + n_0,\ 0 \le n_i < p \quad (2)$$

$-$ представления неотрицательных целых чисел k и n по основанию p. (Здесь $m -$ любое целое, при котором $k, n < p^{m+1}$). На множестве неотрицательных целых чисел определим отношение частичного порядка (отношение *предшествования*) $\preccurlyeq_p$, полагая $k \preccurlyeq_p n$, тогда и только тогда, когда

$$k_0 \le n_0, k_1 \le n_1, ..., k_m \le n_m. \quad (3)$$

14.4. ***Теорема*** (Люка, 1878). Пусть n, k удовлетворяют (1) $-$ (3). Тогда

$$\binom{n}{k} \equiv \binom{n_m}{k_m} ... \binom{n_1}{k_1}\binom{n_0}{k_0} (mod\ p).$$

Доказательство. Согласно лемме 14.3 имеем $\binom{n}{k} \equiv \binom{a}{b}\binom{n_0}{k_0} (mod\ p)$, где $a = n_{m-1}p^{m-1} + \cdots + n_2 p^1 + n_1$, $b = k_{m-1}p^{m-1} + \cdots + k_2 p^1 + k_1$. Применяя эту лемму повторно к $\binom{a}{b}$ надлежащее число раз, получаем требуемый результат. □

Замечание. Теорема не верна для непростых p. Например [**14**],

$$\binom{14}{12} \equiv 1\ (mod\ 10), \text{ но } \binom{1}{1}\binom{4}{2} \equiv 6\ (mod\ 10);$$

$$\binom{4}{2} \equiv 2\ (mod\ 4), \text{ но } \binom{1}{0}\binom{0}{2} \equiv 0 (mod\ 4). \square$$

14.5. ***Следствие***.

$$\binom{n}{k} \not\equiv 0\ (mod\ p) \Leftrightarrow k \preccurlyeq_p n.$$

Глава III. Алгебраические структуры с одной бинарной операцией

§ 15. Группоиды, полугруппы, моноиды

Определение. *Бинарной алгебраической операцией* (или *законом композиции*) на непустом множестве S называется отображение τ**:** $S^{\mathbf{2}} \longrightarrow S$, сопоставляющее паре (a, b) элементов $a, b \in S$ однозначно определённый элемент $c = \tau(a, b) \in S$.

На множестве S может быть задано много операций τ. (Если, например, S конечно, то число способов равно k^{k^2}, где k − число элементов в S.) Желая выделить одну их них, например, τ, пишут (S, τ). Такой объект называют *бинарной алгеброй*, или *группоидом*. Вместо $\tau(a, b)$ часто пишут $a\tau b$, а саму операцию обозначают каким-либо символом ($+$, $\cdot$, $*$, $\circ$ и т.п.).

Замечание. Наряду с бинарными операциями рассматривают более общие n-арные операции (унарные при $n = 1$, тернарные при $n = 3$ и т.д.). Связанные с ними алгебраические структуры (системы) составляют предмет исследования т.н. универсальных алгебр. □

Бинарная операция $*$ на множестве S называется *ассоциативной*, если $(a * b) * c = a * (b * c)$, для любых $a, b, c \in S$.

Группоид с ассоциативной операцией называют *полугруппой*.

Пример неассоциативного группоида. На множестве $\mathbb{Z}$ определим операцию $a * b = -(a + b)$. Операция неассоциативна: $(1 * 2) * 3 = 0$, но $1 * (2 * 3) = 4$.

15.1. ***Теорема.*** *Если бинарная операция $*$ на S ассоциативна, то значение выражения $x_1 * x_2 * \ldots * x_n$ не зависит от расстановки в нём скобок.*

Доказательство. При $n = 1$, 2 или 3 утверждение очевидно. Для $n \geq 4$ достаточно, применяя индукцию, показать, что

$$(x_1 * \ldots * x_k) * (x_{k+1} * \ldots * x_n) = (x_1 * \ldots * x_l) * (x_{l+1} * \ldots * x_n) \qquad (1)$$

для любых $1 \leq k,\ l \leq n - 1$. По предположению индукции расстановка скобок в $x_1 * \ldots * x_{n-1}$ не существенна; в частности,

$$(x_1 * \ldots * x_k) = (\ldots((x_1 * x_2) * x_3) * \ldots * x_{k-1}) * x_k.$$

Если $k = n - 1$, то

$$(x_1 * \ldots * x_{n-1}) * x_n = (((x_1 * x_2) * x_3) * \ldots * x_{n-1}) * x_n.$$

Если $k < n - 1$, то

$(x_1 * \ldots * x_k) * (x_{k+1} * \ldots * x_n)$
$= (x_1 * \ldots * x_k) * ((x_{k+1} * \ldots * x_{n-1}) * x_n)$
$= ((x_1 * \ldots * x_k) * (x_{k+1} * \ldots * x_{n-1})) * x_n$
$= (((x_1 * x_2) * x_3) * \ldots * x_{n-1}) * x_n.$

К такому же виду приводится и правая часть доказываемого равенства (1). □

Элемент $e \in S$ называется *нейтральным* относительно операции $*$, если $e * a = a * e = a$ для любого $a \in S$.

Полугруппу $(S, *)$ с элементом e называют *моноидом* (или *полугруппой с единицей*) и обозначают $(S, *, e)$.

В полугруппе (группоиде) может быть не более одного нейтрального элемента: если e_1, e_2 − нейтральные элементы, то $e_1 = e_1 * e_2 = e_2$.

Группоид (полугруппу) $(S', *)$ называют *подгруппоидом* (*подполугруппой*) группоида (полугруппы) $(S, *)$, если

$S' \subseteq S$ и $a * b \in S'$ для любых $a, b \in S'$. (2)

В этом случае говорят, что подмножество S' *замкнуто относительно операции* $*$.

Моноид $(M', *, e')$ называют *подмоноидом* моноида $(M, *, e)$, если выполняется (2) и $e = e' \in S'$.

Элемент a моноида $(M, *, e)$ называется *обратимым*, если найдётся элемент $b \in M$ такой, что $a * b = b * a = e$ (очевидно, что тогда и b обратим). Если таким же свойством обладает и элемент b', т.е. $a * b' = b' * a = e$, то из равенств $b = b * (a * b') = (b * a) * b' = b'$ следует, что элемент b является на самом деле единственным (по отношению к a). Это позволяет говорить об *обратном* элементе a^{-1}, к (обратимому) элементу a, со свойствами:

$$a^{-1} * a = a * a^{-1} = e, (a^{-1})^{-1} = a.$$

Если $a, b -$ обратимые элементы моноида $(M, *, e)$, то их произведение $a * b -$ также обратимый элемент, поскольку $(a * b) * (b^{-1} * a^{-1}) = e$, $(b^{-1} * a^{-1}) * (a * b) = e$. Очевидно, что $e -$ обратимый элемент. Следовательно, имеет место

15.2. ***Теорема.*** Множество всех обратимых элементов моноида $(M, *, e)$ замкнуто относительно операции $*$ и образует подмоноид в $(M, *, e)$.

§ 16. Группы

Определение. Моноид $(G, *, e)$, все элементы которого обратимы, называется *группой.*

Другими словами, группа − это множество G с бинарной операцией $*$, для которого выполняются следующие аксиомы:

G1.(*Замкнутость операции*.) $\forall a, b \in G\ (a * b \in G)$.

G2.(*Ассоциативность операции*.) $\forall a, b \in G\ ((a * (b * c) = (a * b) * c))$.

G3.(*Существование нейтрального элемента*.) $\exists e \in G\ \forall a \in G\ (a * e = e * a = a)$.

G4.(*Существование обратного элемента*.) $\forall a \in G\ \exists b \in G\ (a * b = b * a = e)$.

Замечание. Возвращаясь к введённым выше алгебраическим структурам, мы наблюдаем среди них следующую иерархию: пара $(M, *)$ является *группоидом*, если выполняется аксиома G1; *полугруппой*, если выполняются аксиомы G1 и G2; *моноидом*, если выполняются аксиомы G1, G2 и G3; *группой*, если выполняются аксиомы G1, G2, G3 и G4. □

Удобно считать, что наряду с бинарной операцией в группе определена унарная операция взятия обратного $^{-1}: G \to G, g \mapsto g^{-1}$. Справедливы формулы:

$$(g^{-1})^{-1} = g,$$

$$(g_1 * g_2 * \ldots * g_n)^{-1} = {g_n}^{-1} * {g_{n-1}}^{-1} * {g_1}^{-1}.$$

Естественным образом определяются степени элементов с очевидными свойствами:

$$g^n = g * g * \ldots * g \ (n \text{ раз}),$$

$$g^{-n} = g^{-1} * g^{-1} * \ldots * g^{-1} \ (n \text{ раз}),\ n \in \mathbb{N},$$

$$g^0 = e;\ g^m * g^n = g^{m+n},\ (g^m)^n = g^{mn},\ m, n \in \mathbb{Z}.$$

Переставлять элементы в выражении $g_1 * g_2$, вообще говоря, нельзя (т.е. $g_1 * g_2 \neq g_2 * g_1$). Если же $g_1 * g_2 = g_2 * g_1$, то элементы называются *перестановочными*, или *коммутирующими*. Если любые

два элемента G группы коммутируют, то группа G называется *коммутативной*, или *абелевой* [12].

Операция в группе чаще всего обозначается либо символом $+$ (сложение), либо символом $\cdot$ (умножение). При этом группа называется соответственно *аддитивной* или *мультипликативной*, её нейтральный элемент $-$ соответственно *нулём* (0) или *единицей* (1). В аддитивной группе элемент, обратный к элементу g, называется *противоположным* и обозначается $-g$, а вместо g^n пишут ng. В мультипликативной группе вместо $g_1 \cdot g_2$ обычно пишут $g_1 g_2$, опуская символ операции.

Примеры аддитивных групп. 1) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ $-$ аддитивные группы кольца $\mathbb{Z}$ и полей $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Пишут просто $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. 2) Любое кольцо $\mathcal{R}$ по сложению $-$ абелева группа. В частности, кольцо многочленов $\mathcal{F}[x_1,\ldots, x_n]$ и кольцо матриц $M(n, \mathcal{F})$ порядка n над полем $\mathcal{F}$ $-$ абелевы группы. 3) Любое векторное пространство $\mathcal{V}$ над полем $\mathcal{F}$ относительно сложения $-$ абелева группа. 4) $\mathbb{Z}_n = \{0, 1,\ldots, n-1\}$ $-$ полная система наименьших неотрицательных вычетов по модулю n с операцией сложения по модулю n $-$ абелева группа.

Примеры мультипликативных групп. 1) $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$, где $A^* = A\backslash\{0\}$, $-$ мультипликативные группы полей $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. 2) $\mathcal{R}^*$ $-$ множество обратимых элементов любого кольца $\mathcal{R}$ с единицей относительно умножения. В частности, $\mathbb{Z}^*= \{\pm 1\}$; $M(n,\mathcal{F})^* = GL(n, \mathcal{F})$ $-$ множество обратимых матриц из $M(n,\mathcal{F})$. 3) C_n $-$ множество всех (вещественных и комплексных) корней уравнения $x^n = 1$

$$x_k = e^{\frac{2\pi i}{n}k} = \cos\frac{2\pi}{n}k + i\sin\frac{2\pi}{n}k\,,\ k = 0, 1,\ldots, n-1,$$

где $i = \sqrt{-1}$ $-$ мнимая единица, $-$ мультипликативная коммутативная группа. 4) D_n $-$ множество вращений правильного n- угольника (при $n \geq 3$) в пространстве. Это некоммутативная группа, как и группа $GL(n, \mathcal{F})$.

---

[12] Названы так в честь норвежского математика ***Нильса Хенрика Абеля*** (5.08.1802 — 6.04.1829). Термин абелева обычно применяется к аддитивным группам.

Далее чаще используется мультипликативная форма записи операции. Группа обычно обозначается одной буквой без указания операции. Множество всех элементов группы G называется *основным множеством группы* и обозначается той же буквой G. Если основное множество конечно, то группа называется *конечной*; в противном случае она называется *бесконечной*. Число элементов конечной группы называется её *порядком*. Группа $G = \{e\}$ порядка 1 называется *единичной*, или т*ривиальной*. О бесконечной группе говорят, что она имеет *бесконечный порядок*. Для обозначения порядка группы (мощности основного множества) используются равноправные символы $Card\ G$ (*кардинальное число*), $|G|$ и $(G: e)$.

Если A, B − подмножества (основного множества) группы, то полагаем $A^{-1} = \{a^{-1} \mid a \in A\}$, $AB = \{ab \mid a \in A, b \in B\}$.

Подгруппой группы G называется подмножество в G само являющееся группой относительно той же операции, что и в G. Другими словами, подмножество $H \subseteq G$ является подгруппой тогда и только тогда, когда $e \in H$ (e − единица в G) и H замкнуто относительно умножения и взятия обратного, т.е. $HH \subseteq H$, $H^{-1} \subseteq H$ (на самом деле здесь даже равенства). Если H − подгруппа в G, то пишут $H \leq G$; если при этом $H \neq G$, то H называется *собственной* подгруппой и это обозначается как $H < G$.

§ 17. Симметрическая и знакопеременная группы

Пусть Ω_n − множество из n элементов. Природа элементов множества Ω_n несущественна; поэтому удобно считать, что $\Omega_n = \{1, 2, \ldots, n\}$. Совокупность всех биективных (т.е. взаимно однозначных) отображений $\Omega_n \longrightarrow \Omega_n$ множества Ω_n на себя с операцией композиции отображений образует группу; её называют *симметрической группой степени* n (или *на* n *точках*) и обозначают через $S(\Omega_n)$, но чаще всего как S_n. Произвольный элемент $\pi \in S_n$ называют *перестановкой*, или *подстановкой* на множестве Ω_n.

Замечание. Термины ″подстановка″ и ″перестановка″ будут считаться синонимами, хотя следует отметить определённое смысловое различие между ними: подстановка − это замена одного объекта другим, а перестановка − это перемещение объекта с одного места на другое. Далее, для определённости, будем пользоваться термином перестановка. □

В наглядной форме перестановку $\pi : i \mapsto \pi(i)$, $i \in \Omega_n$ записывают в виде двустрочной таблицы

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}, \qquad (1)$$

где нижняя строка содержит те же элементы, что и верхняя, но, возможно, в другом порядке. Поскольку верхняя строка таблицы стандартна, то перестановка записывается в виде слова $\pi(1)\pi(2)\dots\pi(n)$. Перестановка

$$e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix},$$

соответствующая тождественному отображению, называется *единичной*, или *тождественной.*

Произведение (умножение) $\pi \circ \sigma$ перестановок π и σ определяется в соответствии с общим правилом композиции отображений: $\pi \circ \sigma(i) = \pi \circ (\sigma(i))$, $i \in \Omega_n$.

Таблица для перестановки π^{-1}, обратной по отношению к перестановке π, получается из таблицы (1) обычной перестановкой строк с последующим упорядочением столбцов так, чтобы верхняя строка получила стандартный вид: 1, 2,…, n. Напомним, что $(\pi \circ \sigma)^{-1} = \sigma^{-1} \circ \pi^{-1}$.

Пример. Пусть $\pi = \begin{pmatrix} 1234 \\ 2341 \end{pmatrix}$, $\sigma = \begin{pmatrix} 1234 \\ 3421 \end{pmatrix}$. Тогда

$$\pi\sigma = \begin{pmatrix} 1234 \\ 4132 \end{pmatrix}, \sigma\pi = \begin{pmatrix} 1234 \\ 4213 \end{pmatrix},$$

$$\pi^{-1} = \begin{pmatrix} 2341 \\ 1234 \end{pmatrix} = \begin{pmatrix} 1234 \\ 4123 \end{pmatrix}, \sigma^{-1} = \begin{pmatrix} 3421 \\ 1234 \end{pmatrix} = \begin{pmatrix} 1234 \\ 4312 \end{pmatrix}.$$

Другой общепринятый способ представления перестановки на множестве Ω_n – это разложение её на независимые циклы вида

$$k \longrightarrow \pi(k) \longrightarrow \pi^2(k) \longrightarrow \cdots \longrightarrow \pi^{r-1}(k) \longrightarrow \pi^r(k) = k, k \in \mathbb{N},$$

где $\pi^s(k) = \pi(\pi^{s-1}(k))$, а $r \in \mathbb{N}$ – наименьшее число, для которого $\pi^r(k) = k$, $k \in \mathbb{N}$. Такому циклу соответствует перестановка

$$\pi^{(k)} = \begin{pmatrix} k & \pi(k) & \dots & \pi^{r-1}(k) \\ \pi(k) & \pi^2(k) & \dots & \pi^r(k) \end{pmatrix} = \begin{pmatrix} k & \pi(k) & \dots & \pi^{r-1}(k) \\ \pi(k) & \pi^2(k) & \dots & k \end{pmatrix},$$

которую будем обозначать как $(k, \pi(k), \pi^2(k),\dots, \pi^{r-1}(k))$ и называть *простым циклом длины* r. Эта перестановка оставляет на месте элементы множества $\Omega_n \setminus \Omega^{(k)}$, где $\Omega^{(k)} = \{k, \pi(k), \pi^2(k), \dots, \pi^{r-1}(k)\}$, т.е. $\pi^{(k)}(j) = j$, если $j \in \Omega_n \setminus \Omega^{(k)}$, и перемещает элемент j в $\pi(j)$, если $j \in \Omega^{(k)}$.

Всякая перестановка π может быть разложена в произведение $\pi = \pi_1\pi_2 \ldots \pi_t$ простых циклов $\pi_1, \pi_2, \ldots, \pi_t$. Такое разложение однозначно, если не принимать во внимание порядок сомножителей, поскольку простые циклы перестановочны: $\pi_i\pi_j = \pi_j\pi_i,\ i \neq j$. Циклы длины 1 называются *тривиальными*. Поскольку им соответствуют неподвижные точки множества Ω_n, то их при записи разложения обычно опускают.

Пример. Перестановка $\pi = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 3\,9\,4\,1\,7\,2\,6\,8\,5 \end{pmatrix} \in S_9$ разлагается в произведение циклов длины 1, 3 и 5: $\pi = (134)(29576)(8) = (134)(29576)$.

Циклы длины 2 называются *транспозициями*. Транспозиция $\tau = (i, j)$ меняет местами элементы i и j, оставляя остальные элементы неподвижными. Очевидно, что $\tau^2 = e$ и $\tau^{-1} = \tau$ (такие преобразования называют *инволютивными*).

17.1. ***Теорема.*** *Всякая перестановка разлагается в произведение транспозиций*.

Доказательство. Имеем $(1\ 2\ 3 \ldots\ l-1\ l) = (1\ l)(1\ l-1) \ldots (1\ 3)(1\ 2)$. Аналогично и любой другой цикл представим в виде произведения транспозиций. Отсюда следует, что и произведение простых циклов, в которое разлагается любая перестановка, можно представить в виде произведения транспозиций. □

Замечание. Транспозиции, вообще говоря, не коммутируют. Например, $(1\ 2)(2\ 3) = (1\ 2\ 3)$, но $(2\ 3)(1\ 2) = (1\ 3\ 2)$. Разложение перестановки в произведение транспозиций в общем случае неоднозначно. □

Пусть $\pi \in S_n$ – любая перестановка, $f(x_1,\ldots, x_n)$ – любая функция от n переменных. Положим

$$(\pi \circ f)(x_1,\ldots, x_n) = f(x_{\pi^{-1}(1)},\ldots, x_{\pi^{-1}(n)}).$$

Говорят, что функция $h = (\pi \circ f)$ получена действием π на f.

Пример. Пусть $\pi = (1\ 3\ 4)(2\ 5)$, $f(x_1,\ldots, x_5) = x_1^3 + 2x_2x_3 + x_4^2x_5$. Тогда $\pi^{-1} = (1\ 4\ 3)(2\ 5)$ и $h(x_1,\ldots, x_n) = x_4^3 + 2x_5x_1 + x_3^2x_2$.

Определение. Функция $f(x_1,\ldots, x_n)$ называется *кососимметрической*, если $\tau \circ f = -f$ для любой транспозиции τ на множестве Ω_n, т.е.

$$f(\ldots, x_i,\ldots, x_j, \ldots) = -f(\ldots, x_j,\ldots, x_i, \ldots) \text{ для любых } i \neq j.$$

Пример кососимметрической функции. *Определитель Вандермонда* [13]

$$f(x_1, \ldots, x_n) = det \begin{vmatrix} x_1 & x_2 & \ldots & x_n \\ x_1^2 & x_2^2 & \ldots & x_n^2 \\ \ldots & \ldots & \ldots & \ldots \\ x_1^n & x_2^n & \ldots & x_n^n \end{vmatrix} = \prod_{1\le k\le n} x_k \prod_{k < l \le n} (x_l - x_k)$$

при перестановке двух столбцов меняет знак. Значит, f – кососимметрическая функция.

17.2. ***Лемма.*** *Пусть* $\alpha,\ \beta \in S_n$ – *любые перестановки,* $f(x_1,\ldots, x_n)$ – *любая функция. Тогда* $(\alpha\beta) \circ f = \alpha \circ (\beta \circ f)$.

***Доказательство*:**

$((\alpha\beta)\circ f)(x_1,\ldots, x_n) = f(x_{(\alpha\beta)^{-1}(1)},\ldots, x_{(\alpha\beta)^{-1}(n)})$

$= f(x_{\beta^{-1}(\alpha^{-1}(1))},\ldots, x_{\beta^{-1}(\alpha^{-1}(n))})$

$= \beta \circ f(x_{\alpha^{-1}(1)},\ldots, x_{\alpha^{-1}(n)}) = (\alpha \circ (\beta \circ f))(x_1,\ldots, x_n)$. □

17.3. ***Теорема.*** *Пусть* $\pi \in S_n$ – *любая перестановка, а* $\pi = \tau_1\tau_2 \ldots \tau_t$ – *любое разложение перестановки* π *в произведение транспозиций. Тогда число* $\varepsilon_\pi = (-1)^t$, *называемое сигнатурой (или чётностью) перестановки* π, *полностью определяется перестановкой* π *и не зависит от способа её разложения в произведение транспозиций; кроме того,*

$$\varepsilon_{\alpha\beta} = \varepsilon_\alpha\varepsilon_\beta \text{ для всех } \alpha, \beta \in S_n. \qquad (2)$$

Доказательство. Пусть $f(x_1,\ldots, x_n)$ – любая кососимметрическая функция, не равная тождественно нулю. Например,

$$f(x_1, \ldots, x_n) = \prod_{k < l \le n} (x_l - x_k).$$

Согласно лемме 17.2 $\pi \circ f = (\tau_1\tau_2 \ldots \tau_{t-1}) \circ (\tau_t \circ f) =$

---

[13] ***Александр Теофил Вандермонд*** (28.02.1735 – 1.01.1796) – французский музыкант и математик, член Парижской академии наук. Известен главным образом благодаря работам по высшей алгебре, особенно по теории детерминантов.

$= -(\tau_1\tau_2 \dots \tau_{t-1}) \circ f = \dots = (-1)^t f = \varepsilon_\pi f$. Поскольку левая часть этого соотношения зависит от π, но не зависит от её разложения в произведение транспозиций, то немедленно получаем первое утверждение. Кроме того,

$$\varepsilon_{\alpha\beta} f = \alpha\beta \circ f = \alpha \circ (\beta \circ f) = \alpha \circ \left(\varepsilon_\beta f\right)$$
$$= \varepsilon_\beta(\alpha \circ f) = \varepsilon_\beta(\varepsilon_\alpha f) = \varepsilon_\alpha \varepsilon_\beta f,$$

что доказывает (2). □

Перестановка π называется *чётной*, если $\varepsilon_\pi = 1$, и *нечётной*, если $\varepsilon_\pi = -1$.

Любая транспозиция − нечётная перестановка.

17.4. ***Теорема.***. *Если перестановка π разлагается в произведение простых циклов $\pi_1, \dots, \pi_t$, с длинами $l_1, \dots, l_t$, то $\varepsilon_\pi = (-1)^{\rho_\pi}$, где*

$$\rho_\pi = \sum_{i=1}^{t} (l_i - 1).$$

Доказательство. Так как простой цикл π_i, имеющий длину l_i, разлагается в произведение $l_i - 1$ транспозиций, то $\varepsilon_{\pi_i} = (-1)^{l_i - 1}$. Остаётся учесть, что $\varepsilon_\pi = \varepsilon_{\pi_1} \dots \varepsilon_{\pi_t}$. □

17.5. ***Теорема.*** $|S_n| = n!$

Доказательство. Нижнюю строку в (1) можно выбрать $n!$ способами**.** □

17.6. ***Теорема.*** *Чётные перестановки в S_n образуют подгруппу порядка $\frac{n!}{2}$.* (Эту подгруппу называют *знакопеременной группой степени n* и обозначают через A_n.)

Доказательство. Имеем

$\alpha, \beta \in A_n \Longrightarrow 1 = \varepsilon_\alpha \varepsilon_\beta = \varepsilon_{\alpha\beta} \Longrightarrow \alpha\beta \in A_n$;

$\varepsilon_e = 1 \Longrightarrow e \in A_n$ − единица в A_n;

$1 = \varepsilon_e = \varepsilon_{\pi \circ \pi^{-1}} = \varepsilon_\pi \varepsilon_{\pi^{-1}} \Longrightarrow \varepsilon_\pi = \varepsilon_{\pi^{-1}} \Longrightarrow (\pi \in A_n \Rightarrow \pi^{-1} \in A_n)$.

Другими словами, для A_n все аксиомы группы выполняются.

Вычислим порядок группы A_n. Представим S_n в виде объединения $A_n \cup \overline{A}_n$, где $\overline{A}_n$ − множество нечётных перестановок. Рассмотрим отображение $f: S_n \longrightarrow S_n$, определяемое правилом $f(\pi) = \tau \circ \pi$, где τ − транспозиция (1 2). Поскольку $\tau \circ \pi_1 = \tau \circ \pi_2 \Longrightarrow \pi_1 = \pi_2$, то $\pi_1 \neq \pi_2 \Longrightarrow \tau \circ \pi_1 \neq \tau \circ \pi_2$. Следовательно, отображение f инъективно и, ввиду конечности S_n, биективно. Оно переводит чётные перестановки в нечётные, а нечётные − в чётные.

Значит, $|A_n| = \left|\overline{A}_n\right| = \frac{|S_n|}{2} = \frac{n!}{2}$. □

§ 18. Морфизмы групп

Определение. Пусть $(G_1, \circ, e_1)$, $(G_2, *, e_2)$ – группы. Отображение $f: G_1 \longrightarrow G_2$ группы G_1 в группу G_2 называется *гомоморфизмом*, если оно сохраняет операцию, т.е.

$$f(a \circ b) = f(a) * f(b), \forall a, b \in G_1. \quad (1)$$

Отметим простейшие свойства гомоморфизма f:

1) *Единица e_1 отображается в единицу e_2*. Так как $e_1 \circ a = a \circ e_1 = a$, $\forall a \in G_1$, то $f(e_1) * f(a) = f(e_1 \circ a) = f(a)$, и следовательно, $f(e_1) = e_2$.

2) $f(a^{-1}) = f(a)^{-1}$. Имеем:

$f(a)^{-1} = f(a)^{-1} * e_2 = f(a)^{-1} * f(e_1) = f(a)^{-1} * f\ (a \circ a^{-1})$
$= \left(f(a)^{-1} * f(a) * f\ (a^{-1})\right) = e_2 * f(a^{-1}) = f(a^{-1})$.

Определение. *Ядром* гомоморфизма f называется множество

$$Ker\ f = \{\, a \in G_1 \mid f(a) = e_2\}.$$

18.1. ***Теорема.*** *$Ker\ f$ – подгруппа в G_1.*

Доказательство. Имеем: $a, b \in Ker\ f \Longrightarrow f(a \circ b) = f(a) * f(b) = e_2 * e_2 = e_2 \Longrightarrow a \circ b \in Ker\ f$; $f\ (e_1) = e_2 \Longrightarrow e_1 \in Ker\ f$; $a \in Ker\ f \Longrightarrow f(a^{-1}) = f(a)^{-1} = e_2^{-1} = e_2 \Longrightarrow a^{-1} \in Ker\ f$. Другими словами, для $(Ker\ f, \circ)$ выполняются все аксиомы группы. □

Аналогично доказывается следующее утверждение:

18.2. ***Теорема.*** *$Im\ f$ – подгруппа в G_2.*

Далее будем опускать знаки операций $\circ$ и $*$.

Определение. Взаимно однозначный (биективный) гомоморфизм $f: G_1 \to G_2$ называется *изоморфизмом*.

18.3. ***Теорема.*** *Если $f: G_1 \longrightarrow G_2$ – изоморфизм, то существует обратное отображение $f^{-1}: G_2 \longrightarrow G_1$, которое также является изоморфизмом.*

Доказательство. Так как f – биекция, то обратное отображение f^{-1} заведомо существует. Поэтому достаточно убедиться в выполнении свойства (1). Ввиду биективности f для любых $x, y \in G_2$ найдутся такие $a, b \in G_1$, что $x = f(a)$, $y = f(b)$ и $a = f^{-1}(x)$, $b = f^{-1}(y)$. Но тогда $x * y = f(a) * f(b) = f(a \circ b) \Longrightarrow f^{-1}(x * y) = a \circ b = f^{-1}(x) * f^{-1}(y)$. □

Группы G и H называются *изоморфными* (обозначение: $G \cong H$), если существуют изоморфизмы, переводящие одну группу в другую.

Изоморфные группы имеют одинаковые алгебраические свойства (если не рассматривать какие-либо дополнительно определённые на них структуры). В абстрактной теории групп к ним относятся как к одинаковым объектам.

Замечание. В определении гомоморфизма от отображения $f: G_1 \longrightarrow G_2$ не требуется не только биективности, но и сюръективности. Однако последнее не очень-то существенно. Поскольку $Im\ f$ – подгруппа в G_2, можно вместо отображения f рассматривать отображение φ**:** $G_1 \longrightarrow Im\ f$, которое уже будет сюръективным. Главное же отличие гомоморфизма от изоморфизма заключается в наличии нетривиального ядра $Ker\ f$, являющегося мерой неинъективности. □

18.4. ***Теорема.*** *Сюръективный гомоморфизм $f: G_1 \longrightarrow G_2$ является изоморфизмом тогда и только тогда, когда ядро отображения f тривиально, т.е. $Ker\ f = \{e_1\}$.*

Доказательство. Если ядро $Ker\ f$ нетривиально, то отображение f не является инъекцией, следовательно, не является изоморфизмом. Теперь предположим, что ядро тривиально, т.е. состоит из одного элемента e_1. Допустим, что $f(a) = f(b)$ для некоторых $a, b \in G_1$. Тогда $e_2 = f(a) * \big(f(b)\big)^{-1} = f\ (a \circ b^{-1}) \Longrightarrow a \circ b^{-1} \in Ker\ f \Longrightarrow$ $a \circ b^{-1} = e_1 \Longrightarrow a = b$. Другими словами, если $a \neq b$, то $f(a) \neq f(b)$. Значит, f – инъективное отображение и, следовательно, изоморфизм. □

18.5. ***Теорема*** Кэли [14]. *Любая конечная группа G порядка n изоморфна некоторой подгруппе симметрической группы S_n.*

Доказательство. Пусть $g_1 = e, g_2, \ldots, g_n$ – все элементы группы G. Для произвольного $a \in G$ рассмотрим отображение $\pi_a: G \longrightarrow G$, определяемое правилом $\pi_a(g) = ag$. Так как $ag_i = ag_j \Longrightarrow g_i = g_j$,

---

[14] ***Артур Кэли*** (16.08.1821 – 26.01.1895) – английский математик. Автор более 700 работ. В частности, ему принадлежит теорема о том, что каждая квадратная матрица является корнем своего характеристического многочлена. Первым сформулировал определение группы в том виде, как она определяется сегодня – множество с бинарной операцией, удовлетворяющее определённым аксиомам.

то $g_i \neq g_j \Longrightarrow ag_i \neq ag_j$. Поэтому π_a – биекция на G, и, следовательно,

$$\pi_a = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ ag_1 & ag_2 & \ldots & ag_n \end{pmatrix} \in S(G)$$

– перестановка на n точках $g_1, g_2, \ldots, g_n$. Положим теперь $\Pi = \{\pi_a \mid a \in G\}$ и покажем, что множество Π образует группу относительно композиции (произведения) отображений, определяемых, как обычно, по правилу $\pi_a \circ \pi_b(g) = \pi_a(\pi_b(g))$. Для этого проверим выполнимость аксиом $\mathrm{G1} - \mathrm{G4}$:

G1. Поскольку $g \overset{\pi_b}{\to} bg \overset{\pi_a}{\to} abg$, то $\pi_a \circ \pi_b = \pi_{ab}$, т.е. множество Π замкнуто относительно операции $\circ$.

G2. Как любая композиция отображений, операция ассоциативна, т.е. $\pi_a \circ (\pi_b \circ \pi_c) = (\pi_a \circ \pi_b) \circ \pi_c = \pi_{abc}$.

G3. Перестановка π_e – нейтральный элемент (единица) в Π.

G4. Так как $\pi_a \circ \pi_{a^{-1}} = \pi_{a^{-1}} \circ \pi_a = \pi_e$, то $\pi_a^{-1} = \pi_{a^{-1}} \in \Pi$, т.е. каждый элемент в Π имеет обратный.

Таким образом, Π – группа. Изоморфизм групп G и Π устанавливается соответствием $a \in G \longrightarrow \pi_a \in \Pi$, которое биективно и удовлетворяет, согласно (1), свойству сохранения операции: $ab \mapsto \pi_a \circ \pi_b$. □

Замечание. Теорема Кэли имеет важное значение в теории групп. Она выделяет универсальный объект – семейство симметрических групп S_n, $n = 1, 2, 3, \ldots$, как хранилище всех конечных групп, рассматриваемых с точностью до изоморфизма. □

Другие морфизмы. Гомоморфизм, являющийся отображением *на*, называется *сюръективным*, или *эпиморфизмом*. Гомоморфизм $f: G \longrightarrow G$ группы G в себя называется *эндоморфизмом.* Изоморфизм группы на себя называется *автоморфизмом*. Множество всех эндоморфизмов образует полугруппу, а множество всех автоморфизмов – группу.

§ 19. Смежные классы по подгруппе

Определение. Пусть G – группа, а H – её подгруппа. *Левый смежный класс* группы G по подгруппе H определяется как множество $gH = \{gh \mid h \in H\}$, $g \in G$. Всякий элемент из gH называется *представителем смежного класса*.

Отображение $f: x \longrightarrow gx$ является биекцией H на gH. Поэтому любые два смежных класса g_1H и g_2H равномощны.

Смежные классы g_1H и g_2H, имеющие хотя бы один общий элемент совпадают. Действительно, пусть $g_1h_1 = g_2h_2$, где $h_1, h_2 \in H$. Тогда $g_1 = g_2h$, $h_2 = h_2h_1^{-1}$. Так как $h \in H$ и $hH = H$, то $g_1H = g_2hH = g_2H$.

Таким образом, G есть объединение непересекающихся левых смежных классов:

$$G = \bigcup_{g \in G} gH.$$

Аналогичные замечания справедливы и для правых смежных классов $Hg = \{hg \mid h \in H\}$, $g \in G$.

Число левых смежных классов группы G обозначается через $(G{:}H)$ и называется *индексом* подгруппы H в G. Индекс тривиальной подгруппы $H = \{e\}$ равен порядку группы G.

Очевидно, что

$$(G{:}H) \cdot |H| = |G|.$$

Таким образом, имеет место

19.1. ***Теорема*** Лагранжа [15]. *Порядок конечной группы делится без остатка на порядок любой её подгруппы.*

19.2. ***Следствие***. *Если порядок группы G равен простому числу, то G не имеет собственных подгрупп, т.е. отличных от самой группы G и тривиальной подгруппы $H = \{e\}$ порядка* 1.

Замечание. Теорема Лагранжа, вообще говоря, не допускает обращения: если m делит порядок $|G|$, то это ещё не означает, что в группе G существует подгруппа порядка m. Например, в знакопеременной группе A_4 нет подгрупп порядка 6. (Проверить самостоятельно.) Однако для абелевых групп обращение теоремы Лагранжа имеет место. Кроме того, если $m = p^k$ – степень простого числа, то в группе G существует подгруппа порядка m (см. теорему Силова). □

Множество левых смежных классов обозначается через G/H (или через $(G\ /\ H)_l$, если есть необходимость отличать его от множества правых смежных классов $(G\ /\ H)_r$). Очевидно, что для абелевых

---

[15] ***Жозеф Луи Лагранж*** (25.01.1736 – 10.04.1813) – французский математик, астроном и механик итальянского происхождения. Наряду с Эйлером – крупнейший математик XVIII века.

групп $(G\ /\ H)_l = (G\ /\ H)_r$, но в общем случае множество левых смежных классов может не совпадать с множеством правых смежных классов.

Примеры. 1) Пусть $G = (\mathbb{Z}, +)$, $H = G = (n\mathbb{Z},+)$, $n \in \mathbb{N}$. Поскольку G и H – абелевы группы, то множества левых и правых смежных классов совпадают. Имеем следующее разложение на G смежные классы:

$$G = [0] \cup [1] \cup \ldots \cup [n-1],$$

где $[a] = a + H = H + a = \{h + a \mid h \in H\} = \{z \mid z \equiv a\ (mod\ n),$ $z \in \mathbb{Z}\}$, $a \in \mathbb{Z}$.

2) Пусть $G = S_3$, $H = S_2 = <(12)>$. Разложения группы G по подгруппе H в левые L и правые смежные R классы имеют вид:

$$G = L_1 \cup L_2 \cup L_3 = R_1 \cup R_2 \cup R_3,$$

где

$$L_1 = \{e, (12)\},\ L_2 = \{(13), (123)\}, L_3 = \{(23), (132)\};$$
$$R_1 = \{e, (12)\},\ R_2 = \{(13), 132)\},\ R_3 = \{(23), (123)\}.$$

§ 20. Нормальные делители. Факторгруппы

В группах особенно важную роль играют те подгруппы, относительно которых левые и правые смежные классы совпадают. Такие подгруппы называют *нормальными*.

Определение. Подгруппа $H \leq G$ называется *нормальной* или *нормальным делителем* группы G, что обозначается $H \trianglelefteq G$, если $Hg = gH$ для любого $g \in G$, т.е. каждый левый смежный класс gH совпадает с правым смежным классом Hg.

Если $H \trianglelefteq G$ – собственная подгруппа в G, то пишем $H \triangleleft G$.

20.1. ***Лемма***. *Любое из следующих условий на подгруппу H группы G равносильно её нормальности*:

(1) $gHg^{-1} = H$ *для любого* $g \in G$;

(2) $ghg^{-1} \in H$ *для любых* $h \in H$, $g \in G$.

Доказательство. (1) $gHg^{-1} = H \Longrightarrow Hg = gH \Longrightarrow gHg^{-1} = H$.

(2) $gHg^{-1} \subset H \Longrightarrow H \subset Hg \Longrightarrow H \subset g^{-1}Hg \Longrightarrow H \subset (g^{-1})^{-1}Hg^{-1}$ $\Longrightarrow H \subset gHg^{-1} \Longrightarrow\ Hg = gH.$ □

В абелевых группах, в силу коммутативности групповой операции, любая подгруппа является нормальным делителем.

Группа G называется *простой*, если в ней нет неединичных собственных нормальных подгрупп. Примером таких групп являются

группы простого порядка p, поскольку в них, как следует из теоремы Лагранжа, нет неединичных собственных подгрупп.

В неабелевых группах могут быть подгруппы как являющиеся, так и не являющиеся нормальными делителями.

Пример. Пусть G $= S_3$. 1) $H = A_3 = \{e = (1)(2)(3), h_1 = (123), h_2 = (312)\}$. Левыми смежными классами группы G по H являются: $eH = A_3$ и gH $= \{(12)(3), (1)(23), (13)(2)\}$, где $g = (12)(3)$. Такие же и правые классы. Значит, A_3 – нормальный делитель в S_3. 2) Пусть теперь $H = S_2 = \{e, (12)\}$. Рассмотрим разложение S_3 в левые и правые смежные классы по подгруппе H:

S_3 ={e, (12)} ∪ {(13), (123)} ∪ {(23), (132)};

S_3 ={e, (12)} ∪ {(13), (132)} ∪ {(23), (123)}.

Множества смежных классов $S_2 g$ и $g S_2$ не совпадают. Значит, S_2 не является нормальной подгруппой в S_3.

***Замечание*:** термин *"ненормальная подгруппа"* не употребляется!

Важным свойством нормальной подгруппы является тот факт, что множество левых (равно, как и правых) смежных классов по ней можно наделить групповой структурой.

20.2. ***Теорема.*** *Пусть $H \trianglelefteq G$ – нормальная подгруппа. Множество всех различных левых смежных классов $\{gH | g \in G\}$ с операцией умножения*

$$g_1 H \circ g_2 H \stackrel{\text{def}}{=} g_1 g_2 H$$

образует группу G/H, которая называется факторгруппой группы G по нормальной подгруппе H.

Доказательство. Вначале докажем, что операция $\circ$ определена корректно, т.е. не зависит от выбора представителей смежных классов. Требуется показать, что $a_1 H = a_2 H,\ b_1 H = b_2 H \Longrightarrow a_1 b_1 H = a_2 b_2 H$, или, что то же самое, $(a_2 b_2)^{-1} a_1 b_1 \in H$.

Имеем $a_2^{-1} a_1 = h_1$, $b_2^{-1} b_1 = h_2$, $h_1 b_1 = b_1 h_3$, причем $h_1, h_2, h_3 \in H$. Тогда $(a_2 b_2)^{-1} a_1 b_1 = b_2^{-1} a_2^{-1} a_1 b_1 = b_2^{-1} h_1 b_1 = b_2^{-1} b_1 h_3 = h_2 h_3 \in H$, что доказывает корректность введённой операции [16].

---

[16] Это можно доказать и короче: если aH, bH – смежные классы, то их произведение также является смежным классом, поскольку $aHbH = abHH = abH$.

Проверим теперь, что для структуры $(G\,/\,H,\circ)$ выполнены все аксиомы группы. Имеем:

G1. Операция $\circ$ замкнута на множестве G/H. Это очевидно.

G2. Операция ассоциативна:

$$(aH\circ bH)\circ cH = abH\circ cH = abcH = aH\circ bcH = aH\circ(bH\circ cH).$$

G3. Нейтральным элементом в $G\,/\,H$ является класс $eH = H$, где $e-$ единица в G.

G4. Элемент (класс) $a^{-1}H$ является обратным для элемента aH:

$$a^{-1}H\circ\ aH = aH\circ a^{-1}H =\ aa^{-1}H = eH.\ \square$$

Пример. Пусть $G = (\mathbb{Z},+)$, $H = (n\mathbb{Z},+)$, где $n\mathbb{Z}-$ множество целых чисел, кратных $n\in\mathbb{N}$. Элементами группы $G\,/\,H\ = \mathbb{Z}\,/\,n\mathbb{Z}$ являются указанные ранее в § 19 смежные классы $[k]$, $0\le k<n$ с операцией сложения $[a]\oplus[b]=[c]$, где $c-$ остаток от деления $a+b$ на n. Эту группу называют *аддитивной группой целых чисел по модулю* n. Она ещё встретится в несколько другом качестве.

20.3. ***Лемма.*** *Пусть* $f\colon G_1\longrightarrow G_2\ -$ *гомоморфизм групп. Тогда* $Ker\ f-$ *нормальная подгруппа в* G_1.

Доказательство. Тот факт, что $Ker\ f-$ подгруппа в G_1, уже доказан в лемме 18.1. Докажем её нормальность. Пусть $h\in Ker\ f$, $g\in G$ – любые элементы. Тогда $f(ghg^{-1}) = f(g)f(h)\,f(g^{-1}) = f(g)e_2f(g^{-1}) = f(g)e_2f(g^{-1}) = f(gg^{-1}) = f(e_1) =\ e_2$. Отсюда следует, что $ghg^{-1}\in Ker\ f$, и, согласно лемме 20.1, $Ker\ f-$ нормальная подгруппа. $\square$

20.4. ***Теорема*** (О гомоморфизмах групп). 1) *Пусть* $\varphi: G\ \longrightarrow G'-$ *сюръективный гомоморфизм группы* G *на группу* G'. *Тогда* $Ker\ \varphi-$ *нормальная подгруппа в* G, *и* $G'\cong G\ /\ Ker\ \varphi$.

2) *Обратно, если* $G-$ *группа, а* $H-$ *её нормальная подгруппа, то отображение* $\psi: G\longrightarrow G\ /\ H$, *определяемое по правилу* $\psi(g) = gH$, *является сюръективным гомоморфизмом с ядром* $Ker\ \psi = H$.

Доказательство. 1) Тот факт, что $H = Ker\ \varphi-$ нормальная подгруппа в G, уже установлен в лемме 20.3.

Пусть $y\in G'-$ произвольный элемент, а $x\in G$ такой элемент, что $y=\varphi(x)$. Так как $\varphi(h)=1$ для любого $h\in H$, то $\varphi(xh) = \varphi(x)\varphi(h) = y$, т.е. все элементы смежного класса xH отображаются при φ в элемент y.

С другой стороны, если $z\in G\ -$ любой элемент такой, что $\varphi(z)=y$, то $\varphi(x^{-1}z) = \varphi(x^{-1})\varphi(z) = y^{-1}y = 1$, откуда следует, что z содержится в смежном классе xH. Таким образом, собирая все эле-

менты группы G, которые отображаются в фиксированный элемент $y \in G'$, мы получаем в точности смежный класс xH.

Соответствие μ, сопоставляющее каждому элементу $y \in G'$ тот смежный класс группы G по нормальному делителю H, который состоит из всех элементов группы G, имеющих элемент y своим образом, будет взаимно однозначным отображением группы G на $G\,/\,H$. Это отображение является изоморфизмом. Действительно, если $\mu(y) = xH$ и $\mu(u) = vH$, т.е. $\varphi(x) = y$ и $\varphi(v) = u$, то $\varphi(xv) = \varphi(x)\varphi(v) = yu$, а поэтому $\mu(yu) = xvH = xH \cdot vH = \mu(y)\mu(v)$.

Наконец, если x – произвольный элемент из G и $\varphi(x) = y$, то $\mu\big(\varphi(x)\big) = \mu(y) = xH$, т.е. последовательное выполнение гомоморфизма φ и изоморфизма μ на самом деле отображает элемент x в порождаемый им смежный класс xH.

2) Пусть теперь H – произвольная нормальная подгруппа в G. Тогда, ставя в соответствие всякому элементу $x \in G$ тот смежный класс xH, в котором этот элемент лежит, мы получим отображение ψ группы G на всю факторгруппу $G\,/\,H$. Из определения умножения в группе $G\,/\,H$ следует, что это отображение – изоморфизм. □

§ 21. Циклические группы

Определение. Пусть G – группа, $g \in G$ – любой элемент. Множество

$$< g > = \{g^n \mid n \in \mathbb{Z}\} \qquad (1)$$

степеней элемента g образуют в G подгруппу. Она называется *циклической* подгруппой, порождённой элементом g. Группа G называется *циклической*, если существует элемент $g \in G$ такой, что $G = < g >$.

Для произвольного $g \in G$ имеются две возможности:

1) $g^m \neq g^n$ при любых $m \neq n$. В этом случае $< g >$ называют *бесконечной циклической подгруппой* (или *группой*), а g – *элементом бесконечного порядка*.

2) $g^m = g^n$ для некоторых $m \neq n$. В этом случае ввиду $g^{m-n} = g^{n-m} = e$ (e – единица в G) существует положительные степени g, равные e. Наименьшее $n \in \mathbb{N}$, для которого $g^n = e$, называют *порядком элемента* g и обозначают $ord\ g$. Очевидно, в конечной группе все элементы имеют конечный порядок; в бесконечной группе могут быть элементы как конечного, так и бесконечного порядка.

Примеры циклических групп. 1) $C_n = \{\omega^0 = 1, \omega^1, \omega^2, \ldots, \omega^{n-1}\}$ – мультипликативная группа корней n-ой степени из 1, порождаемая элементом $\omega = e^{2\pi i/n}$, где $i = \sqrt{-1}$, а также любым элементом ω^k, где НОД $(k,n) = 1$; её порядок равен n. 2) $\mathbb{Z}$ – аддитивная группа целых чисел, порождаемая как числом 1, так и числом -1; это бесконечная группа.

Замечание. В определении (1) использовалась мультипликативная форма записи групповой операции. При использовании аддитивной записи вместо (1) следует написать $< g > = \{ng \mid n \in \mathbb{Z}\}$, где $ng = g + \cdots + g$ (n слагаемых), если $n \geq 1$; $0g = 0$ (0 – нулевой элемент группы); $ng = (-n)(-g)$, если $n < 0$. Если $mg \neq ng$ при любых $m \neq n$, то g называется элементом бесконечного порядка. Если $mg = ng$, для некоторых $m > n$, то порядком элемента g называется наименьшее n, для которого $ng = 0$.

21.1. ***Теорема***. *Пусть G – группа порядка n, а $g \in G$ – элемент порядка d. Тогда*

$$g^s = g^t \Leftrightarrow s \equiv t \,(mod\ d); \tag{2}$$

$$< g > = \{ g^0 = e, g^1, g^2, \ldots, g^{d-1}\}; \tag{3}$$

$$d \mid n. \tag{4}$$

Доказательство. Представим число $s \in \mathbb{Z}$ в виде $s = dq + r$, где $0 \leq r < d$ (r – остаток от деления s на d). Тогда $g^e = g^{dq} \cdot g^r = g^r$; отсюда вытекают утверждения (2) и (3). Поскольку $< g >$ – подгруппа в G, то по теореме Лагранжа имеет место (4). □

21.2. ***Теорема***. *Группа G простого порядка p всегда циклическая.*

Доказательство. Порядок любого элемента $g \in G \setminus \{e\}$ больше 1 и является делителем числа p, т.е. равен p. Значит, $G = < g >$. □

21.3. ***Теорема***. *Любые циклические группы $G_1 = < g_1 >$ и $G_2 = < g_2 >$ одного и того же порядка* (*в том числе и бесконечного*) *изоморфны.*

Доказательство. Изоморфизм $G_1 \cong G_2$ устанавливается соответствием $g_1^n \leftrightarrow g_2^n$, $n \in \mathbb{Z}$, которое взаимно однозначно и сохраняет операции. □

21.4. ***Следствие.*** *Любая конечная циклическая группа порядка n изоморфна группе C_n; любая бесконечная циклическая группа изоморфна группе $\mathbb{Z}$.*

21.5. ***Теорема***. *Пусть G – группа, $g \in G$ и $ord\ g = n$. Тогда*

$$ord\ g^r = \frac{n}{d}, \text{ где } d = \text{НОД}\,(n, r).$$

Доказательство. Порядок элемента g^r равен наименьшему $x \in \mathbb{N}$, для которого $rx \equiv 0\ (mod\ n)$, или, что равносильно, $\frac{r}{d}x \equiv 0\ (mod\ \frac{n}{d})$. Так как $\frac{n}{d}$ и $\frac{r}{d}$ взаимно просты, то $x \equiv 0\ (mod\ \frac{n}{d})$ и $x = \frac{n}{d}$. □

21.6. ***Следствие***. *Множество порождающих элементов группы* $G = < g >$ *порядка* n *состоит в точности из элементов* g^r, *для которых* НОД $(n, r) = 1$. *Число таких элементов равно* $\varphi(n)$, *где* $\varphi(n)$ *– функция Эйлера.*

21.7. ***Теорема*** . *Бесконечная циклическая группа имеет в точности два порождающих элемента, причем, если* g *– один из них, то* g^{-1} *– единственный другой. В частности, группа* $\mathbb{Z}$ *порождается обычной* 1 *и* -1.

Доказательство. Все бесконечные циклические группы изоморфны группе $\mathbb{Z}$. Поскольку в $\mathbb{Z}$ только два порождающих элемента, то столько же и в любой другой бесконечной циклической группе. □

21.8. ***Теорема***. *Любая подгруппа циклической группы также является циклической. При этом*:

a) *Подгруппы конечной циклической группы* $< g >$ *порядка* n *исчерпываются группами* $< g^d >$, где $d \mid n$.

b) *Подгруппы бесконечной циклической группы* $< g >$ *исчерпываются тривиальной группой* $< e >$ *порядка* 1 *и бесконечными группами* $< g^d >$, $d \in \mathbb{N}$. (*В частности, подгруппами аддитивной группы целых чисел* $\mathbb{Z}$ *являются тривиальная группа* $< 0 >$, *состоящая из одного числа* 0, *и группы* $d\mathbb{Z}$, *образованные целыми числами, кратными* $d \in \mathbb{N}$).

Доказательство. a) Пусть H – подгруппа в $< g >$, а $d \in \mathbb{N}$ – наименьшее целое, для которого $g^d \in H$. Очевидно, $< g^d > \subseteq H$. Покажем, что в действительности $< g^d > = H$ и $d \mid n$. Возьмём в H произвольный элемент, он имеет вид g^k, $0 \le k < n$. Представим числа k и n в виде $k = ad + r$, $n = bd + s$; $a,b,r,s \in \mathbb{Z}$, $0 \le r,s < d$. Имеем $g^r = g^k(g^d)^{-a} \in H$, $g^s = g^n(g^d)^{-b} \in H$, откуда, по выбору числа d, следует, что $r = s = 0$, т.е. $d \mid k$ и $d \mid n$.

b) Очевидно, что $< e >$ и $< g^m >$, где $m \in \mathbb{N}$, – подгруппы в $< g >$. Покажем, что других групп в $< g >$ нет. Пусть H – любая подгруппа в $< g >$, отличная от $< e >$, и пусть $d \in \mathbb{N}$ – наименьшее, а $k \in \mathbb{Z}$ – любое, для которых $g^d, g^k \in H$. Тогда, представляя k в виде $k = ad + r$, где $a, r \in \mathbb{Z}$, $0 \le r < d$, имеем $g^r = g^k(g^d)^{-a} \in H$.

Отсюда заключаем, что $r = 0$, $d \mid k$, а подгруппа H состоит из элементов вида g^{da}, $a \in \mathbb{Z}$, т.е. $H = < g^d >$. □

21.9. ***Теорема*** . *Пусть $a, b -$ перестановочные элементы группы G (т.е. $ab = ba$) порядков r и s соответственно. Тогда*:

a) *Если r и s взаимно просты, т.е.* НОД $(r,s) = 1$, то $ord(ab) = rs$, $< a,b >=< ab >$, где $< a, b > -$ *группа, порождённая элементами a и b (т.е. состоящая в данном случае из всевозможных произведений элементов a^k и b^l; $0 \le k < r$, $0 \le l < s$).*

b) *Если* НОД $(r, s) = d \ge 1$, *то в G существует элемент c порядка* $t =$ НОК $[r, s]$.

Доказательство. a) Вначале покажем, что $< a > \cap < b >= \{e\}$. Действительно, если $c = a^k = b^l$, то $c^r = a^{kr} = e$, $c^s = b^{ls} = e$; отсюда следует, что $ord(c) \mid r$ и $ord(c) \mid s$. Так как r и s взаимно просты, то $ord\,(c) = 1$ и $c = e$. Пусть $ord\,(ab) = n$. Тогда $(ab)^n = a^n b^n = e \Longrightarrow a^n = b^{-n} \Longrightarrow a^n = e, b^n = e \Longrightarrow r \mid n,\ s \mid n \Longrightarrow rs \mid n$.

С другой стороны, $n \mid rs$, так как $(ab)^{rs} = e$. Следовательно, $n = rs$. Учитывая, что $|< a,b >| = |\{a^k b^l \mid 0 \le k < r, 0 \le l < s\}| \le rs = n$ и $< ab > \subseteq < a, b >$, заключаем, что $< ab > = < a,b >$.

b) Пусть $r = p_1^{\alpha_1} \ldots p_t^{\alpha_t}$, $s = p_1^{\beta_1} \ldots p_t^{\beta_t} -$ разложения чисел r и s на простые множители, причем будем считать, что простые числа перенумерованы так, что $\alpha_1 \ge \beta_1, \ldots, \alpha_u \ge \beta_u$; $\alpha_{u+1} \le \beta_{u+1}, \ldots, \alpha_t \le \beta_t$. Положим

$$r_1 = p_1^{\alpha_1} \ldots p_u^{\alpha_u},\ r_2 = p_{u+1}^{\alpha_{u+1}} \ldots p_t{}^{\alpha_t},$$
$$s_1 = p_1^{\beta_1} \ldots p_u^{\beta_u},\ s_2 = p_{u+1}^{\beta_{u+1}} \ldots p_t^{\beta_t}.$$

Поскольку $ord(a^{r_2}) = r_1$, $ord(b^{s_1}) = s_2$, НОД $(r_1, s_2) = 1$, то согласно утверждению предыдущего пункта элемент $c = a^{r_2} b^{s_1}$ имеет порядок равный $r_1 s_2 =$НОК $[r, s]$. □

21.10. ***Следствие***. *Пусть $G -$ конечная абелева группа, а $m -$ максимальный порядок её элементов, т.е. $m = max\,\{ord\,(g) \mid g \in G\}$. Тогда порядок любого элемента $g \in G$ является делителем ла m.*

Доказательство. Пусть $g \in \mathrm{G} -$ любой элемент, $ord\,(g) = d$. Согласно пункту b) предыдущей теоремы существует элемент $c \in G$ порядка $t =$ НОК $[d, m]$. Если $d \nmid m$, то НОК $[d, m] > m$, что противоречит выбору числа m. Значит, $d \mid m$. □

§ 22. Теоремы Силова [17]

Определение. Подгруппу H конечной группы G называют p- *подгруппой,* или *примарной подгруппой, если* $|H| = p^k$, *где* $p -$ простое число, $k \in \mathbb{N}$. Если $p^k -$ наибольшая степень числа p, делящая $|G|$, то H называют *силовской подгруппой* группы G.

Определение. Подгруппы H и H' группы G называются *сопряженными*, если $H' = gHg^{-1}$ *для некоторого* $g \in G$.

22.1. ***Теоремы*** Силова**.** *Пусть* $G -$ *конечная группа,* $p^k -$ *наибольшая степень простого числа* p, *делящая* $|G|$. *Тогда*:

1) *Для любого числа* $0 \leq l \leq k$ *в группе* G *найдётся подгруппа порядка* p^l.

2) *Если* $0 \leq l \leq k-1$, *то любая подгруппа* H_l *порядка* p^l *содержится в некоторой подгруппе порядка* p^{l+1}. *В частности, подгруппы порядка* p^k *и только они являются максимальными* p- *подгруппами группы* G. *Они называются силовскими* p-*подгруппами группы* G.

3) *Все силовские* p-*подгруппы группы* G *сопряжены между собой*.

4) *Число силовских подгрупп в* G *сравнимо с единицей по модулю* p *и делит порядок группы* G.

Доказательство. См.[**11**, **39**].

§ 23. Мультипликативная группа целых чисел по модулю n

Пусть $n \in \mathbb{N}$. Обозначим через $\mathbb{Z}_n^*$ мультипликативную группу обратимых элементов кольца $\mathbb{Z}_n$. Элементами этой группы являются смежные классы $\overline{a} = a + n\mathbb{Z}$, $a \in G_n$, $n \in \mathbb{Z}$, где $G_n -$ любая приведённая система вычетов по модулю n. Для определённости, в качестве G_n возьмём приведённую систему наименьших неотрицательных вычетов по модулю n, т.е.

$$G_n = \{a \in \mathbb{Z} \mid 1 \leq a < n, \text{НОД}\,(a, n) = 1\}.$$

В этом разделе уточняется строение группы $\mathbb{Z}_n^*$.

---

[17] ***Петер Людвиг Мейделль Сюлов*** **(*Силов*)** (12.12.1832– 7.09.1918) — норвежский математик. Автор работ по теории эллиптических функций и теории групп. Теоремы Силова образуют фундаментальную часть теории конечных групп.

Для взаимно простых чисел $a \in \mathbb{Z}$ и $n \in \mathbb{N}$ обозначим через $ord_n(a)$ наименьшее $\delta \in \mathbb{N}$, для которого $a^\delta \equiv 1(mod\, n)$. Число $ord_n(a)$ называется *мультипликативным порядком* числа a по модулю n. Отметим некоторые свойства величины $ord_n(a)$ (как частные случаи соответствующих утверждений о циклических группах):

$$a^\lambda \equiv 1\ (mod\, n) \Longrightarrow ord_n(a) | \lambda; \quad (1)$$

$$ord_n(a) = r,\ ord_n(b) = s,\ \text{НОД}\ (r, s) = 1 \Longrightarrow ord_n(ab) = rs; \quad (2)$$

$$\text{НОД}\ (a, n) = 1 \Longrightarrow a^{\lambda(n)} \equiv 1\ (mod\, n), \quad (3)$$

где $\lambda(n)$ – наибольший мультипликативный порядок по модулю n среди элементов $a \in G_n$, т.е. $\lambda(n) = max\ \{ord_n(a) \mid a \in G_n\}$.

Заметим, что $\lambda(n) \mid \varphi(n)$. Поскольку можно указать n, для которых $\lambda(n) < \varphi(n)$, то утверждение (3)) является уточнением теоремы Эйлера. (Например, $\varphi(36) = 12$, а $\lambda(36) = 6$. Поэтому $a^6 \equiv 1(\text{mod } 36)$ для любого нечетного a, которое не делится на 3.) Формула для $\lambda(n)$, называемой *функцией Кармайкла*, устанавливается ниже. Число a, для которого $ord_n(a) = \lambda(n)$, называется *примитивным* (или *первообразным*) элементом по модулю n. Если при этом $\lambda(n) = \varphi(n)$, то a называется *первообразным корнем* по модулю n.

23.1. ***Теорема.*** *Пусть* НОД $(r, s) = 1$. *Тогда*

$$\mathbb{Z}^*_{rs} \cong \mathbb{Z}^*_r \times \mathbb{Z}^*_s, \quad (4)$$

$$\lambda(n) = \text{НОК}\ [\lambda(r), \lambda(s)]. \quad (5)$$

Доказательство. Рассмотрим множество чисел

$$c_{a,b} = as^{\varphi(r)} + br^{\varphi(s)};\ a \in G_r, b \in G_s.$$

Покажем, что

$$c_{a,b} \not\equiv c_{a',b'}\ (mod\, rs),\ \textit{если}\ (a, b) \neq (a', b'); \quad (6)$$

$$\text{НОД}\ (c_{a,b}, rs) = 1\ \textit{для любых чисел}\ a \in G_r, b \in G_s; \quad (7)$$

$$c_{a,b}\, c_{a',b'} \equiv c_{\alpha,\beta} (mod\, rs),\ \textit{где}\ \alpha = aa'\ mod\ r,\ \beta = bb'\ mod\ s. \quad (8)$$

Действительно, если $c_{a,b} \equiv c_{a',b'}\ (mod\, rs)$, *то* $(a - a')s^{\varphi(r)} + (b - b')r^{\varphi(s)} = 0$, и, следовательно, $r \mid (a - a')\ u\ s \mid (b - b')$, но тогда $(a, b) = (a', b')$. Если НОД $(c_{a,b}, rs) = d > 1$, то d кратно некоторому простому числу p, которое кратно либо r, либо s. Пусть, для определённости, $r \mid p$. Тогда $p \mid a$, что невозможно для $a \in G_r$. Для доказательства (8) отметим, что

$$s^{2\varphi(r)} \equiv s^{\varphi(r)}(1 + qr) \equiv s^{\varphi(r)} (mod\, rs).$$

Аналогично, $r^{2\varphi(s)} \equiv r^{\varphi(s)} (mod\, rs)$. Поэтому

$$c_{a,b} c_{a',b'} = (as^{\varphi(r)} + br^{\varphi(s)})(a's^{\varphi(r)} + b'r^{\varphi(s)})$$

$= aa's^{\varphi(r)} + bb'r^{\varphi(s)} + (ab' + a'b)s^{\varphi(r)}r^{\varphi(s)})$
$= \alpha s^{\varphi(r)} + \beta r^{\varphi(s)} (mod\ rs).$

Теперь можно непосредственно приступить к доказательству (4) и (5). Из (6) и (7) следует, что множество $\mathbb{Z}_{rs}^*$ совпадает с множеством смежных классов $\overline{c_{a,b}} = c_{a,b} + rs \cdot \mathbb{Z}; a \in G_r, b \in G_s$. Группа $\mathbb{Z}_r^* \times \mathbb{Z}_s^*$ состоит из пар $(\overline{u}, \overline{v})$ таких, что $\overline{u} \in \mathbb{Z}_r^*$ и $\overline{v} \in \mathbb{Z}_s^*$, с умножением $(\overline{u}_1, \overline{v}_1)\ (\overline{u}_2, \overline{v}_2) = (\overline{u}_1\overline{u}_2, \overline{v}_1\overline{v}_2)$. Рассмотрим отображение $f: \mathbb{Z}_r^* \times \mathbb{Z}_s^* \longrightarrow \mathbb{Z}_{rs}^*$, определяемое как $f((\overline{u}, \overline{v})) = \overline{c_{u,v}}$. Из (5) и равномощности множеств $\mathbb{Z}_r^* \times \mathbb{Z}_s^*$ и $\mathbb{Z}_{rs}^*$ следует, что отображение f биективно, т.е. взаимно однозначно. Учитывая (7), получаем

$$f((\overline{u}_1, \overline{v}_1)\ (\overline{u}_2, \overline{v}_2)) = f\big((\ \overline{u}_1\overline{u}_2, \overline{v}_1\overline{v}_2)\big)$$
$$= \overline{c_{u_1u_2, v_1v_2}} = \overline{c_{u_1u_2}}\ \overline{c_{v_1v_2}} = f((\overline{u}_1, \overline{v}_1))f((\overline{u}_2, \overline{v}_2)).$$

Другими словами, $f -$ изоморфизм. Остаётся только доказать (5).

Пусть $(\overline{u}, \overline{v}) \in \mathbb{Z}_r^* \times \mathbb{Z}_s^*$ – любой элемент. Тогда, согласно теореме 21.9 $ord\ ((\overline{u}, \overline{v})) =$ НОК $[ord\ (\overline{u}), ord\ (\overline{v})]$. Так как $ord\ (\overline{u})$ и $ord\ (\overline{v}) -$ делители чисел $\lambda(r)$ и $\lambda(s)$ соответственно, то $ord\ ((\overline{u}, \overline{v}))$ – делитель числа НОК $[\lambda(r), \lambda(s]$. В тоже время равенство $ord\ ((\overline{u}, \overline{v})) =$ НОК $[\lambda(r), \lambda(s)]$ достигается для чисел u и v, являющихся примитивными элементами по модулям r и s соответственно. Так что имеет место (5). □

23.2. ***Следствие.*** *Пусть* $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ – *каноническое разложение числа* n. *Тогда* (9)

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{\alpha_1}}^* \times \dots \times \mathbb{Z}_{p_k^{\alpha_k}}^*,$$
$$\lambda(n) = \text{НОК}\ [\lambda(p_1^{\alpha_1}), \dots, \lambda(p_k^{\alpha_k})].$$

Таким образом, чтобы окончательно уточнить строение группы $\mathbb{Z}_n^*$ и установить формулу для функции $\lambda(n)$, достаточно исследовать случай $n = p^\alpha$.

23.3. ***Лемма.*** *Для любого неотрицательного целого числа* α *выполняются сравнения*

$x^{2^{\alpha+1}} \equiv 1(mod\ 2^{\alpha+3})$, *где* $x -$ *любое нечетное число*; (10)

$5^{2^\alpha} \equiv 1 + 2^{\alpha+2}\ (mod\ 2^{\alpha+3})$; (11)

$(1 + p)^{p^\alpha} \equiv 1 + p^{\alpha+1}(mod\ p^{\alpha+2})$, *где* $p -$ *любое нечетное простое число.* (12)

Доказательство (индукция по α). Для $\alpha = 0$ сравнения очевидны. Предположим, что каждое из указанных сравнений выполняется

для некоторого $\alpha = \beta \geq 0$. Тогда для подходящих $a, b, c, a_1, b_1, c_1 \in \mathbb{Z}$ имеем:

$$x^{2^{\beta+2}} = (1 + a\,2^{\beta+3})^2 = \left(1 + a_1\,2^{\beta+4}\right) \equiv 1\ (mod\ 2^{\beta+4});$$

$$5^{2^{\beta+1}} = \left(1 + 2^{\beta+2} + b\,2^{\beta+3}\right)^2 = 1 + 2^{\beta+3} + b2^{\beta+4} + b_1 2^{\beta+4}$$
$$\equiv 1 + 2^{\beta+3}\ (mod\ 2^{\beta+4});$$

$$(1+p)^{p^{\beta+1}} = (1 + p^{\beta+1}(1+cp))^p$$
$$= \sum_{i=0}^{p} \binom{p}{i} p^{(\beta+1)i}(1+cp)^i = 1 + p^{\beta+2} + c_1 p^{\beta+3}$$
$$\equiv 1 + p^{\beta+2}\left(mod\ p^{\beta+3}\right).$$

(В доказательстве сравнения (12) для $\alpha = 1$ необходимо учесть, что $\binom{p}{0} = \binom{p}{p} = 1$ и $\binom{p}{i} \equiv 0\ (mod\ p)$ при $1 \leq i \leq p-1$; затем доказательство для случая $\alpha \geq 2$ проводится по индукции.) Так что выполнение сравнений $(10) - (12)$ для $\alpha = \beta$ влечет их выполнение для $\alpha = \beta + 1$. □

23.4. ***Лемма*** Лагранжа. *Пусть p – простое число, а $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ – многочлен степени $n < p$ с целыми коэффициентами. Тогда, если сравнение*

$$f(x) \equiv 0\ (mod\ p\ ) \qquad (13)$$

имеет более чем n решений, то все коэффициенты многочлена $f(x)$ кратны p.

Доказательство. Пусть сравнение (13) имеет $n+1$ решений. Обозначая вычеты этих решений через $x_1, \ldots, x_{n+1}$, представим многочлен $f(x)$ в виде

$$f(x) = b_0 + \sum_{k=1}^{n} b_k (x - x_1)\ldots(x - x_k);\ b_0, \ldots, b_n \in \mathbb{Z}. \qquad (14)$$

Существование такого представления для подходящих чисел $b_0, \ldots, b_n \in \mathbb{Z}$ доказывается по индукции, учитывая, что

$$f(x) = b_n(x - x_1)\ldots(x - x_n) + g(x),\ b_n = a_n,$$

где $g(x) \in \mathbb{Z}[x]$ – некоторый многочлен степени $\leq n-1$. Полагая в (14) последовательно $x = x_1, \ldots, x_{n+1}$ и учитывая, что эти числа попарно несравнимы по модулю p, убеждаемся, что все b_k и, следовательно, все a_k кратны p. □

23.5. ***Следствие***. *Для любого простого числа p и любого $\tau \in \mathbb{N}$, $\tau < p$, сравнение $x^\tau \equiv 1\ (mod\ p)$ имеет не более τ решений.*

23.6. ***Лемма*** Гаусса [18]. *Для любого простого числа* p *группа* $\mathbb{Z}_p^*$ *является циклической.*

Доказательство. Мультипликативный порядок по модулю p любого элемента в $\mathbb{Z}_p^*$ является делителем числа $p-1$. Поэтому уравнение $x^{\lambda(p)} \equiv 1\ (mod\ p)$ имеет в $\mathbb{Z}_p^*$ $p-1$ решений, и, согласно следствию 23.5, $p-1 \leq \lambda(p)$. Поскольку $\lambda(n) \mid \varphi(n)$ и $\varphi(n) = p-1$, то $\lambda(n) = p-1$. Таким образом, в группе $\mathbb{Z}_p^*$, состоящей из $p-1$ элементов, имеется элемент порядка $p-1$, т.е. $\mathbb{Z}_p^*$ − циклическая группа**.** □

23.7. ***Лемма.*** *Пусть* $\alpha \in \mathbb{N}$. *Тогда*:

1) *Если* p − *нечетное простое число, то* $\mathbb{Z}_{p^\alpha}^*$ − *циклическая группа.*

2) *Группы* $\mathbb{Z}_2^*$ *и* $\mathbb{Z}_4^*$ − *циклические порядков* 1 *и* 2 *соответственно*; $\mathbb{Z}_{2^\alpha}^*$, $\alpha \geq 3$, − *прямое произведение циклической группы порядка* $2^{\alpha-2}$ *и циклической группы порядка* 2.

Доказательство. 1) Случай $\alpha = 1$ рассмотрен в лемме 23.6; поэтому пусть $\alpha > 1$. Покажем, что $\mathbb{Z}_{p^\alpha}^* = <\overline{u}\,\overline{v}>$, где $\overline{u} = u + p^\alpha\mathbb{Z}$, $u = a^{p^\alpha}$, a − первообразный корень по модулю p (согласно лемме 23.6 a существует); $\overline{v} = v + p^\alpha\mathbb{Z}$, $v = 1 + p$. Отметим, что $a^{p^{\alpha-1}} \equiv a\ (mod\ p)$ согласно следствию Малой теоремы Ферма; числа u^0, u^1, …, u^{p-2} попарно несравнимы по модулю p, а, следовательно, и по модулю p^α; $u^{p-1} = a^{(p-1)p^\alpha} = a^{\varphi(p^\alpha)} \equiv 1\ (mod\ p^\alpha)$ согласно теореме Эйлера. Поэтому $ord_{p^\alpha}(u) = p-1$. Согласно (12) имеем $v^{p^{\alpha-1}} \equiv 1\ (mod\ p^\alpha)$ и $v^{p^{\alpha-2}} \equiv 1 + p^{\alpha-1} \not\equiv 1 (mod\ p^\alpha)$. Поэтому $ord_{p^\alpha}(v) = p^{\alpha-1}$. Таким образом, элементы $\overline{u}$ и $\overline{v}$ порождают в $\mathbb{Z}_{p^\alpha}^*$ циклические подгруппы взаимно простых порядков $p-1$ и p^α. Согласно п. 1) тео-

---

[18] ***Иоганн Карл Фридрих Гаусс*** (30.04.1777−23.02.1855) − выдающийся немецкий математик. С его именем связаны фундаментальные исследования почти во всех основных областях математики, а также в аналитической и небесной механике, астрономии, физике и геодезии. Гаусса называли "королём математиков". Лемма 23.6 − частный случай теоремы 49.4 о цикличности мультипликативной группы любого конечного поля.

ремы 21.9 элемент $\overline{u}\,\overline{v}$ имеет порядок $(p-1)p^{\alpha}$, и, следовательно, порождает группу $\mathbb{Z}_{p^{\alpha}}^{*}$ (как имеющую тот же порядок).

2) Очевидно, что группы $\mathbb{Z}_{2^{\alpha}}^{*}$ при $\alpha = 1$ и 2 являются циклическими. Пусть $\alpha \geq 3$. Из (10) следует, что мультипликативный порядок любого нечетного числа по модулю 2^{α} является делителем числа $2^{\alpha-2}$. С другой стороны, согласно (11), $ord_{2^{\alpha}}5 = 2^{\alpha-2}$. Это означает, что $\mathbb{Z}_{2^{\alpha}}^{*}$ не является циклической группой, но смежный класс $5 + 2^{\alpha}\mathbb{Z}$ порождает в $\mathbb{Z}_{2^{\alpha}}^{*}$ циклическую подгруппу порядка $2^{\alpha-2}$ и индекса 2. Заметим, что $-1 + 2^{\alpha}\mathbb{Z} \notin < 5 + 2^{\alpha}\mathbb{Z} >$, поскольку обратное предположение приводит к противоречию:

$$5^{s} \equiv -1(\mathrm{mod}\ 2^{\alpha}) \Longrightarrow 5^{s} \equiv -1(\mathrm{mod}\ 4) \Longrightarrow 1 \equiv -1(\mathrm{mod}\ 4).$$

Следовательно, $\mathbb{Z}_{2^{\alpha}}^{*} = \{\overline{u}\,\overline{v} \mid \overline{u} \in < 5 + 2^{\alpha}\mathbb{Z} >, \overline{v} \in < -1 + 2^{\alpha}\mathbb{Z} >\} \cong < 5 + 2^{\alpha}\mathbb{Z} > \times < -1 + 2^{\alpha}\mathbb{Z} >$. □

23.8. ***Следствие.*** *Группа* $\mathbb{Z}_{n}^{*}$ *является циклической тогда и только тогда, когда целое число* $n > 1$ *имеет вид*

$$2,\ 4,\ p^{\alpha} \text{ или } 2p^{\alpha}, \text{ где } p - \text{нечетное простое число}, \alpha \in \mathbb{N}. \qquad (15)$$

23.9. ***Следствие*** (Теорема Кармайкла). *Для любых взаимно простых чисел* $a \in \mathbb{Z}$, $n \in \mathbb{N}$

$$a^{\lambda(n)} \equiv 1\ (mod\ n),$$

где $\lambda(n)$ *вычисляется согласно формулам, указанным в теореме* 10.7.

Замечание. Для чисел n вида (15) имеет место равенство $\lambda(n) = \varphi(n)$. Во всех остальных случаях $\lambda(n)$ – собственный делитель числа $\varphi(n)$ и для них соотношение (16) уточняет теорему Эйлера. □

Глава IV. Комбинаторика. Элементы комбинаторного анализа

Основная задача комбинаторики – подсчет и перечисление элементов в конечных множествах. В современной комбинаторике наряду с перечислительными задачами рассматриваются также экстремальные задачи, проблемы существования, выбора и расположения комбинаторных объектов, теория матроидов и упорядоченных структур.

§ 24. Элементарные методы подсчёта

Правило суммы. Пусть X и Y – конечные множества. Тогда

$$|X \cup Y| = |X| + |Y| - |X \cap Y|;$$

в частности, если $|X \cap Y| = \emptyset$, то $|X \cup Y| = |X| + |Y|$.

Последняя формула в комбинаторике называется *правилом суммы*: если объект x можно выбрать n способами, а объект y – другими m способами, то выбор "либо x, либо y" можно реализовать $n + m$ способами. В общем случае имеем: если $X_1, X_2, \ldots, X_m$ – попарно непересекающиеся множества, т.е. $X_i \cap X_j = \emptyset$ при $i \neq j$, то

$$|X_1 \cup X_2 \cup \ldots \cup X_m| = \sum_{i=1}^{m} |X_i|.$$

Правило произведения. Для конечных множеств X и Y имеем

$$|X \times Y| = |X| \cdot |Y|.$$

Эта формула в комбинаторике называется *правилом произведения*: если объект x можно выбрать n способами, а объект $y - m$ способами (независимо от выбора x), то выбор упорядоченной пары $< x, y >$ можно реализовать $n \cdot m$ способами. В общем случае имеет место обобщенное правило произведения:

$$|X_1 \times X_2 \times \ldots \times X_m| = \prod_{i=1}^{m} |X_i|,$$

доказательство которого нетрудно провести, применяя индукцию по m.

Биективные соответствия. Пусть S и $T -$ конечные множества, между элементами которых можно установить взаимно однозначное соответствие. Тогда $|S| = |T|$. Это вполне очевидное утверждение позволяет свести решение перечислительной задачи для мно-

жества S к решению соответствующей перечислительной задачи для множества T.

Выборки (размещения и перестановки). Пусть дано
ство S из n элементов и

$$(a_1, a_2, \dots, a_m) \qquad (1)$$

– упорядоченный набор элементов S, не обязательно различных. Два набора $(a_1, a_2, \dots, a_m)$ и $(b_1, b_2, \dots, b_m)$ равны, если $a_i = b_i$. $i = 1, 2, \dots, m$. Набор (1) назовем *выборкой из S*, или *размещением из n элементов по m*. Число таких выборок обозначим через U_n^m. Согласно правилу произведения $U_n^m = n^m$.

Набор (1), у которого все компоненты различны, называется *перестановкой из n элементов по m*, или *размещением из n элементов по m без повторений*. Из обобщенного правила произведения следует, что число таких перестановок задается формулой

$$P_n^m = n(n-1)\dots(n-m+1).$$

Если $n = m$, то соответствующие перестановки называются просто *перестановками из n элементов*. Их число равно $P_n = P_n^n = n!$

Неупорядоченные выборки (сочетания). Неупорядоченные выборки вида (1), у которых все компоненты различны называются *сочетаниями из n элементов по m*. Сочетание – это любое m-элементное подмножество n-элементного множества. Число сочетаний из n по m обозначают через C_n^m (или через $\binom{n}{m}$). Из каждого сочетания $(a_1, a_2, \dots, a_m)$ путем перестановки компонент можно получить $m!$ перестановок. Поэтому

$$C_n^m = \frac{P_n^m}{m!} = \frac{n(n-1)\dots(n-m+1)}{m!} = \frac{n!}{m!\,(n-m)!}.$$

Отметим, что

$$C_n^m = C_n^{n-m}.$$

Весом вектора будем называть число его ненулевых компонент.

24.1. *Теорема.* *Число двоичных векторов длины n веса m равно C_n^m.*

Доказательство. Каждому вектору $v = (v_1, v_2, \dots, v_n)$, у которого $v_{i_1} = v_{i_2} = \dots = v_{i_m} = 1$ (а остальные v_i равны нулю) сопоставим сочетание $a = (a_{i_1}, a_{i_2}, \dots, a_{i_m})$ из m элементов множества $A = \{a_1, a_2, \dots, a_n\}$. Данное соответствие между указанными множествами двоичных векторов веса m и сочетаний из n по m является взаимно

однозначным. Отсюда следует, что число двоичных векторов длины n и веса m равно числу сочетаний из n по m, т.е. C_n^m. □

Пример. Биективное соответствие между двоичными векторами длины 4 веса 2 и сочетаниями из 4 по 2 выглядит следующим образом:

вектор	сочетание	вектор	сочетание
0011	a_3a_4	0110	a_2a_3
0101	a_2a_4	1010	a_1a_3
1001	a_1a_4	1100	a_1a_2

Обозначим через $\hat{C}_n^m$ число сочетаний из n элементов по m элементов с повторениями элементов.

24.2. ***Теорема***.

$$\hat{C}_n^m = C_{n+m-1}^m = \frac{(n+m-1)!}{m!\,(n-1)!}.$$

Доказательство. Каждому сочетанию $a = \left(a_{i_1}, a_{i_2}, \dots, a_{i_m}\right)$ из m элементов множества $A = \{a_1, a_2, \dots, a_n\}$ с повторениями сопоставим двоичный вектор $1^{k_1}01^{k_2}0\,\dots\,01^{k_n}$, где 1^k – сокращенная запись k единиц подряд, k_i – число букв a_i в сочетании a, $i = 1, 2, \dots, n$. Длина данного двоичного вектора равна $k_1 + k_2 + \cdots + k_n + n - 1 = n + m - 1$, а число единиц в векторе равно m. Указанное соответствие между сочетаниями из n элементов по m с повторениями и двоичными векторов длины $n + m - 1$ веса m является взаимно однозначным. Поэтому остаётся воспользоваться утверждением предыдущей теоремы. □

Пример. Биективное соответствие между сочетаниями из 4 элементов по 2 с повторениями и двоичными векторами выглядит следующим образом:

сочетание	вектор	сочетание	вектор
a_1a_1	11000	a_2a_3	01010
a_1a_2	10100	a_2a_4	01001
a_1a_3	10010	a_3a_3	00110
a_1a_4	10001	a_3a_4	00101
a_2a_2	01100	a_4a_4	00011

§ 25. Биномиальная формула

Рассмотрим произведение $(1 + x_1 t)(1 + x_2 t) \dots (1 + x_n t)$, где $x_1, x_2, \dots, x_n$ – формальные символы. Раскрывая скобки и располагая члены по степеням t, получим

$$t^n + (x_1 + x_2 + \cdots + x_n)t^{n-1} + (x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n)t^{n-2} + \cdots + x_1 x_2 \dots x_n,$$

или

$$t^n + a_1 t^{n-1} + a_2 t^{n-2} + \cdots + a_n t^1 + a_n,$$

где $a_1, a_2, \dots, a_n$ – *элементарные симметрические функции* от n переменных, определяемые приведенными выше выражениями. Число слагаемых каждого выражения a_i равно C_n^i. Следовательно, полагая $x_1 = x_2 = \cdots = x_n = 1$, получим

$$(1 + t)^n = \sum_{i=0}^{n} C_n^i t^i.$$

Это выражение для $(1 + t)^n$ называется *биномом Ньютона* [19], или *перечисляющей производящей функцией* сочетаний из n элементов, или просто *энумератором*. Числа сочетаний называют также *биномиальными коэффициентами*.

Полиномиальная формула.

$$(x_1 + x_2 + \cdots + x_m)^n = \sum_{n=n_1+n_2+\cdots+n_m} \frac{n!}{n_1!\, n_2! \dots n_m!} x_1^{n_1} x_2^{n_2} \dots x_m^{n_m},$$

где суммирование производится по всем упорядоченным разбиениям числа n на m слагаемых $n_1, n_2, \dots, n_m$.

---

[19] *Сэр* ***Исаак Ньютон*** (25.12.1642 – 20.03.1727) – выдающийся английский физик, математик, механик и астроном, один из создателей классической физики. Автор фундаментального труда «Математические начала натуральной философии», в котором он изложил закон всемирного тяготения и три закона механики, ставшие основой классической механики. Разработал дифференциальное и интегральное исчисления, теорию цвета, заложил основы современной физической оптики, создал многие другие математические и физические теории.

§ 26. Принцип включения и исключения

Пусть дано множество S из N элементов, всякому $a \in S$ приписан вес $w(a) \in F$, где F – некоторое поле. (Никаких ограничений на выбор поля F не накладывается, но во многих задачах веса полагают равными единице.) Пусть P обозначает некоторое множество из n свойств $P_1, P_2, \ldots, P_n$, которыми могут как обладать, так и не обладать элементы множества S. Пусть $W(P_{i_2}, P_{i_2}, \ldots, P_{i_k})$ обозначает суммарный вес элементов множества S, обладающих свойствами $P_{i_1}, P_{i_2}, \ldots, P_{i_k}$ (но, возможно, обладающих и некоторыми другими свойствами). Если таких элементов в множестве нет, то полагаем $W(P_{i_1}, P_{i_2}, \ldots, P_{i_k}) = 0$. Обозначим

$$W(k) = \sum_{1 \le i_1 < \ldots < i_k \le n} W(P_{i_1}, P_{i_2}, \ldots, P_{i_k}), \qquad (1)$$

где суммирование распространено на все подмножества $\{P_{i_1}, P_{i_2}, \ldots, P_{i_k}\}$ из k элементов множества свойств P. Полагаем также $W(0)$ равным сумме весов элементов множества S. Обозначим через $N(m)$ суммарный вес элементов множества S, удовлетворяющих в точности m свойствам.

26.1. ***Теорема*** (Принцип включении и исключения).

$$N(m) = \sum_{i=0}^{n-m} (-1)^i \binom{m+i}{m} W(m+i). \qquad (2)$$

В частности,

$$N(0) = \sum_{i=0}^{n} (-1)^i W(i) \qquad (3)$$
$$= W(0) - W(1) + W(2) - \cdots + (-1)^n W(n).$$

Доказательство. Пусть элемент $a \in S$, обладающий весом $w(a)$, удовлетворяет в точности k свойствам. Если $k < m$**,** то a даёт нулевой вклад в правую часть (2). Если $k = m$**,** то вклад a в правую часть (2) равен $w(a)$. Если $k > m$, то соответствующий вклад равен

$$w(a) \sum_{i=0}^{n-m} (-1)^i \binom{m+i}{m} \binom{k}{m+i}$$
$$= w(a) \sum_{i=0}^{r} (-1)^i \binom{k}{m} \binom{k-m}{k-(m+i)}$$

$$= w(a)\binom{k}{m}\sum_{i=0}^{n-m}(-1)^i\binom{k-m}{k-(m+i)}$$

$$= w(a)\binom{k}{m}\sum_{i=0}^{k-m}(-1)^i\binom{k-m}{(k-m)-i)}$$

$$= w(a)\binom{k}{m}\sum_{i=0}^{k-m}(-1)^i\binom{k-m}{i} = w(a)\binom{k}{m}(1-1)^{k-m} = 0.$$

Таким образом, правая часть (2) равна в точности сумме весов элементов множества S, удовлетворяет в точности m свойствам. □

Если каждому элементу множества S приписан вес, равный 1, то $W(0) = N$. Получающаяся при этом формула (3) называется *формулой решета*. Воспользуемся этой формулой для получения формулы для функции Эйлера $\varphi(n)$. Напомним, что функция Эйлера $\varphi(n)$, где n – натуральное число, есть число целых чисел k таких, что $0 < k \leq n$, НОД $(k, n) = 1$.

26.2. ***Лемма***. *Пусть* $a_1, a_2, \ldots, a_m$ *– попарно взаимно простые натуральные числа, т.е.* $(a_i, a_j) = 1$, $i \neq j$. *Тогда число целых чисел, таких, что* $0 < k \leq n$, $a_i \nmid n, i = 1,2, \ldots, m$, *равно*

$$n - \sum_{1\leq i\leq m}\left[\frac{n}{a_i}\right] + \sum_{1\leq i<j\leq m}\left[\frac{n}{a_i a_j}\right] - \cdots + (-1)^m\left[\frac{n}{a_1 a_2 \ldots a_m}\right]. \qquad (4)$$

Доказательство. Пусть S – множество натуральных чисел $1,2,\ldots,n$, а P_i – свойство числа означающее, что число из S делится на a_i без остатка, $i = 1,2, \ldots, m$. Так как числа a_i попарно взаимно просты, то количество чисел из S, взаимно простых с числом $a_{i_1} a_{i_2} \ldots a_{i_k}$ равно

$$W(P_{i_1}, P_{i_2}, \ldots, P_{i_k}) = \left[\frac{n}{a_{i_1} a_{i_2} \ldots a_{i_k}}\right].$$

Другими словами, с учетом формулы решета имеет место формула (4). □

26.3. ***Следствие***. *Пусть* $n \in \mathbb{N}$. *Тогда*

$$\varphi(n) = n\prod_p\left(1 - \frac{1}{p}\right),$$

где произведение распространено на все простые делители p *числа* n. *Другими словами, если* $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m}$ *– каноническое разложение числа на простые множители, то*

$$\varphi(n) = p_1^{\alpha_1-1}p_2^{\alpha_2-1} \dots p_m^{\alpha_{m-1}}(p_1-1)(p_2-1)\dots(p_m-1).$$

Доказательство. Достаточно применить предыдущую лемму, заменив a_i на p_i и учесть, что

$$n - \sum_{1\le i\le m}\left[\frac{n}{p_i}\right] + \sum_{1\le i<j\le m}\left[\frac{n}{p_ip_j}\right] - \dots + (-1)^m\left[\frac{n}{p_1p_2\dots p_m}\right]$$
$$= n\sum_{i=1}^{m}\left(1-\frac{1}{p_i}\right). \ \square$$

§ 27. Производящие функции и рекуррентные соотношения

Пусть имеется последовательность чисел

$$a_0, a_1, a_2, \dots, a_n, \dots \qquad (1)$$

С этой последовательностью будем связывать её *производящую функцию*, которую можно определить как формальный степенной ряд

$$A(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n + \dots = \sum_{i=0}^{\infty} a_ix^i \qquad (2)$$

Если ряд (2) сходится в круге радиуса $R > 0$, то может случиться, что свойства функции $A(x)$ позволят вычислить коэффициенты a_n или получить какую-либо другую информацию об этих коэффициентах.

Отметим некоторые свойства производящих функций**.** Пусть

$$B(x) = b_0 + b_1x + b_2x^2 + \dots + b_nx^n + \dots$$

− ещё одна производящая функция. $A(x)$ и $B(x)$ являются равными, если $a_n = b_n$ для всех $n = 0, 1, 2, \dots$ Сумма или разность $A(x)$ и $B(x)$ определяются равенствами

$$\sum_{i=0}^{\infty}(a_i \pm b_i)x^i,$$

а их произведение задаётся формулой

$$A(x)B(x) = \sum_{i=0}^{\infty}\sum_{j=0}^{i}\left(a_jb_{i-j}\right)x^i.$$

Отношение $C(x) = A(x)/B(x)$ имеет место тогда и только тогда, когда $C(x)B(x) = A(x)$. Если отношение $A(x)/B(x)$ существует, то оно всегда единственно, так как если $C(x)B(x) = D(x)B(x)$, то $(C(x) - D(x))B(x) = 0$, и, как нетрудно проверить, $B(x) = 0$, либо $C(x) = D(x)$. Если $a_0 = 0$, то $A(x)B(x) = 0\ mod\ x$ при любом $B(x)$**,** и урав-

нение $A(x)B(x) = 1$ не разрешимо относительно $B(x)$. Если $a_0 \neq 0$, то

$$\frac{A(x)}{a_0} = 1 + \sum_{i=1}^{\infty} \frac{a_i}{a_0} x^i$$

и

$$\frac{a_0}{A(x)} = \frac{1}{1 + \sum_{i=1}^{\infty} \frac{a_j}{a_0} x^i} = \sum_{n=0}^{\infty} \left[- \sum_{i=1}^{\infty} \frac{a_i}{a_0} x^i \right]^n .$$

Следовательно,

$$\frac{1}{A(x)} = \frac{1}{a_0} \sum_{n=0}^{\infty} \left[- \sum_{i=1}^{\infty} \frac{a_i}{a_0} x^i \right]^n .$$

Так что производящая функция имеет мультипликативную обратную тогда и только тогда, когда $a_0 \neq 0$.

Замечание. Указанные свойства производящих функций не зависят от сходимости или расходимости ряда (2) при некоторых значениях x. Коэффициенты a_i не обязательно должны быть действительными или комплексными числами. Производящие функции можно рассматривать над любым полем. □

Для производящей функции (2) можно определить её формальную производную

$$A'(x) = \sum_{i=1}^{\infty} i a_i x^{i-1},$$

причем для формальной производной выполняются свойства обычной производной. Отличие состоит лишь в том, что формальная производная не связана с предельным переходом.

Производящие функции можно использовать, например, для решения линейных рекуррентных соотношений с постоянными коэффициентами. Последовательность (1) удовлетворяет *линейному рекуррентному соотношению с постоянными коэффициентами порядка* r, если

$$a_{n+r} = c_1 a_{n+r-1} + c_2 a_{n+r-2} + \cdots + c_r a_n, n = 0, 1, 2, ..., \qquad (3)$$

где c_i, $i = 1, 2, ..., r$, $c_r \neq 0$ – постоянные, причем $c_r \neq 0$. Тогда, если $A(x)$ – производящая функция последовательности (1) и если через $k(x)$ обозначен многочлен

$$k(x) = 1 - c_1 x - c_2 x^2 - \cdots - c_r x^r, \qquad (4)$$

то

$$A(x)k(x) = d_0 + d_1x + \cdots + d_{r-1}x^{r-1} = D(x), \qquad (5)$$

где $D(x)$ – многочлен степени не выше $r-1$. Действительно, если d_{n+r} – коэффициент при x^{n+r} в (5), то $d_{n+r} - a_{n+r} - c_1a_{n+r-1} - c_2a_{n+r-2} - \cdots - c_ra_n = 0$.

Таким образом, для последовательности (1), удовлетворяющей линейному рекуррентному соотношению (3) производящая функция $A(x)$ есть рациональная функция

$$A(x) = \frac{D(x)}{k(x)}.$$

С линейным рекуррентным соотношением (3) мы связываем характеристический многочлен

$$f(x) = x^r - c_1x^{r-1} - \cdots - c_r. \qquad (6)$$

Многочлен $f(x)$ имеет r корней и разлагается на линейные множители

$$f(x) = (x-\alpha_1)^{e_1} \ldots (x-\alpha_s)^{e_s},\ e_1 + \cdots + e_s = r, \qquad (7)$$

где $\alpha_1,\ldots,\alpha_s$ – корни многочлена $f(x)$, а $e_1, \ldots, e_s$ – их кратности. Сравнивая многочлены (4) и (6), мы видим, что

$$k(x) = x^r f\left(\frac{1}{x}\right). \qquad (8)$$

Ввиду (7) и (8) получаем следующее разложение многочлена $k(x)$:

$$k(x) = (1-\alpha_1x)^{e_1} \ldots (1-\alpha_sx)^{e_s},\ \ e_1 + \cdots + e_s = r.$$

Теперь рациональную функцию $A(x) = \frac{D(x)}{k(x)}$ можно выразить в виде суммы простых дробей

$$A(x) = \frac{D(x)}{k(x)} = \sum_{i=1}^{s}\sum_{k=1}^{e_i} \frac{\beta_{ik}}{(1-\alpha_ix)^k}. \qquad (9)$$

Таким образом, формула (9) позволяет выразить $A(x)$ в виде суммы функций вида

$$\beta(1-\alpha x)^{-k}. \qquad (10)$$

Разлагая выражение (10) по формуле бинома, получаем

$$\beta(1-\alpha x)^{-k} = \beta\left(1 + \frac{(-k)(-\alpha x)}{1!} + \cdots + \frac{(-k)\ldots(-k-n+1)(-\alpha x)^n}{n!} + \cdots\right),$$

причем в этом выражении коэффициент при x^n равен

$$\frac{\beta(n+k-1)\ldots k}{n!}\alpha^n = \beta\binom{n+k-1}{n}\alpha^n = \beta\binom{n+k-1}{k-1}\alpha^n,$$

где $\binom{n}{m}$ – число сочетаний из n элементов по m. Поэтому

$$\sum_{k=1}^{e_i} \beta_{ik} \binom{n+k-1}{k-1} \alpha_i^n = P_i(n)\alpha_i^n,$$

где $P_i(n)$ – многочлен от n степени не выше $e_i - 1$, причем такой многочлен может быть получен соответствующим выбором постоянных β_{ik}. Но тогда (9) можно записать в виде

$$A(x) = \sum_{n=0}^{\infty} a_n x^n = \sum_{n=0}^{\infty} \sum_{i=1}^{s} P_i(n)\alpha_i^n x^n .$$

Сравнивая коэффициенты при x^n, получаем

$$a_n = \sum_{i=1}^{s} P_i(n)\alpha_i^n,$$

где степень $P_i(n)$ не выше $e_i - 1$.

Полученный результат сформулируем в виде теоремы.

27.1. *Теорема.* *Пусть последовательность $a_0, a_1, a_2, \ldots$ удовлетворяет линейному рекуррентному соотношению с постоянными коэффициентами*

$$a_{n+r} = c_1 a_{n+r-1} + c_2 a_{n+r-2} + \cdots + c_r a_n,\ n \geq 0,\ c_r \neq 0,$$

Назовём $f(x) = x^r - c_1 x^{r-1} - \cdots - c_r$ характеристическим многочленом данного рекуррентного соотношения, и пусть

$$f(x) = (x - \alpha_1)^{e_1} \ldots (x - \alpha_s)^{e_s},\ e_1 + \cdots + e_s = r,$$

– разложение $f(x)$ на линейные множители. Тогда

$$a_n = \sum_{i=1}^{s} P_i(n)\alpha_i^n$$

для всех n, где $P_i(n)$ – многочлен от n степени не выше $e_i - 1$. Коэффициенты многочлена $P_i(n)$ определяются начальными значениями $a_0, a_1, \ldots, a_{r-1}$ последовательности $\{a_n\}$.

С помощью производящих функций можно находить решения и для некоторых рекуррентных соотношений, не являющихся линейными.

Числа Каталана. Рассмотрим задачу о числе способов образования бинарного неассоциативного произведения n сомножителей

$x_1, x_2, \ldots, x_n$. Искомое число способов обозначим через u_n (эти числа называют *числами Каталана* [20]) Для $n = 2, 3$ и 4 существуют следующие возможности:

$n = 2$	x_1x_2.
$n = 3$	$x_1(x_2x_3)$, $(x_1x_2)x_3$.
$n = 4$	$x_1(x_2(x_3x_4))$, $x_1((x_2x_3)x_4)$, $(x_1x_2)(x_3x_4)$, $(x_1(x_2x_3))x_4$, $((x_1x_2)x_3)x_4$.

(11)

Видим, что $u_2 = 1$, $u_3 = 2$, $u_4 = 5$. Естественно также считать, что $u_1 = 1$. Последовательность $x_1x_2\ldots x_n$ с некоторой расстановкой скобок получается как композиция некоторого произведения $x_1x_2\ldots x_r$ и некоторого произведения $x_{r+1}x_{r+2}\ldots x_n$ для какого-либо $r = 1, \ldots, n-1$: $x_1x_2\ldots x_n = (x_1x_2\ldots x_r)(x_{r+1}\ldots x_n)$. В произведении $x_1x_2\ldots x_r$ скобки могут быть расставлены u_r способами, а в $x_{r+1}\ldots x_n$ $- u_{n-r}$ способами. Поэтому с учетом правил произведения и суммы получаем, что

$$u_n = u_1u_{n-1} + u_2u_{n-2} + \cdots + u_{n-1}u_1, n \geq 2. \quad (12)$$

Запишем производящую функцию для последовательности u_n в виде

$$u(x) = u_1x + u_2x^2 + \cdots + u_nx^n + \cdots, \quad (13)$$

оставляя временно в стороне вопрос о сходимости данного ряда. Из (12) следует, что

$$(u(x))^2 = -x + u(x). \quad (14)$$

Решая (4) как квадратное уравнение относительно $u(x)$, получаем

$$u(x) = \frac{1 - \sqrt{1 - 4x}}{2}, \quad (15)$$

где перед $\sqrt{1 - 4x}$ берём знак минус, так как $u(x)$ не имеет свободного члена. Разлагая правую часть выражения (15) в ряд по степеням x, найдём коэффициент u_n при x^n:

$$u_n = \frac{\left(\frac{1}{2}\right)\left(-\frac{1}{2}\right)\ldots\left(\frac{3-2n}{2}\right)(-4)^n\left(-\frac{1}{2}\right)}{n!} = \frac{(2n-2)!}{n!(n-1)!}$$

$$= \frac{1}{2n-1}\binom{2n-1}{n} = \frac{1}{n}\binom{2n-2}{n-1}.$$

---

[20] ***Эжен Шарль Каталан*** (30.05.1814−14.02.1894) − бельгийский математик.

С вычисленным значением u_n ряд (13) сходится при $|\ x\ | < \frac{1}{4}$, и для этих значений выполняется равенство (15) и имеет место рекуррентное соотношение (13). Заметим, что доказать сходимость ряда (13), опираясь только на соотношение (12), чрезвычайно сложно.

§ 28. Обращение Мёбиуса на частично упорядоченных множествах

28.1. Исходные понятия

Частично упорядоченным множеством называется система $\Sigma = (P, \preccurlyeq)$ из элементов множества P с заданными на нём *отношением частичного порядка* $x \preccurlyeq y$ для некоторых пар $(x,\ y) \in P \times P$ и отношением равенства $x = y$, удовлетворяющих для любых $x, y, z \in P$ следующим аксиомам:

P1. (*Рефлективность*.) $x \preccurlyeq x$;

P2. (*Антисимметричность*.) $x \preccurlyeq y\ \&\ y \preccurlyeq x \Rightarrow x = y$;

P3. (*Транзитивность*.) $x \preccurlyeq y\ \&\ y \preccurlyeq z \Rightarrow x \preccurlyeq z$.

Запись $x \preccurlyeq y$ обычно читается как $''x$ меньше или равно y''. Если $x \preccurlyeq y$ и $x \neq y$, то будем писать $x \prec y$; запись $x \not\preccurlyeq y$ означает, что отношение $x \preccurlyeq y$ не имеет места.

Если дополнительно к P1– P3 выполняется аксиома

P4. (*Линейность*.) $x \preccurlyeq y \vee y \preccurlyeq x$ (при $x \neq y$ верно одно из двух: либо $x \prec y$, либо $x \prec y$), то Σ называется *линейно упорядоченным множеством*, или *цепью*.

Частично упорядоченные множества $\Sigma_1 = (P_1, \preccurlyeq_1)$ и $\Sigma_2 = (P_2, \preccurlyeq_2)$ называются *изоморфными* (этот факт записывается как $\Sigma_1 \cong \Sigma_2$), если существует биекция $\varphi\colon P_1 \to P_2$, сохраняющая отношение порядка, т.е.

$$x \preccurlyeq_1 y \Leftrightarrow\ \varphi(x) \preccurlyeq_2 \varphi(y),\ \ \forall x, y \in P_1.$$

Другими словами, изоморфные частично упорядоченные множества отличаются друг от друга лишь обозначениями элементов и обозначениями отношения порядка.

Прямым произведением частично упорядоченных множеств $\Sigma_1 = (P_1, \preccurlyeq_1)$ и $\Sigma_2 = (P_2, \preccurlyeq_2)$ называется частично упорядоченное множество $\Sigma = \Sigma_1 \times \Sigma_2 = (P, \preccurlyeq)$ такое, что

а) $P = P_1 \times P_2 = \{(x, y) |\ x \in P_1, y \in P_2\}$,

б) $(x_1, y_1) \preccurlyeq (x_2, y_2)$ тогда и только тогда, когда $x_1 \preccurlyeq_1 x_2$ и $y_1 \preccurlyeq_2 y_2$.

Сегментом (или *интервалом*) $[x, y]$ называется множество всех $z \in P$ таких, что $x \preccurlyeq z \preccurlyeq y$. Частично упорядоченное множество называется *локально конечным*, если каждый его сегмент состоит из конечного числа элементов.

Элемент $x \in P$ называется *нулевым* (соответственно, *единичным*), если $x \preccurlyeq y$ (соответственно, $y \preccurlyeq x$) при любом $y \in P$. Множество P может и не иметь нулевого (единичного) элемента, но, как следует из аксиомы P2, если такой элемент существует, то он является единственным. Очевидно, что для любого частично упорядоченного множества P и любых $x, y \in P$ таких, что $x \preccurlyeq y$, *индуцированное* множество $\Sigma_{x,y}^{P} = ([x, y], \preccurlyeq)$ является частично упорядоченным с нулевым элементом x и единичным элементом y.

Частично упорядоченные множества с небольшим числом элементов удобно изображать с помощью *диаграмм Хассе* [21]. В такой диаграмме элементы $x, y \in P$ изображаются точками, причём точка y помещается выше x, если $x \preccurlyeq y$; точка x соединяется линией с точкой y, если $[x, y] = \{x, y\}$.

28.2. Примеры частичных упорядочений

(1) *Естественный порядок на множестве целых чисел*. Множества: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{N}_{n+1} = \{0, 1, \dots, n\}$ с обычным отношением порядка ($x \leq y$ тогда и только тогда, когда $y - x$ неотрицательно) являются линейно упорядоченными множествами. Первые три множества не имеют ни нулевого, ни единичного элементов; элемент 1 является нулевым в $\mathbb{N}$, а единичный отсутствует; 0 и n – нулевой и единичный элементы в $\mathbb{N}_{n+1}$.

(2) *Упорядочение по включению*. Пусть S − некоторое множество, а $\mathcal{P} = P(S)$ − множество всех подмножеств множества S. Структура $\Sigma_S = (\mathcal{P}, \subseteq)$, где символ $\subseteq$ имеет обычный теоретико-

---

[21] ***Хельмут Хассе*** (25.08.1898 — 26.12.1979) — немецкий математик. Основные труды по алгебраической теории чисел, работы о локальной дзета-функции.

множественный смысл (включения одного множества в другое), является частично упорядоченной. Элементы $\emptyset$ (пустое множество) и S являются соответственно нулевым и единичным элементами в Σ_S.

Отметим также, что ″подсистемы″ (подполугруппы, подгруппы, подкольца, подполя, подпространства) ″математических систем″ (полугрупп, групп, колец, полей, пространств), упорядоченные по включению, образуют частично упорядоченные множества.

(3) *Упорядочение по делимости*. Пусть запись $a \mid b$ означает $″a$ делит $b″$, или, что то же самое, $″ b$ делится на a без остатка″. Тогда структуры $\Sigma = (\mathbb{N}, \mid)$ и $\Sigma_n = (D_n, \mid)$, где $D_n = \{1, \dots, n\}$, являются частично упорядоченными.

Диаграмма Хассе структуры $(D_{10}, \mid)$, представлена на рис.3. Элемент 1 является нулевым в Σ и Σ_n.

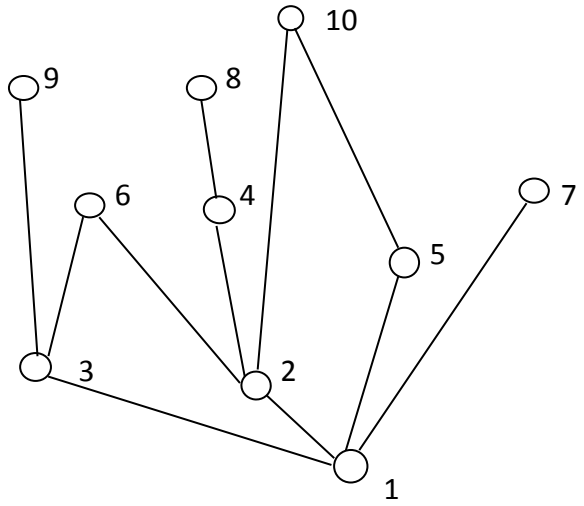

Рис. 3. Диаграмма Хассе частично-упорядоченного множества $(D_{10}, \mid)$.

Аналогично, рассматривая делимость многочленов в том или ином кольце многочленов, можно указать частично упорядоченные множества многочленов, например, $(\mathbb{Z}[x], \mid)$, $(\mathbb{F}_q[x], \mid)$.

28.3. Обращение Мёбиуса

Пусть $P -$ локально конечное частично упорядоченное множество, K – коммутативное ассоциативное кольцо с единицей (пусть 0 и 1 – нуль и единица этого кольца). Обозначим через $A = A(P, K)$ множество всех двуместных функций $f: P \times P \to K$, для которых $f(x, y) = 0$, если $x \not\leqslant y$. На множестве A введём

а) операцию *сложения функций*, полагая $h = f + g$, если $h(x, y) = f(x, y) + g(x, y), \quad \forall x, y \in P$;

б) операцию *умножения функций на скаляр* $c \in K$,
полагая $h = cf$, если $h(x,y) = c \cdot f(x,y), \quad \forall x, y \in P$;
и, наконец,

в) операцию *произведения-свертки функций* (эту операцию называют *произведением Шура* [22]), полагая $h = f \circ g$, если

$$h(x,y) = \sum_{z \in [x,y]} f(x,z)g(z,y)\,, \forall x, y \in P,$$

где суммирование ведётся по всем z из сегмента $[x,y]$; при $x \not\leqslant y$ сегмент пуст, в этом случае полагаем $h(x,y) \equiv 0$. Отметим, что произведение $f \circ g$ определено корректно, поскольку рассматриваемая сумма конечна ввиду локальной конечности множества P.

Очевидно, что множество A замкнуто относительно введённых операций. Произведение $'' \circ ''$ ассоциативно и дистрибутивно, но, вообще говоря, некоммутативно. Если $K -$ поле, то $A(P,K) -$ ассоциативная алгебра над K, которую называют *алгеброй инцидентности* множества P. Обычно рассматривают случай, когда $K = \mathbb{R} -$ поле действительных чисел.

Единицей в A является *дельта-функция Кронекера*

$$\delta(x,y) = \begin{cases} 1, & \text{если } x = y, \\ 0, & \text{если } x \neq y, \end{cases}$$

поскольку $\delta \circ f = f \circ \delta = f$ для любой $f \in A$. Функцию $f_{\text{л}}^{-1} \in A$ (при условии, что такая функция существует) назовём *левой обратной* к функции $f \in A$, если $f_{\text{л}}^{-1} \circ f = \delta$. Аналогично определяется *правая обратная* функция $f_{\text{пр}}^{-1}$: $f \circ f_{\text{пр}}^{-1} = \delta$. Если функция f имеет как левую обратную функцию $f_{\text{л}}^{-1}$, так и правую обратную функцию $f_{\text{пр}}^{-1}$, то $f_{\text{л}}^{-1} = f_{\text{пр}}^{-1}$. Действительно,

$$f_{\text{л}}^{-1} \circ \left(f \circ f_{\text{пр}}^{-1}\right) = \left(f_{\text{л}}^{-1} \circ f\right) \circ f_{\text{пр}}^{-1} \Rightarrow f_{\text{л}}^{-1} \circ \delta = \delta \circ f_{\text{пр}}^{-1} \Rightarrow f_{\text{л}}^{-1} = f_{\text{пр}}^{-1}.$$

---

[22] ***Исайа Шур*** (10.01.1875 – 10.01.1941) – выдающийся белорусский алгебраист, работавший в Германии и Израиле. Основные работы Шура относятся к теории групп, в первую очередь теории представлений и теории линейных групп, теории матриц, алгебраической теории чисел и теории степенных рядов.

Если $f^{-1} \circ f = f \circ f^{-1} = \delta$, то функцию f^{-1} будем называть *обратной* к f. Очевидно, если функция f^{-1} существует, то она определяется однозначно.

28.1. ***Лемма.*** (Об обратной функции). *Функция* $f \in A(P, K)$ *имеет обратную тогда и только тогда, когда*

$$a_x \equiv f(x, x) \neq 0 \text{ для любого } x \in P. \qquad (1)$$

Доказательство. Предположим, что обратная функция f^{-1} существует. Тогда

$$f^{-1}(x, x) \circ f(x, x) = f^{-1}(x, x) \cdot f(x, x) = \delta(x, x) = 1,$$
$$f(x, x) \circ f^{-1}(x, x) = f(x, x) \cdot f^{-1}(x, x) = \delta(x, x) = 1.$$

Отсюда следует, что выполнение условия (1) необходимо.

Предположим теперь, что условие (1) выполнено. Покажем, что функции $f_{\text{л}}^{-1}$ и $f_{\text{пр}}^{-1}$ могут быть построены рекуррентно. Поскольку в этом случае $f_{\text{л}}^{-1} = f_{\text{пр}}^{-1} = f^{-1}$, то утверждение леммы будет доказано. Ограничимся построением функции $f_{\text{л}}^{-1}$, так как для построения $f_{\text{пр}}^{-1}$ может быть применен аналогичный подход.

Во-первых, для сегмента $[x, y]$, состоящего из одного элемента x, имеем $f_{\text{л}}^{-1}(x, x) = a_x^{-1}$. Далее, предположим, что мы умеем вычислять значение $f_{\text{л}}^{-1}(x, y)$ в том случае, когда длина (число элементов) сегмента $[x, y]$ не превосходит m. Покажем, что значение $f_{\text{л}}^{-1}(x, y)$ можно определить тогда и для сегмента длины $m + 1$. Другими словами, докажем существование $f_{\text{л}}^{-1}(x, y)$ по индукции.

Пусть $x \neq y$ и длина сегмента $[x, y]$ равна $m + 1$. Тогда

$$f_{\text{л}}^{-1}(x, y) \circ f(x, y) = \sum_{z \in [x,y]} f_{\text{л}}^{-1}(x, z) \cdot f(z, y) = \delta(x, y) = 0,$$

и, следовательно,

$$f_{\text{л}}^{-1}(x, y) f(y, y) = - \sum_{z:\, x \preccurlyeq z \prec y} f_{\text{л}}^{-1}(x, z) \cdot f(z, y),$$

или

$$f_{\text{л}}^{-1}(x, y) = - a_y^{-1} \sum_{z:\, x \preccurlyeq z \prec y} f_{\text{л}}^{-1}(x, z) \cdot f(z, y).$$

Так как при $z \prec y$ длина сегмента $[x, z]$ не превосходит m, то все слагаемые в правой части последнего выражения известны. Поэтому значение может быть вычислено. Для правой обратной функции аналогом последнего соотношения будет

$$f_{\text{пр}}^{-1}(x,y) = -\,a_x^{-1} \sum_{z:\, x \prec z \preccurlyeq y} f_{\text{пр}}^{-1}(x,z)\cdot f(z,y)\,. \quad \square$$

Определим теперь *дзета-функцию* $\zeta(x,y) \in A(P,K)$, полагая

$$\zeta(x,y) = \begin{cases} 1, & \text{если } x \preccurlyeq y, \\ 0, & \text{если } x \not\preccurlyeq y. \end{cases}$$

Функция $\mu(x,y) \in A(P,K)$, обратная к ζ, называется *функцией Мёбиуса* множества P.

Из леммы об обратной функции вытекает

28.2. ***Следствие.*** Для любых $x, y \in P$, $x \preccurlyeq y$, имеют место равенства

1) $\mu(x,x) = 1$,

2) $\mu(x,y) = -\sum\limits_{z:\, x \preccurlyeq z \prec y} \mu(x,z)$,

3) $\mu(x,y) = -\sum\limits_{z:\, x \prec z \preccurlyeq y} \mu(z,y)$;

4) $\sum\limits_{z:\, x \preccurlyeq z \preccurlyeq y} \mu(z,y) = \delta(x,y) = \begin{cases} 1, \text{если } x = y, \\ 0, \text{если } x \prec y. \end{cases}$

28.3. ***Теорема*** (Об обращении Мёбиуса). *Пусть P – локально конечное частично упорядоченное множество с нулевым элементом $\emptyset$, K – коммутативное ассоциативное кольцо с единицей, $\mu(x,y)$ – функция Мёбиуса множества P, $f(x)$, $g(x)$ – функции, определённые для всех $x \in P$ и принимающие значения из K. Тогда, если*

$$f(x) = \sum_{y \in [\emptyset, x]} g(y)\,, \qquad \forall x \in P, \tag{2}$$

то

$$g(x) = \sum_{y \in [\emptyset, x]} f(y)\mu(y,x),\ \forall x \in P. \tag{3}$$

Доказательство. Так как каждый сегмент $[\emptyset, x]$ конечен, то суммы в (2) и (3) определены корректно. Для фиксированного x рассмотрим сумму

$$S = \sum_{y \in [\emptyset, x]} f(y)\mu(y,x) = \sum_{y \in [\emptyset, x]} \left(\sum_{z \in [\emptyset, y]} g(z) \right) \mu(y,x)$$

$$= \sum_{z \in [\emptyset, x]} g(z) \sum_{y \in [\mathrm{z}, x]} \mu(y,x),$$

где значение $f(y)$ заменено на $\sum_{z\in[\emptyset,y]} g(z)$. Учитывая, что

$$\sum_{y\in[\emptyset,x]}\ \sum_{z\in[\emptyset,y]} g(z)\,\mu(y,x) = \sum_{z\in[\emptyset,x]}\ \sum_{y\in[\mathrm{z},x]} g(z)\mu(y,x)$$

и $\sum_{y\in[\mathrm{z},x]} \mu(y,x) = 0$ при $z \neq x$, получаем

$$S = g(x) + \sum_{z\in[\emptyset,x],z\neq x} g(z) \sum_{y\in[\mathrm{z},x]} \mu(y,x)$$

$$= g(x) + \sum_{z\in[\emptyset,x],z\neq x} g(z)\cdot 0 = g(x).$$

Так как $S = g(x)$, то утверждение теоремы доказано. □

Определим теперь функцию Мёбиуса для двух частных случаев частичных упорядочений, рассмотренных выше.

1. ***Упорядочение по включению***. Пусть S – некоторое множество, $\Sigma_S = (\mathcal{P}, \subseteq)$ – частично упорядоченное множество $\mathcal{P} = P(S)$ всех подмножеств множества S по отношению включения $\subseteq$.

28.4. ***Теорема.*** Для любых подмножеств x, y множества S таких, что $x \subseteq y$, $\mu(x,y) = (-1)^{|y|-|x|}$, где $|z|$ – число элементов в z.

Доказательство. Утверждение справедливо, если $|y| - |x| = 0$ или 1. Допустим по индукции, что формула верна при $|y| - |x| = r - 1$, и докажем, что формула верна и при $|y| - |x| = r$. Тогда равенство 2) в следствии 28.2 принимает вид

$$\mu(x,y) = -\sum_{z:\, x\subseteq z\subset y} \mu(x,z) = -\sum_{j=0}^{r-1} C_r^j\,(-1)^j,$$

поскольку существует C_r^j подмножеств z таких, что $x \subseteq z \subset y$ и $|z| - |x| = j$ (z получается из x присоединением j из r элементов y, не входящих в x). Так как значение

$$-\sum_{j=0}^{r-1} C_r^j\,(-1)^j = -\left(\sum_{j=0}^{r} C_r^j\,(-1)^j - (-1)^r\right) = -((1-1)^r - (-1)^r)$$

равно $(-1)^r$, то $\mu(x,y) = (-1)^r$, а это и требовалось доказать. □

Пусть $S = \{1, 2, \ldots, n\}$ – множество чисел, которым сопоставлены свойства $P(1), P(2), \ldots, P(n)$. Пусть N – множество из m элементов, каждый из которых обладает свойствами $P(i)$, $i \in x$, для некоторого подмножества $x \subseteq S$. Пусть $f(x)$ – число элементов множества N, имеющих в точности свойства $P(i)$, $i \notin x$. (Здесь x – фиксированное подмножество в S.) Тогда, если положить

$$g(x) = \sum_{y \leqslant x} f(y),$$

то $g(x)$ – это число элементов N, имеющих все свойства $P(i)$ для $i \notin x$, и, быть может, еще и другие свойства. При $x = S$ формула обращения принимает вид

$$f(S) = g(S) + \sum_{j=1}^{n} (-1)^j \sum_{|y|=n-j} g(y)\,. \qquad (4)$$

Учитывая найденное выражение для μ, заключаем, что формула (4) есть принцип включения и исключения.

2. ***Упорядочение по отношению делимости. Теоретико-числовая формула обращения Мебиуса***. Пусть $P = (\mathbb{N}, \leqslant)$ – частично упорядоченное множество натуральных чисел, где $x \leqslant y$ (или $x \mid y$) означает, что x делит y (y делится на x без остатка). Если $x \leqslant z \leqslant y$, то $z = dx$, где $d \mid \frac{y}{x}$ и, следовательно, элементы отрезка $[x, y]$ образованы всевозможными делителями числа $\frac{y}{x}$. Число 1 является нулевым элементом множества P. Сравнение равенства 2) в следствии 28.2 с равенством

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1, \text{если } n = 1, \\ 0, \text{если } n > 1 \end{cases}$$

в лемме 13.1 показывает, что $\mu(x, y) = \mu\left(\frac{y}{x}\right)$. Другими словами, теорема 13.2 о теоретико-числовом обращении Мебиуса является частным случаем теоремы 28.4 для множества натуральных чисел, упорядоченных отношением делимости.

§ 29. Теория перечисления Пойа

Значительная часть комбинаторного анализа связана с решением перечислительных задач: подсчетом числа элементов множеств заданного типа. Технические трудности, связанные с получением формул для числа рассматриваемых комбинаторных объектов, часто могут быть преодолены использованием метода производящих функций. Однако многие трудности носят, скорее всего, не технический, а принципиальный характер. Это связано с тем, что, казалось бы, разные объекты приходится рассматривать как одинаковые. Возникает

это тогда, когда на множестве объектов задано отношение эквивалентности, и необходимо перечислять не число объектов, а число классов эквивалентности. Другой тип трудностей состоит в том, что перечисляемые объекты могут иметь разные веса. При этом требуется перечислить классы эквивалентности с заданным весом.

Все аспекты перечисления – комбинаторные конфигурации, заданные как отображения одних множеств в другие, производящие функции, эквивалентности, порождаемые группами, и веса встречаются в теореме перечисления Пойа. Эта фундаментальная теорема занимает центральное место в перечислительной теории.

29.1. Действие группы на множестве. Цикловой индекс группы перестановок

Определение. Говорят, что задано действие группы $(G,\circ,e)$ на множестве $S=(1,2,\dots,n)$, если определен гомоморфизм τ группы G в симметрическую группу перестановок S_n: $\tau: G \longrightarrow S_n$.

Напомним, что свойство гомоморфизма сохранять операцию в данном случае заключается в следующем: если $g_1,\ g_2 \in G$, то $\tau(g_1 \circ g_2) = \pi_1 \cdot \pi_2$, где

$$\pi_1 = \tau(g_1) = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}, \pi_2 = \tau(g_2) = \begin{pmatrix} 1 & 2 & \dots & n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} \in S_n.$$

Замечание. Обычно действие G на S возникает естественным образом, как группа симметрий структуры, определенной на S. □

Пример. Пусть $S=(1,2,3,4,5,6,7,8)-$ множество вершин куба, изображенного на рис. 4б. Группа самосовмещений этого куба при его вращениях в трехмерном евклидовом пространстве имеет порядок 24 и состоит из следующих преобразований и соответствующих им перестановок в S_8:

1) тождественное преобразование, вершины куба остаются на своих местах, что соответствует тождественной перестановке

$$\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8 \\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8 \end{pmatrix} = (1)(2)(3)(4)(5)(6)(7)(8) \in S_8;$$

2) шесть поворотов на $\pm 90°$ вокруг осей (типа t), проходящих через середины противоположных граней, соответствующие перемещения вершин описываются перестановками

(1432)(5876) (2376)(1485) (1265)(3784)
(1234)(5678) (2673)(1584) (1562)(3487)

3) три поворота на $180°$ вокруг осей (типа t), проходящих через середины противоположных граней, соответствующие перемещения вершин описываются перестановками

(13)(24)(57)(68) (27)(36)(18)(45) (16)(25)(38)(47)

4) шесть поворотов на $180°$ вокруг осей (типа f), проходящих через середины противоположных ребер, соответствующие перемещения вершин описываются перестановками

(15)(28)(37)(46) (12)(35)(46)(78) (14)(28)(35)(67)
(17)(26)(35)(48) (17)(28)(34)(56) (17)(23)(46)(58)

5) восемь поворотов на $\pm 120°$ вокруг осей (типа r), проходящих через противоположные вершины, соответствующие перемещения вершин описываются перестановками

(1)(7)(254)(368) (2)(8)(136)(475) (3)(5)(274)(168) (4)(6)(138)(275)
(1)(7)(245)(386) (2)(8)(163)(457) (3)(5)(186)(472) (3)(5)(183)(257)

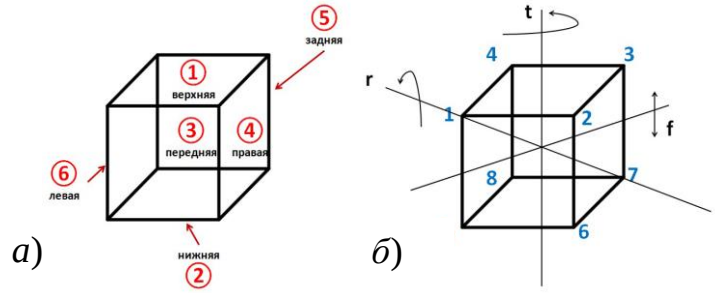

Рис. 4. *а*) Нумерация граней куба;
б) типичные вращения куба вокруг осей t, r, f.

Если дана перестановка π на множестве $S = (1, 2, \dots, n)$, то она разбивает S на циклы. Если l – длина этого цикла, а s – некоторый элемент этого цикла, то цикл состоит из следующих элементов: s, πs, $\pi^2 s$, … , $\pi^{l-1} s$, где $\pi^k s = \pi \circ \pi^{k-1} s$. Произведение $\pi \circ \sigma$ перестановок π и σ определяется в соответствии с общим правилом композиции отображений:

$$\pi \circ \sigma(s) = \pi \circ (\sigma(s)), s \in S.$$

Если перестановка π разбивает множество S на m_1 циклов длины 1, на m_2 циклов длины 2 и т.д., то мы говорим, что перестановка имеет тип $1^{m_1} 2^{m_2} \dots n^{m_n}$.

Очевидно, что $m_1 + 2m_2 + 3m_3 + \cdots + nm_n = n$, так как общее число элементов в S равно n. Цикловой индикатор для перестановки π такого типа определяется выражением

$$I_\pi(x_1, x_2, \dots, x_n) = {x_1}^{m_1} {x_2}^{m_2} \dots {x_n}^{m_n}.$$

Определение. *Цикловой индекс* группы перестановок G на множестве $S = (1, 2, \dots, n)$ определяется как

$$P_G(x_1, x_2, \dots, x_n) = \frac{1}{|\,G\,|}\sum_{\pi\in G} I_\pi(x_1, x_2, \dots, x_n)$$

$$= \frac{1}{|\,G\,|}\sum_{\pi\in G} {x_1}^{m_1}{x_2}^{m_2} \dots {x_n}^{m_n}.$$

Примеры. 1) Пусть $\mathfrak{E}_n$ – группа перестановок степени n порядка 1, состоящая из одной тождественной перестановки $\mathcal{E} = (1)(2) \dots (n)$. Очевидно, что

$$P_{\mathfrak{E}_n}(x_1) = x_1^n.$$

2) Для вычисленной выше группы перестановок $\mathfrak{K}_8$ на множестве вершин куба, порожденной вращениями куба в трёхмерном евклидовом пространстве, получаем, что

$$P_{\mathfrak{K}_8}(x_1, x_2, x_3, x_4x_5, x_6) = \frac{1}{24}(x_1^8 + 9x_2^4 + 6x_4^2 + 8x_1^2x_3^2).$$

3) Пусть $\mathfrak{C}_n$– циклическая группа перестановок порядка n, порожденная перемещениями вершин правильного n-угольника при его вращении на плоскости. Эта группа порождается полноцикловой перестановкой $\pi = (23 \dots n1)$ и состоит из перестановок π^0, π^1, π^2, …, π^{n-1}, где π^0 – тождественная перестановка. Перестановка π^k разлагается на $d =$ НОД (n, k) простых циклов длины n/d. При фиксированном делителе d числа n, число целых k, $0 \le k \le n-1$, удовлетворяющих равенству НОД $(n, k) = n/d$, равно $\varphi(d)$, где $\varphi(\cdot)$ – функция Эйлера. Поэтому

$$P_{\mathfrak{C}_n}(x_1, \dots, x_n) = \frac{1}{n}\sum_{d|n} \varphi(n/d)x_{n/d}^d = \frac{1}{n}\sum_{d|n} \varphi(d)x_d^{n/d}.$$

4) Пусть $\mathfrak{D}_n$ – группа перестановок порядка $2n$, порожденная перемещениями вершин правильного n- угольника при его вращении на плоскости и в пространстве. Эта группа (её называют *группой диэдра*) порождается перестановками $\pi = (23 \dots n1)$ и $\tau = (1)(2, n)(3, n-1)$. Из прямых вычислений следует, что $\pi^n = \tau^2 = (1)(2) \dots (n)$ и $\pi\tau = (1n\, n-1 \dots 2) = \pi^{n-1} = \pi^{-1}$, или $\pi\tau = \tau\pi^{n-1}$. Итерация последнего равенства показывает, что $\pi^k\tau = \tau\pi^{n-k}$ при любом k. Поэтому

$$\mathfrak{D}_n = \{\pi^0, \pi^1, \pi^2, \dots, \pi^{n-1}, \tau, \tau\pi^1, \tau\pi^2, \dots, \tau\pi^{n-1}\}.$$

Цикловая структура этой группы может быть найдена в два приёма. Группа $\mathfrak{C}_n = \{\pi^0, \pi^1, \pi^2, \dots, \pi^{n-1}\}$ даёт следующий вклад в цикловой индекс:

$$\sum_{d|n} \varphi(d) x_d^{n/d}.$$

Далее рассмотрим совокупность перестановок $\{\tau, \tau\pi^1, \tau\pi^2, \dots, \tau\pi^{n-1}\}$. Перестановки P и T называются *подобными*, если $P = STS^{-1}$ для некоторой перестановки S. Подобные перестановки имеют одинаковые цикловые структуры. Так как

$$\pi^{n-k}(\tau\pi^s)\pi^k = \pi^{n-k}\tau\pi^{s+k} = \tau\pi^k\pi^{s+k} = \tau\pi^{s+2k},$$

то перестановки $\tau\pi^s$ и $\tau\pi^{s+2k}$ являются подобными и имеют одинаковую цикловую структуру. Для нечетного $n = 2k-1$ все перестановки $\tau\pi^s$, $0 \le s \le n-1$, имеют одинаковую цикловую структуру, совпадающую с τ. Их вклад в цикловой индекс равен $nx_1x_2^{k-1}$. Для четного $n = 2k$ перестановки $\tau\pi^{2k}$ имеют ту же цикловую структуру, что и τ. Их вклад равен $kx_1^2x_2^{k-1}$. Остальные перестановки $\tau\pi^{2k+1}$ имеют ту же цикловую структуру, что и $\tau\pi$, делая вклад в цикловой индекс, равный kx_2^k. Окончательно получаем, что

$$P_{\mathfrak{D}_n}(x_1, \dots,)x_n)$$

$$= \left(\frac{1}{2n}\sum_{d|n} \varphi(d) x_d^{n/d}\right) + \begin{cases} \frac{1}{2}x_1x_2^{k-1}, & \text{если } n = 2k-1, \\ \frac{1}{4}(x_1^2x_2^{k-1} + x_2^k), & \text{если } n = 2k \end{cases}.$$

Приведём без доказательства цикловые индексы для некоторых известных групп:

5) $\mathcal{T}_4$ – группа перестановок на множестве вершин тетраэдра степени 4 порядка 12, порождённая вращениями тетраэдра в пространстве:

$$P_{\mathcal{T}_4}(x_1, x_2, x_3, x_4) = \frac{1}{12}(x_1^4 + 8x_1x_3 + 3x_2^2).$$

6) $\mathfrak{K}_6$ – группа перестановок на множестве граней куба степени 6 порядка 24, порождённая вращениями куба в пространстве:

$$P_{\mathfrak{K}_6}(x_1, x_2, x_3, x_4x_5, x_6) = \frac{1}{24}(x_1^6 + 6x_1^2x_4 + 3x_1^2x_2^2 + 6x_2^3 + 8x_3^2).$$

7) $\mathfrak{K}_{12}$ – группа перестановок на множестве ребер куба степени 12 порядка 24, порождённая вращениями куба в пространстве:

$$P_{\mathfrak{K}_{12}}(x_1, x_2, x_3, x_4x_5, x_6) = \frac{1}{24}\left(x_1^{12} + 6x_4^3 + 6x_1^2x_2^5 + 3x_2^3 + 8x_3^3\right).$$

8) $\mathfrak{S}_n$– симметрическая группа перестановок степени n порядка $n!$

$$P_{\mathfrak{S}_n}(x_1, \dots, x_n) = \sum_{(b_1,\dots,b_n),\ \sum i b_i = n} \frac{1}{b_1! \dots b_n! 1^{b_1} \dots n^{b_n}} x_1^{b_1} \dots x_n^{b_n} x_1^{b_1} \dots x_n^{b_n}.$$

9) $\mathfrak{A}_n$ – знакопеременная группа четных перестановок степени n порядка $n!/2$.

$$P_{\mathfrak{S}_n}(x_1, \dots, x_n) = \sum_{(b_1,\dots,b_n),\sum i b_i = n} \frac{1 + (-1)^{b_2 + b_4 + \cdots}}{b_1! \dots b_n! 1^{b_1} \dots n^{b_n}} x_1^{b_1} \dots x_n^{b_n}. \quad \square$$

Замечание. Цикловой индекс группы перестановок даёт некоторую информацию о комбинаторных свойствах группы, но даёт мало сведений о её мультипликативной структуре. В частности, можно указать неизоморфные группы одного и того же порядка с одинаковыми цикловыми индексами (см. [**32**], раздел 26, стр. 64−65).

29.2. Лемма Бернсайда о числе транзитивных множеств

В этом разделе рассматривается лемма Бернсайда, которая составляет основную часть перечислительной теории Пойа.

Пусть G – конечная группа, элементы которой ведут себя как перестановки некоторого множества S. Другими словами, каждому элементу $g \in G$ соответствует некоторая перестановка π_g, заданная на множестве S. Предположим также, что это соответствие является гомоморфизмом, т.е. $\pi_{gg'} = \pi_g \cdot \pi_{g'}, \quad \forall g, g' \in G$.

Элементы $s_1, s_2 \in S$ называются *эквивалентными* (пишем $s_1 \sim s_2$), если существует элемент $g \in G$ такой, что $s_2 = \pi_g s_1$. Введённое отношение $\sim$

1) рефлексивно: $s_1 = \pi_e s_1 \Longrightarrow s_1 \sim s_1$, где $e \in G$ – единичный элемент группы G, π_e – тождественная перестановка, оставляющая на месте все точки множества S;

2) симметрично: $s_1 \sim s_2 \Longrightarrow s_2 = \pi_g s_1 \Longrightarrow s_1 = \pi_{g^{-1}} s_2 \Longrightarrow s_2 \sim s_1$, так как $\pi_g^{-1} = \pi_{g^{-1}}$;

3) транзитивно: $s_1 \sim s_2$ и $s_2 \sim s_3 \Longrightarrow s_1 \sim s_3$, так как $s_2 = \pi_g s_1$ и $s_3 = \pi_{g'} s_2 \Longrightarrow s_3 = \pi_{g'} \pi_g s_1 = \pi_{g'g} s_1$.

Отношение со свойствами 1), 2), 3) является отношением эквивалентности, оно разбивает множество S на классы эквивалентных

между собой элементов, Эти классы будем называть *транзитивными множествами*.

29.1. ***Лемма Бернсайда*** [23]. *Число транзитивных множеств равно*

$$m = \frac{1}{|\,G\,|}\sum_{\pi\in G}\psi(g),$$

где $\psi(g)$ *обозначает число элементов* $s \in S$, *для которых* $\pi_g s = s$.

Доказательство. Рассмотрим все пары (g, s), для которых $g \in G, s \in S, \pi_g s = s$. Число N таких пар может быть вычислено двумя способами.

Первый способ. Для каждого $g \in G$ можно подсчитать число $s \in S$, удовлетворяющих условию $\pi_g s = s$. Очевидно, что

$$N = \sum_{\pi\in G}\psi(g).$$

Второй способ. Для каждого $s \in S$ можно подсчитать число $g \in G$, удовлетворяющих условию $\pi_g s = s$. Обозначим это число через $\lambda(s)$. Тогда

$$N = \sum_{s\in S}\lambda(s) = \sum_{\pi\in G}\psi(g).$$

Для фиксированного s элементы группы G со свойством $\pi_g s = s$ образуют подгруппу G_s порядка $\lambda(s)$. Если $s_1 \sim s$, то число элементов $g \in G$ таких, что $\pi_g s = s_1$, равно $|\,G_s\,|$. Действительно, $s = \pi_h s_1$ для некоторого $h \in G$. Но тогда $\pi_h \pi_g s = \pi_{hg} s = \pi_h s_1 = s$ для любого $g \in G_s$ и, следовательно, $hg \in G_s$. Таким образом, при фиксированных s_1и s число возможностей для выбора g со свойством $\pi_g s = s_1$ равно числу элементов в G_s. Соответственно G может быть разбита на подмножества, каждое из которых состоит из $|\,G_s\,|$ элементов и соответствует ровно одному элементу того класса эквивалентности, в который входит элемент s. Отсюда следует, что этот класс эквивалентности содержит $|\,G\,|/|\,G_s\,|$ элементов. Поэтому

$$\lambda(s) = \frac{|G|}{\text{число элементов в классе эквивалентности,содержащем } s}.$$

---

[23] ***Уильям Бёрнсайд*** (2.07.1852— 21.08.1927) — английский математик-алгебраист.

Суммируя по s, получаем, что сумма чисел $\lambda(s)$ для всех s, принадлежащих одному и тому же классу эквивалентности, равна $|\ G\ |$. Следовательно,

$$\sum_{s\in S}\lambda(s) =|\ G\ |\cdot m=\sum_{\pi\in G}\psi(g)\ \Longrightarrow\ m=\frac{1}{|\ G\ |}\sum_{\pi\in G}\psi(g)\,.\ \square$$

29.3. Комбинаторные конфигурации как отображения f: D ⟶ R

Пусть D и R – конечные множества. Рассмотрим отображения (функции) $f\colon D\longrightarrow R$, определенные на множестве D со значениями в R. Такие отображения, удовлетворяющие определенным ограничениям, называют *комбинаторными конфигурациями*. Множество D называется *областью определения*, а множество R – *областью значений*. Множество всех отображений обозначается через R^D. Число $|R^D|$ всех элементов множества R^D равно $|R|^{|D|}$.

Пусть дана группа G перестановок множества D. Эта группа порождает отношение эквивалентности на множестве R^D: функции f_1, $f_2\in R^D$, называются *эквивалентными* (обозначение: $f_1\sim f_2$), если существует перестановка $g\in G$ такая, что

$$f_1(gd)=f_2(d)\quad\text{для всех } d\in D. \qquad (1)$$

Соотношение (1) кратко записывается как $f_1g=f_2$ (в произведении f_1g отображений f_1 и g сначала выполняется g, затем f_1). Введенное отношение равенства является отношением эквивалентности, так как оно рефлексивно, симметрично и транзитивно:

1) $f\sim f$ ввиду $fe=f$, где $e-$ единица (т.е. тождественная перестановка) в G;

2) $f_1\sim f_2\Longrightarrow f_2\sim f_1$ ввиду $g\in G\Longrightarrow g^{-1}\in G$ и $f_1g=f_2\Longrightarrow f_2g^{-1}=f_1$;

3) $f_1\sim f_2$ и $f_2\sim f_3\Longrightarrow f_1\sim f_3$ ввиду $g_1, g_1\in G\Longrightarrow g_1g_2\in G$ и $f_1g_1=f_2$ и $f_2g_2=f_3\Longrightarrow f_1g_1g_2=f_3$.

Так как отношение $\sim$ является отношением эквивалентности, то с его помощью множество R^D разбивается на классы эквивалентности.

Пример. Рассмотрим задачу о числе способов раскраски граней куба в два цвета (белый и чёрный). При решении этой задачи сначала необходимо уточнить, какие раскраски считать различными, а какие неразличимыми (т.е. эквивалентными). Самое простое допущение заключается в том, что раскрашиваемый куб зафиксирован в простран-

стве и не подвержен вращениям (т.е. его группа вращений состоит из одной тождественной перестановки). В этом случае все отображения $f: D \longrightarrow R$, где $D = \{1,2,3,4,5,6\} -$ множество граней куба, $R = \{б,ч\}$ – множество цветов, являются различными. Их число равно $2^6 = 64$. В другом случае можно считать, что два куба, расположенные параллельно, раскрашены одинаково, если один из них можно повернуть в пространстве так, что их раскраски совпадут, т.е. перестанут казаться различными. В этом случае раскраски указанных кубов считаются эквивалентными. Таких классов эквивалентности будет 10. Перечислим их (в скобках – число функций в соответствующем классе): 1) все грани белые (1); 2) одна грань черная, остальные белые (6); 3) две противоположные грани черные, остальные белые (3); 4) две смежные грани черные, остальные белые (12); 5) три грани с общей вершиной черные, остальные белые (8); 6) три грани, не имеющие общей вершины, черные, остальные белые (12); 7) две смежные грани белые, остальные черные (12); 8) две противоположные грани белые, остальные белые (3); 9) одна грань белая, остальные черные (6); 10) все грани черные (1). Так как $1 + 6 + 3 + 12 + 8 + 12 + 12 + 3 + 6 + 1 = 64$, то учтены все 64 конфигурации. Отметим, что во втором случае классы эквивалентных конфигураций порождены действием указанной выше группы перестановок $\mathfrak{S}_6$ на множестве D. □

Задача. Перечислить все подгруппы группы $\mathfrak{S}_6$. Установить число классов эквивалентных конфигураций в R^D, порождаемых действием этих подгрупп на множестве D.

Каждому элементу множества R придадим *вес*. Весами могут быть числа, а в общем случае рациональные переменные, перенумерованные элементами множества R. Вес, приданный элементу $r \in R$ обозначим через $w(r)$. Веса можно складывать, перемножать, умножать на рациональные числа. Эти операции должны удовлетворять обычным законам ассоциативности, коммутативности и дистрибутивности.

Определение. Вес функции $f \in R^D$ определяется как произведение

$$W(r) = \prod_{d \in D} w(f(d)) .$$

Пусть функции f_1и f_2 принадлежат одному и тому же классу эквивалентности, т.е. $f_1 g = f_2$ для некоторой перестановки $g \in G$. Тогда

$$\prod_{d\in D} w(f_1(d)) = \prod_{d\in D} w(f_1(gd)) = \prod_{d\in D} w(f_2(d)).$$

Другими словами, функции f_1 и f_2 имеют одинаковые веса. Это позволяет определить вес $W(F)$ класса эквивалентности F, полагая его равным весу любой функции из данного класса.

Пример. Возвращаясь к предыдущему примеру с $G = \mathfrak{K}_6$, присвоим элементам *б*, *ч* $\in R$ соответственно веса x и y. Тогда десять классов эквивалентности 1) $-$10) будут иметь следующие веса:

$$x^6, x^5y, x^4y^2, x^4y^2, x^3y^3, x^3y^3, x^2y^4, x^2y^4, xy^5, y^6. \square$$

Этот пример показывает, что различные классы эквивалентности могут иметь одинаковые веса. Если положить $w(r) = 1$ для каждого $r \in R$, то все классы эквивалентности будут иметь вес, равный 1.

29.4. Теорема Пойа о перечне классов эквивалентности

Определение. *Перечень* (или *производящая функция*) множества классов эквивалентности определяется как

$$\sum_F W(F),$$

где суммирование распространено на все классы эквивалентности.

В предыдущем примере перечень множества классов эквивалентности равен

$$\sum_F W(F) = x^6 + x^5y + 2x^4y^2 + 2x^3y^3 + 2x^2y^4 + xy^5 + y^6,$$

откуда, в частности, следует, что имеется в точности две неэквивалентные раскраски куба с 4 белыми и 2 черными гранями.

29.2. ***Теорема*** Пойа [24] (1937). *Перечень классов эквивалентности равен*

$$\sum_F W(F) = P_G\left(\sum_{r\in R} w(r), \sum_{r\in R} w(r)^2, \sum_{r\in R} w(r)^3, \dots\right), \qquad (2)$$

---

[24] ***Дьёрдь Пойа*** (13.12.1887 $-$ 7.09.1985) $-$ венгерский, швейцарский и американский математик, популяризатор науки.

где P_G – цикловой индекс группы перестановок G. В частности, если все веса $w(r)$ равны 1, то

$$\sum_F W(F) = P_G(|R|, |R|, |R|, \dots). \qquad (3)$$

Доказательство. Пусть ω – одно из значений, которое может принимать вес функции, а S – множество всех функций $f \in R^D$ таких, что $W(f) = \omega$. Если $g \in G$ и $f_1 g = f_2$, то $W(f_1) = W(f_2)$. Поэтому $f_1 \in S \Longrightarrow f_1 g^{-1} \in S$. Это означает, что каждому элементу $g \in G$ соответствует отображение π_g множества S в себя, определяемое как $\pi_g f = f g^{-1}$, где π_g – перестановка, поскольку имеет обратную $\pi_g^{-1} = \pi_{g^{-1}}$.

Отображение $g \longrightarrow \pi_g$ является гомоморфизмом, т.е. $\pi_{gg'} = \pi_g \cdot \pi_{g'} \forall g, g' \in G$, поскольку для каждой функции $f \in S$ имеем $\pi_{gg'} f = f(gg')^{-1}, \pi_g(\pi_{g'} f) = \pi_g(f g'^{-1}) = f g'^{-1} g^{-1}, (gg')^{-1} = g'^{-1} g^{-1}$.

Элементы f_1 и f_2 из S эквивалентны, как это определено в лемме Бернсайда, тогда и только тогда, когда они эквивалентны согласно определению предыдущего параграфа. Существование перестановки $g \in G$ такой, что $\pi_g f_2 = f_1$, равносильно существованию $g \in G$ такой, что $f_2 = f_1 g$. Следовательно, классы эквивалентности в S суть те же, что описаны выше в разделе 29.2. Тогда согласно лемме 29.1 число классов эквивалентности в S равно

$$\frac{1}{|G|} \sum_{g \in G} \psi_\omega(g), \qquad (4)$$

где $\psi_\omega(g)$ – число функций f, таких, что $W(f) = \omega$, $f g^{-1} = f$ (или, что то же самое, $f = fg$). Умножая на ω и суммируя по всем возможным значениям ω, получаем

$$\sum_F W(F) = \frac{1}{|G|} \sum_\omega \sum_{g \in G} \psi_\omega(g)\omega = \frac{1}{|G|} \sum_{g \in G} \sum_\omega \psi_\omega(g)\omega .$$

Так как

$$\sum_\omega \psi_\omega(g)\omega = \sum_{f \in R^D, f = fg} W(f),$$

то

$$\sum_F W(F) = \frac{1}{|G|} \sum_{g \in G} \sum_{f \in R^D,\, f = fg} W(f) . \qquad (5)$$

Оценим внутреннюю сумму в последней формуле. Перестановка g множества D разбивает это множество на циклы вида d, gd, g^2d,... Условие $f = fg$ означает, что $f(d) = f(gd) = f(g^2d) = \cdots$ Следовательно, функция f постоянна на каждом цикле. Обратно, каждая функция f, постоянная на каждом цикле, удовлетворяет условию $f = fg$, поскольку d принадлежит всегда тому же циклу, что и gd. Обозначим сумму весов классов эквивалентности, на которые разбивается множество S, как *перечень* S. Если перестановка g разбивает множество D на циклы D_1, D_2,…, D_k, то сумма

$$\sum_{f \in R^{D},\ f=fg} W(f)$$

выражается формулой

$$\text{Перечень } S = \sum_{i=1}^{k} \sum_{r \in R} |w(r)|^{|D_i|}.$$

Пусть $|D| = n$, а $1^{b_1}2^{b_2}\ldots n^{b_n}$ – тип перестановки g. Это означает, что среди чисел $|D_1|$, $|D_2|$,…, $|D_k|$ число 1 встречается b_1 раз, число $2 - b_2$ раз,…, число $n - b_n$раз, при этом $b_1 + 2b_2 + \cdots + nb_n = n$. Следовательно,

$$\sum_{f \in R^{D},\ f=fg} W(f) = \left(\sum_{r \in R} w(r)\right)^{b_1} \left(\sum_{r \in R} w(r)\right)^{b_2} \ldots \left(\sum_{r \in R} w(r)\right)^{b_n}. \quad (6)$$

Выражение (6) может быть получено подстановкой

$$x_1 = \sum_{r \in R} w(r), \qquad x_2 = \sum_{r \in R} w(r)^2, \ldots, \qquad x_n = \sum_{r \in R} w(r)^n, \quad (7)$$

в произведение $x_1^{b_1}x_2^{b_2} \ldots x_n^{b_n}$, которое является цикловым индикатором перестановки g в P_G. Суммируя по g и деля на $|G|$, заключаем, что значение (5) получено заменой переменных $x_1, x_2, \ldots, x_n$ в $P_G(x_1, x_2, \ldots, x_n)$ согласно (7). □

Глава V. Алгебраические структуры с двумя бинарными операциями

§ 30. Кольца. Основные определения и свойства

До сих пор рассматривались множества с одной бинарной операцией – группоиды, полугруппы, моноиды и группы. Теперь будем рассматривать множества с двумя бинарными операциями, одну из которых принято называть *сложением* (и обозначать символом $+$), а другую – *умножением* (и обозначать символом $\cdot$, который, впрочем, обычно опускают).

Определение. Алгебраическая структура $\mathcal{R} = (R, +, \cdot)$ называется *кольцом*, если для неё выполнены следующие аксиомы:

R1. $(R, +)$ – абелева группа;

R2. $(R, \cdot)$ – полугруппа;

R3. для любых $x,y,z \in R$ выполняются *дистрибутивные законы*:

$$(x + y) \cdot z = (x \cdot z) + (y \cdot z),$$
$$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$$

Структура $(R, +)$ называется *аддитивной группой* кольца. Нуль этой группы (т.е. нейтральный элемент относительно сложения) называется *нулём кольца* $\mathcal{R}$ и обозначается символом 0. Как и в случае аддитивных групп, элемент, противоположный к x (т.е. обратный к x относительно сложения), обозначается как $(-x)$. Операция вычитания в кольце определяется как $x - y = x + (-y)$.

Структура $(R, \cdot)$ называется *мультипликативной полугруппой* кольца. Если данная полугруппа обладает единицей (т.е. нейтральным элементом относительно умножения), то она называется *единицей кольца* $\mathcal{R}$ и обозначается нами как 1 или e.

Замечание. В общей теории колец рассматривают алгебраические системы, в которых аксиома R2 либо устраняется, либо заменяется на другую, например, на следующую:

R2′. $(R, \cdot)$ − группоид.

В этом случае говорят о *неассоциативных кольцах*. Здесь же рассматриваются только *ассоциативные кольца*. □

Если умножение коммутативно, т.е. $x \cdot y = y \cdot x$ для любых $x,y \in R$, то кольцо $\mathcal{R}$ называется *коммутативным*.

Одноэлементное кольцо $R = \{0\}$ называется, *тривиальным*, или *нулевым*.

Множество R называется *основным множеством* кольца $\mathcal{R}$. Далее, для краткости, кольцо будем обозначать той же буквой, что и основное множество.

Поскольку кольцо является одновременно аддитивной группой и мультипликативной полугруппой, то для колец могут быть переформулированы свойства, присущие указанным структурам. Вместе с тем в кольцах обнаруживаются новые (специфические) свойства, обусловленные взаимодействием двух структур − аддитивной и мультипликативной − через связывающие их дистрибутивные законы. Отметим некоторые из них.

Во-первых, $0 \cdot x = x \cdot 0 = 0$ для всех $x \in R$. Действительно, $0 + x = x \Longrightarrow (0 + x) \cdot x = x^2 \Longrightarrow 0 \cdot x + x^2 = x^2 \Longrightarrow 0 \cdot x = 0$. Аналогично, $x \cdot 0 = 0$.

Далее, из равенств

$$0 = x \cdot \big(y + (-y)\big) = x \cdot y + x \cdot (-y) \text{ и } 0 = \big(x + (-x)\big) \cdot y = x \cdot y + (-x) \cdot y$$

следует, что $x \cdot (-y) = (-x) \cdot y = -(x \cdot y)$ и $(-x) \cdot (-y) = x \cdot y$ для всех $x, y \in R$.

Применяя индукцию (сначала по m, затем по n), можно вывести *общий дистрибутивный закон*:

$$(x_1 + \cdots + x_m)(y_1 + \cdots + y_n) = \sum_{i=1}^{m} \sum_{j=1}^{n} x_i y_j. \qquad (1)$$

В аддитивной группе кольца определим кратные $m \cdot x$ для любых $m \in \mathbb{Z}$ и $x \in R$, полагая $m \cdot x = 0$ для $m = 0$, $m \cdot x = x + \cdots + x$ (m слагаемых) для $m > 0$ и $m \cdot x = -((-m) \cdot x)$ для $m < 0$. Тогда из (1) следует, что $(m \cdot x)(n \cdot y) = (n \cdot x)(m \cdot y) = (mn)(x \cdot y)$ для всех $m,n \in \mathbb{Z}$ и $x,y \in R$.

Подчеркнём, что $m \cdot x$ не является произведением двух элементов кольца, поскольку $m \notin R$ (исключая, конечно, случай, когда $\mathbb{Z} \subset R$). Однако, если кольцо обладает единицей, то $m \cdot x$ можно записать как произведение двух элементов из R: $(m \cdot x) = (m \cdot 1) \cdot x$.

Для коммутативного кольца справедлива формула (бином Ньютона):

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\text{, где } x^0 = y^0 = 1.$$

Наконец, предположим на мгновение, что кольцо обладает единицей 1 и $1 = 0$. Тогда из $x = x \cdot 1 = x \cdot 0 = 0$ следует, что равенство $1 = 0$ возможно только для нулевого (т.е. одноэлементного) кольца.

Определение. Ненулевые элементы x и y кольца R называются *делителями нуля*, если $x \cdot y = 0$. Более точно: ненулевой элемент $x \in R$ называется *левым делителем нуля*, если существует ненулевой элемент $y \in R$ такой, что $x \cdot y = 0$. Аналогично определяется *правый делитель нуля*. Для коммутативного кольца эти понятия совпадают. Кольцо, в котором нет ни левых, ни правых делителей нуля, называется *кольцом без делителей нуля*. Коммутативное кольцо с единицей $1 \neq 0$ и без делителей нуля называется *целостным кольцом* (или *областью целостности*).

Очевидно, что кольцо без делителей нуля − это кольцо R, у которого множество $R^{(0)} = R \setminus \{0\}$ замкнуто относительно умножения, т.е. $R^{(0)}$ − полугруппа. Аналогично, целостное кольцо − это кольцо, у которого $(R^{(0)}, \cdot)$ − коммутативный моноид.

30.1. ***Теорема***. *Кольцо R является кольцом без делителей нуля тогда и только тогда, когда в нём выполняются законы сокращения*:

$xz = yz,\ z \neq 0 \Longrightarrow x = y,$

$zx = zy,\ z \neq 0 \Longrightarrow x = y$

для всех $x,y,z \in R$.

Доказательство. Пусть R − кольцо без делителей нуля. Тогда $z \neq 0,\ xz = yz \Longrightarrow (x-y)z = 0 \Longrightarrow x = y,$ т.е. первый закон сокращения выполняется. Аналогично доказывается и второй закон сокращения. Обратно, пусть выполняются оба закона сокращения. Тогда $xy = 0 \Longrightarrow xy = 0y \Longrightarrow x = 0$ или $y = 0$, т.е. в кольце делителей нуля нет. □

30.2. ***Следствие.*** *Ненулевое коммутативное кольцо R без делителей нуля является целостным кольцом тогда и только тогда, когда в нём выполняется закон сокращения*

$xz = yz,\ z \neq 0 \Longrightarrow x = y$ для всех $x, y, z \in R$.

Определение. Пусть R − кольцо с единицей. Элемент $x \in R$ называется *левым обратным для* $y \in R$, если $xy = 1$. Аналогично определяется *правый обратный для* y. Элемент x называется *обратимым* в R, если существует $y \in R$ такой, что $xy = yx = 1$. При этом

элемент y называется *двусторонним обратным* (или просто *обратным*) для x и обозначается x^{-1}. Множество обратимых элементов кольца R обозначим через R^*.

Отметим некоторые свойства обратимых элементов. Элемент $x \in R$ может не иметь или иметь несколько левых или правых обратных. Однако, если x имеет левый обратный y и правый обратный z, то $y = z$. Действительно,

$$y = y \cdot 1 = y(xz) = (yx)z = 1 \cdot z = z.$$

Для коммутативных колец понятия левого и правого обратных, очевидно, совпадают. То же самое справедливо и для колец без делителей нуля:

$$yx = 1 \Longrightarrow x(yx) = x \cdot 1 = 1 \cdot x \Longrightarrow (xy)x = 1 \cdot x \Rightarrow xy = 1.$$

Обратимый элемент не может быть делителем нуля:

$$xy = 0 \Longrightarrow (xy)y^{-1} = 0 \Longrightarrow x(yy^{-1}) = 0 \Longrightarrow x \cdot 1 = 0 \Longrightarrow x = 0;$$

аналогично, $yx = 0 \Longrightarrow x = 0$.

Разумеется, что для обратимых элементов $x,y \in R$ справедливы равенства: $(xy)^{-1} = y^{-1}x^{-1}$, $(x^{-1})^{-1} = x$. Следующее утверждение является аналогом соответствующей теоремы о моноидах:

30.3. ***Теорема.*** *Множество R^* обратимых элементов кольца R с единицей образует мультипликативную группу.*

Группу R^* называют *группой обратимых элементов кольца* R. Её обозначают также $U(R)$ и называют *группой делителей единицы* или, более кратко, *группой единиц кольца* R.

§ 31. Тела и поля

Определение. Кольцо с единицей $1 \neq 0$, в котором всякий ненулевой элемент обратим, называется *кольцом с делением*, или *телом*. Другими словами, тело $-$ это кольцо, ненулевые элементы которого образуют мультипликативную группу.

Определение. Коммутативное тело называется *полем*.

Поскольку полям уделяется особое внимание, повторим определение поля ещё раз:

Определение. *Поле* $-$ алгебраическая структура $\mathcal{F} = (F, +, \cdot)$, удовлетворяющая аксиомам:

F1. $(F, +)$ $-$ абелева группа;

F2. $(F^*, \cdot)$, где $F^* = F \setminus \{0\}$, $-$ абелева группа;

F3. Сложение и умножение связаны дистрибутивным законом:

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z) \text{ для всех } x,y,z \in R$$

(умножение коммутативно, поэтому надобность во втором законе отпадает).

Таким образом, поле − гибрид двух абелевых групп.

Любое поле, очевидно, является целостным кольцом. Обратное, вообще говоря, неверно. Например, $\mathbb{Z}$ − целостное кольцо, но не поле, поскольку 1 и (-1) − единственные обратимые элементы.

31.1. ***Теорема.*** *Если конечное кольцо R содержит элемент $x \neq 0$, не являющийся делителем нуля, то R − кольцо с единицей, в котором любой элемент из $R \setminus \{0\}$, не являющий делителем нуля, обратим.*

Доказательство. Если $y, z \in R$ и $yx = zx$, то $(y - z)x = 0$, и, следовательно, $y = z$. Другими словами, $yx \neq zx$ при $y \neq z$, откуда, ввиду конечности множества R, получаем, что $Rx = R$. Аналогично, $xR = R$.

Из равенства $Rx = R$ следует, что существует элемент e такой, что $ex = x$. Тогда для произвольного $y \in R$ имеем: $z = ye \Longrightarrow zx = yex = yx \Longrightarrow z = y \Longrightarrow y = ye$. Аналогично, из равенства $xR = R$ следует, что существует элемент $e' \in$ R такой, что $y = ye'$ при любом $y \in R$. Поскольку $e = ee' = e'$, то R − кольцо с единицей e.

Из равенств $xR = Rx = R$ следует, что $xy = y'x = e$ для некоторых y, $y' \in R$. Поскольку $y = (y'x)y = y'(xy) = y'$, то элемент x обратим, а y − его обратный элемент. □

31.2. ***Следствие.*** *Конечное ненулевое коммутативное кольцо R является полем тогда и только тогда, когда в $R \setminus \{0\}$ отсутствуют делители нуля. В частности, конечное целостное кольцо является полем.*

Замечание. На бесконечные кольца доказанные теоремы и следствие не распространяются. Например, в кольце $2\mathbb{Z}$ нет делителей нуля, но нет и единицы. Кольцо $\mathbb{Z}$, как отмечено выше, является целостным, но полем не является. Отметим также, всякое поле является телом, но не всякое тело является полем. Однако для конечных тел справедлива следующая теорема:

31.3. ***Теорема Веддербёрна*** [25]. *Любое конечное тело является полем.*

Доказательство см. в § 51.

Примеры. 1) Множество $\mathbb{F}_2 = \{0, 1\}$ с операциями с операциями сложения и умножения по модулю 2 (в частности, $1 + 1 = 0$) – поле из двух элементов. 2) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ – поля рациональных, вещественных, комплексных чисел. 3) $\mathbb{Q}(\sqrt{2}) = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \}$ – расширение поля $\mathbb{Q}$ путём присоединения элемента (числа) $\sqrt{2}$. Обратным к ненулевому числу $q = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ является ненулевое число $q^{-1} = (a - b\sqrt{2})(a^2 - 2b^2)^{-1}$.

Пример тела, которое не является полем. В 1843 г. У. Гамильтон [26] нашёл алгебру, которая является ассоциативным телом, но не коммутативна. (См., например, [**27**].) Её элементы были названы *кватернионами*. Тело $\mathfrak{Q}$ кватернионов имеет своей базой символы 1, $\boldsymbol{i}$, $\boldsymbol{j}$, $\boldsymbol{k}$, из которых первый служит единицей, а остальные перемножаются по правилам:

$$\boldsymbol{i^2 = j^2 = k^2 = -1},\ \boldsymbol{ij = -ji = k, jk = -kj = i, ki = -ik = j}.$$

Каждый кватернион однозначно записывается в виде линейной формы $\alpha + \beta\boldsymbol{i} + \gamma\boldsymbol{j} + \delta\boldsymbol{k}$ от элементов базы с действительными коэффициентами $\alpha, \beta, \gamma, \delta \in \mathbb{R}$. Перемножаются кватернионы в соответствии с дистрибутивным законом и таблицей умножения базы. Неотрицательное вещественное число $\alpha^2 + \beta^2 + \gamma^2 + \delta^2$ называется *нормой кватерниона* $q = \alpha + \beta\boldsymbol{i} + \gamma\boldsymbol{j} + \delta\boldsymbol{k}$ и обозначается $N(q)$. Кватернион $\alpha - \beta\boldsymbol{i} - \gamma\boldsymbol{j} - \delta\boldsymbol{k}$ называется *сопряжённым* к кватерниону $q = \alpha +$

---

[25] ***Джозеф Генри Маклаген Веддербёрн*** (1882–1948) – шотландский, позднее американский математик, профессор Принстонского университета, алгебраист. Основные труды посвящены общей алгебре, из его достижений наиболее известна теорема о коммутативности конечных тел.

[26] Сэр ***Уильям Роуэн Гамильтон*** (4.08.1805 – 2.09.1865) – ирландский математик, механик-теоретик, физик-теоретик. Один из величайших математиков XIX века. Известен фундаментальными открытиями в математике (кватернионы, основы векторного анализа, вариационное исчисление, обоснование комплексных чисел), аналитической механике и оптике.

$\beta\boldsymbol{i} + \gamma\boldsymbol{j} + \delta\boldsymbol{k}$ и обозначается $\overline{q}$. Непосредственные вычисления показывают, что

$$\overline{q_1 + q_1} = \overline{q}_1 + \overline{q}_2, \quad \overline{q_1 \cdot q_2} = \overline{q}_1 \cdot \overline{q}_2;$$
$$\overline{\alpha \cdot q} = \alpha \cdot \overline{q}, \quad \alpha \in \mathbb{R};$$
$$q \cdot \overline{q} = \overline{q} \cdot q = N(q), \quad N(q_1 \cdot q_2) = N(q_1) \cdot N(q_2).$$

Каждый элемент $q \neq 0$ мультипликативной группы $(\mathfrak{Q}^*, \cdot)$ обратим: полагая $q^{-1} = \frac{1}{N(q)}\overline{q}$, будем иметь $q^{-1}q = qq^{-1} = 1$.

§ 32. Подкольца и идеалы колец

В теории колец особую роль, аналогичную роли подгрупп и нормальных делителей в теории групп, играют подкольца и идеалы.

Определение. Подмножество S кольца R называется *подкольцом в* R, если S само является кольцом относительно операций, заданных в R. Другими словами, $S -$ подкольцо в R, если $S \subset R$, $0 \in S$ (здесь $0 -$ нулевой элемент в R) и $x + y, -x, xy \in S$ всякий раз, когда $x,y \in S$.

Тривиальными подкольцами в R являются *нулевое кольцо* $\{0\}$ и само R. Пересечение любого семейства подколец кольца R является его подкольцом. Поэтому для любого непустого подмножества $X \subseteq R$ существует наименьшее подкольцо, содержащее X. Обозначим его через $< X >$. Если $S = < X >$, то говорят, что X является *множеством* (*кольцевых*) *образующих* для S; если при этом S конечно, то говорят, что S *конечно порождено*.

Отметим, если $S -$ подкольцо в R, и S и R имеют единицы, то эти единицы могут не совпадать.

Пример. Множества квадратных матриц

$$M_1 = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix} \middle| \alpha \in \mathbb{Z} \right\} \text{ и } M_2 = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \middle| \alpha, \beta, \gamma, \delta \in \mathbb{Z} \right\}$$

относительно операций сложения и умножения матриц являются кольцами, причем M_1 подкольцо в M_2. Единицы у них разные: $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ и $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ соответственно для M_1 и M_2.

Всякое кольцо S может быть вложено в некоторое кольцо R с единицей. В качестве R можно взять, например, множество пар (x, m), где $x \in S$, $m \in \mathbb{Z}$, а операции определяются равенствами:

$$(x, m) + (y, n) = (x + y, m + n),$$
$$(x, m) \cdot (y, n) = (xy + nx + my, mn).$$

Элементы кольца S отождествляются с парами $(x, 0)$. Единицей в R служит пара $(0, 1)$. Про кольцо R говорят, что оно получено *внешним присоединении единицы*. Подчеркнём, что если в S существовала единица, то единица в R будет отлична от неё.

Определение. Элемент x кольца R называется нильпотентным, если $x^n = 0$ для некоторого $n \in \mathbb{N}$. Если при этом $x^{n-1} \neq 0$, то число n называется индексом нильпотентности элемента x. Если $x -$ нильпотентный элемент индекса n в кольце с единицей, то $1 - x -$ обратимый элемент, поскольку $(1 - x)(1 + x + x^2 + \cdots + x^{n-1}) = 1 = (1 + x + x^2 + \cdots + x^{n-1})(1 - x)$.

Очевидно, обратим и элемент $1 + x$.

Определение. Элемент z кольца R называется *центральным*, если $xz = zx$ для любого $x \in R$. Совокупность всех центральных элементов кольца R называется *центром кольца* R и обозначается как $Z(R)$.

32.1. ***Следствие.*** *$Z(R) -$ подкольцо кольца R.*

Доказательство оставляем читателю. □

Очевидно, что кольцо R коммутативно тогда и только тогда, когда его центр совпадает с самим кольцом, т.е. $Z(R) = R$.

Определение. Подкольцо J кольца R называется *двусторонним идеалом* (или просто *идеалом*), если $JR, RJ \subseteq J$ (т.е. $xy, yx \in J$ для любых $x \in J, y \in R$).

Замечание. В теории колец вводят понятия левого и правого идеалов. *Левый* (соответственно *правый*) *идеал* определяется как подкольцо J кольца R, для которого $JR \subseteq J$ (соответственно $RJ \subseteq J$). *Двусторонний* идеал $-$ подкольцо, одновременно являющееся как левым, так и правым идеалом. Для коммутативных колец понятия левого и правого идеалов совпадают. Мы будем рассматривать только двусторонние идеалы. □

Запись $J \lhd R$ означает, что $J -$ идеал кольца R.

Нулевое подкольцо $\{0\}$ и само кольцо R являются идеалами в R; первый из них называется *нулевым*, а второй $-$ *единичным* идеалами. Идеал кольца, отличающийся от нулевого и единичного, называется *собственным* идеалом кольца. Пересечение любого семейства идеалов кольца R является идеалом кольца R. При этом, если $I, J -$ идеалы в R, то $IJ \subset I \cap J$. В частности, идеалом оказывается пересечение всех идеалов, содержащих множество $X \subseteq R$. Этот идеал называется *идеалом, порождённым множеством* X и обозначается через $J = (X)$; при этом элементы множества X называются *образующими* идеала J.

Отметим, что не у всякого идеала существует конечная система образующих. Подкольца, порождённые множеством X, вообще говоря, меньше идеала порождённого тем же множеством, т.е. $< X > \subset (X)$, где включение может быть строгим.

Определение. Идеал, порождённый одним элементом, называется *главным*.

Нулевой идеал (0) всегда является главным; если кольцо обладает единицей, то $R = (1)$ − главный идеал. Для любого $x \in R$ главный идеал (x) составляют элементы вида

$$\sum_i y_i x z_i + \sum_j u_j x + \sum_k x v_k + m \cdot x,$$

где $y_i, z_i, u_j, v_k \in R$, $m \in \mathbb{Z}$, а при наличии в кольце R единицы − элементы вида

$$\sum_i y_i x\, z_i\,.$$

Если R − коммутативное кольцо, то эти выражения выглядят проще: соответственно как

$$\sum_i y_i x + mx \text{ и } \sum_i y_i x$$

Для более общего случая имеем:

$$(x_1, \ldots, x_n) = (x_1) + \cdots + (x_n).$$

Определение. Коммутативное кольцо с единицей, в котором каждый идеал является главным, называется *кольцом главных идеалов*.

32.2. ***Теорема.*** *В коммутативном кольце R с единицей множество $(a) = \{xa\}$ всех кратных $xa = ax$ любого фиксированного элемента $a \in R$ является идеалом в R.*

Доказательство. Если $xa \in (a)$ и $ya \in (a)$, то $xa \pm ya = (x \pm y)a \in (a)$, кроме того, для любого элемента $r \in R$ имеем $r(xa) = (rx)a \in R$ и $(xa)r = a(xr) \in R$. □

32.3. ***Следствие.*** *Коммутативное кольцо R с единицей является полем тогда и только тогда, когда оно не имеет собственных идеалов.*

Доказательство. Любое поле содержит два идеала: нулевое (0) и единичное (1). Других (т.е. собственных) идеалов в поле нет. Если R не является полем, то в R имеется необратимый элемент $a \neq 0$, среди кратных которого нет единицы. Поэтому (a) является собственным идеалом в R. □

Замечание. Следующий контрпример показывает, что как конечное, так и бесконечное некоммутативное кольцо, содержащее необратимый элемент, может не иметь собственных идеалов. Рассмотрим кольцо $R = M_2(\mathcal{F})$ матриц $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ второго порядка над произвольным полем $\mathcal{F}$. Пусть в этом кольце E^{hk} означает матрицу, у которой $a_{hk} = 1$, а на остальных местах нули. Другими словами,

$$E^{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, E^{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, E^{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, E^{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Пусть $H \subset R -$ ненулевой идеал в R и $A -$ матрица из этого идеала с ненулевым элементом a_{ij}. Тогда идеал должен содержать все матрицы вида $E^{hi}a_{ij}E^{jk} = a_{ij}E^{hk}$. Выберем любую матрицу $B = (b_{ij}) \in M_2(\mathcal{F})$. Так как $a_{ij} \neq 0$, то мы можем положить $c_{hk} = a_{ij}^{-1}b_{hk}$, а затем, обозначив через $c_{hk}I$ матрицу с элементами c_{hk} на главной диагонали и нулями вне её, мы можем представить B в виде

$$B = \sum_{h,k} c_{hk} I\, E^{hi} A E^{jk}.$$

Таким образом, $H = M_2(\mathcal{F})$. Отсюда следует, матричное кольцо не имеет собственных идеалов, причем оно конечно или бесконечно в зависимости от того, конечно или бесконечно $\mathcal{F}$. □

§ 33. Морфизмы колец

Определение. Пусть A, $B -$ кольца. Отображение $f: A \longrightarrow B$ называется *кольцевым гомоморфизмом*, если оно сохраняет обе операции, т.е.

$$f(x + y) = f(x) + f(y);$$
$$f(x \cdot y) = f(x) \cdot f(y)$$

для любых $x,y \in A$. (Знаки $+$ и $\cdot$ в левой и правой частях этих равенств имеют разный смысл: слева это операции в кольце A, справа в кольце B.)

Далее вместо “кольцевой гомоморфизм” будем говорить также “гомоморфизм колец” или просто “гомоморфизм”, если ясно, что речь идёт о кольцах.

Ядром кольцевого гомоморфизма $f: A \longrightarrow B$ называется множество

$$Ker\, f = \{\, a \in A \mid f(a) = 0_B \},$$

где $0_B -$ нуль в кольце B.

33.1. ***Теорема.*** *Ядро кольцевого гомоморфизма* $f: A \longrightarrow B$ *всегда является идеалом в* B.

Доказательство. Пусть $x \in Ker\ f$, $a \in A$. Тогда

$$f(ax) = f(xa) = 0_B \Longrightarrow ax, xa \in Ker\ f \Longrightarrow$$
$$A \cdot Ker\ f, Ker\ f \cdot A \subseteq Ker\ f.$$

Очевидно, что $Ker\ f$ − подкольцо в A, но тогда и идеал в A. □

33.2. ***Теорема.*** *Пусть* $f: A \longrightarrow B$ *− гомоморфизм колец. Тогда образ* $f(A)$ *отображения* f *− подкольцо в* B.

Доказательство. Поскольку f − гомоморфизм аддитивных абелевых групп, то, согласно теореме 18.2, $f(A)$ − аддитивная абелева группа (подгруппа группы $(B, +)$). Пусть $a, b \in f(A)$, а $x, y \in A$ таковы, что $f(x) = a,\ f(y) = y$. Тогда $ab = f(x)f(y) = f(xy) \Longrightarrow ab \in f(A)$, т.е. $f(A)$ замкнуто относительно умножения в B. Поскольку остальные аксиомы кольца − ассоциативность умножения и дистрибутивные законы − для $f(A)$ заведомо выполняются, то $f(A)$ − подкольцо в B. □

В дополнение к теореме отметим, что $f(n \cdot a) = n \cdot f(a)$ для любых $n \in \mathbb{Z}$, $a \in A$. Если A − кольцо с единицей, то $f(1)$ служит единицей кольца $f(A)$, но может не быть единицей кольца B. Элемент $f(1)$ обязан быть единицей кольца B, если $f(A) = B$.

Гомоморфизм $f: A \longrightarrow B$ называется:

мономорфизмом, или *инъективным гомоморфизмом*, если $Ker\ f = \{0\}$ (в этом случае f − инъекция, т.е.$f(x) \neq f(y)$, если $x \neq y$);

эпиморфизмом, или *сюръективным гомоморфизмом*, если образ отображения f совпадает с B, т.е. $f(A) = B$ (в этом случае f − сюръекция, т.е. для любого $b \in B$ существует $a \in A$ такой, что $f(a) = b$);

изоморфизмом, или *биективным гомоморфизмом*, если f мономорфно и эпиморфно (в этом случае f − биекция, т.е. взаимно однозначное отображение). Факт изоморфизма записывается как $A \cong B$.

33.2. ***Теорема.*** *Если* $f: A \longrightarrow B$ *− изоморфизм колец, то обратное* (*в теоретико-множественном смысле*) *отображение* $f^{-1}: B \longrightarrow A$ *также является изоморфизмом колец.*

Доказательство этого утверждения нетрудно осуществить по аналогии с доказательством соответствующего утверждения об изоморфизмах групп. □

Ясно, что инъективный кольцевой гомоморфизм $f: A \longrightarrow B$ устанавливает изоморфизм между кольцом A и его образом $f(A)$.

§ 34. Классы вычетов и факторкольца

Пусть J – идеал кольца R. Поскольку каждый идеал кольца является нормальной подгруппой аддитивной группы кольца, то идеал J задаёт некоторое разбиение множества R на смежные классы по аддитивной подгруппе J. В данном случае эти классы называются *классами вычетов кольца R по модулю идеала J*. Соответствующее множество классов (фактор-множество) обозначим через $R\,/\,J$. Класс вычетов, содержащий элемент $a \in R$, будем обозначать через $[a] = a + J$; он состоит из элементов вида $a + x$, $x \in J$. Так как один и тот же класс может быть представлен разными элементами, то будет уместно напомнить, что $[a] = [b] \Leftrightarrow a - b \in J$.

34.1. ***Лемма.*** *Пусть* $[a] = [b]$ *и* $[c] = [d]$. *Тогда* $[a + c] = [b + d]$ *и* $[ac] = [bd]$.

Доказательство. Из $[a] = [b]$ и $[c] = [d]$ следует, что $a = b + j_1$ и $c = d + j_2$ для некоторых $j_1, j_2 \in J$. Тогда

$(a + c) - (b + d) = b + d + j_1 + j_2 - (b + d) = j_1 + j_2 \in J \Longrightarrow [a + c] = [b + d]$;

$ac - bd = (b + j_1)(d + j_2) - bd = bj_2 + j_1(d + j_2) \in J \Longrightarrow [ac] = [bd]$. □

На элементах (классах) множества $R\,/\,J$ определим операции $\oplus$ (сложение) и $\odot$ (умножение), полагая:

$$[a] \oplus [b] = [a + b],$$
$$[a] \odot [b] = [a \cdot b].$$

Из доказанной выше леммы следует, что эти операции определены корректно, т.е. не зависят от выбора представителей классов вычетов.

34.2. ***Теорема.*** *Структура* $(R\,/\,J, \oplus, \odot)$ *является кольцом, которое называют факторкольцом кольца R по идеалу J.*

Доказательство. Проверим выполнимость аксиом кольца. Тот факт, что $(R\,/\,J, \oplus)$ – группа по существу уже доказан ранее в теореме 20.2. Сложение коммутативно:

$$[a] \oplus [b] = [a + b] = [b + a] = [b] \oplus [a].$$

Значит, группа $(R\,/\,J, \oplus)$ абелева.

Операция умножения ассоциативна:

$$([a] \odot [b]) \odot [c] = [ab] \odot [c] = [abc] = [a] \odot [bc] = [a] \odot ([b] \odot [c]).$$

Дистрибутивные законы также выполняются:

$$([a] \oplus [b]) \odot [c] = [a + b] \odot [c] = [ac + bc] = [ac] \oplus [bc] = ([a] \odot [c]) \oplus ([b] \odot [c]),$$
$$[a] \odot ([b] \oplus [c]) = [a] \odot [b + c] = [ab + ac] = [ab] \oplus [ac]$$

$$= ([a] \odot [b]) \oplus ([a] \odot [c]). \ \square$$

Элементы $a, b \in R$, принадлежащие одному и тому же классу вычетов по модулю идеала J, будем называть *сравнимыми по модулю J* и записывать это как $a \equiv b \ (mod\ J)$. Отметим следующие свойства определённого таким образом сравнения:

1) если $a \equiv b \ (mod\ J)$, то

$a + r \equiv b + r \ (mod\ J)$,

$ar \equiv br \ (mod\ J)$, $ra \equiv rb \ (mod\ J)$ и $n \cdot a \equiv n \cdot b \ (mod\ J)$

для любых $r \in R$ и $n \in \mathbb{Z}$;

2) если, кроме того, $r \equiv s \ (mod\ J)$, то

$a + r \equiv b + s \ (mod\ J)$ и $ar \equiv bs \ (mod\ J)$.

Пример. Пусть $R = (\mathbb{Z}, +, \cdot)$ − кольцо целых чисел, $J = (\ n\,\mathbb{Z}, +, \cdot) = (n)$, где $n \in \mathbb{N}$, − идеал (главный) в кольце $\mathbb{Z}$, состоящий из чисел, кратных n. Элементами кольца $(\mathbb{Z}\ /\ n\mathbb{Z}, \oplus, \odot)$ являются смежные классы с операциями: $[a] \oplus [b] = [c]$, $[a] \odot [b] = [d]$, где c и d − остатки от деления соответственно $a + b$ и $a \cdot b$ на n. Это кольцо называют *кольцом целых чисел по модулю* n и обозначают обычно через $\mathbb{Z}_n$.

§ 35. Кольцо $\mathbb{Z}_n$

35.1. ***Теорема.*** *Кольцо $\mathbb{Z}_n$ является полем тогда и только тогда, когда n − простое число.*

Доказательство. Пусть n − составное число, т.е. $n = ab$ для некоторых целых $1 < a, b < n$. Тогда $[a][\ b] = [ab] = [n] = [0]$, откуда следует, что $\mathbb{Z}_n$ − кольцо с делителями нуля. Значит, $\mathbb{Z}_n$ − не поле.

Теперь предположим, что $n = p$ − простое число. Пусть $[a] \in \mathbb{Z}_n$ – любой ненулевой элемент. Так как $ar \not\equiv as \ (mod\ p)$ при $r \not\equiv s \ (mod\ p)$, то элементы $[1a]$, $[2a]$, …, $[(p-1)a]$ различны и совпадают с элементами $[1]$, $[2]$, …, $[(p-1)]$ (но, возможно, в другом порядке). Тогда

$[1][2] \ldots [(p-1)] = [1a][2a] \ldots [(p-1)a] = [1][2] \ldots [(p-1)][a^{p-1}]$.

На языке сравнений это означает, что $1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \cdot a^{p-1} \ (mod\ p)$. Так как числа $1, 2, \ldots, (p-1)$ взаимно просты с p, то обе части полученного сравнения можно сократить на эти числа. В результате получаем $a^{p-1} \equiv 1 (mod\ p) \Longrightarrow [a^{p-1}] = [1] \Longrightarrow [a^{p-2}]\,[a] = [1] \Longrightarrow [a]^{-1} = [a]^{p-2}$, т.е. $[1]$ – единица в $\mathbb{Z}_p$, а элемент $[a]$ имеет обратный. Значит, $\mathbb{Z}_p$ − поле. $\square$

Замечание. Из этой теоремы следует, что существуют поля, содержащие конечное число элементов. Они находят многочисленные применения в различных областях математики. *Конечное поле*, содержащее q элементов, будем обозначать через $\mathbb{F}_q$ (используют также обозначение $\mathrm{GF(q)} -$ от $Galois\ Field -$ поле Галуа [27] $-$ по имени фр. математика Э. Галуа, заложившего фундаментальные основы теории групп). В частности, $\mathbb{F}_p = \mathbb{Z}_p$, если $p -$ простое число. Заметим, что $\mathbb{Z}_4$ и $\mathbb{Z}_6$, как кольца с делителями нуля, не являются полями. Вместе с тем поле $\mathbb{F}_4$ существует, а поле $\mathbb{F}_6$ не существует. Далее будет установлено, при каких q существует поле $\mathbb{F}_q$, и уточнено строение этих полей. □

§ 36. Теорема о гомоморфизмах колец

36.1. ***Теорема.*** *Пусть A, B − кольца. Тогда*:

1) *Если $\varphi: A \longrightarrow B -$ сюръективный гомоморфизм, то $J = Ker\ \varphi -$ идеал в A, а $B \cong A\ /\ J$.*

2) *Обратно, если $J -$ идеал в A, то отображение $\psi: A \to A\ /\ J$, определяемое по правилу $\psi(a) = [a] = a + J$, является сюръективным гомоморфизмом с ядром $Ker\ \psi = J$. Гомоморфизм ψ называют естественным, или каноническим.*

Доказательство. 1) Тот факт, что $J -$ идеал в A, доказан в теореме 33.1. Покажем, что изоморфизм между $A\ /\ J$ и B устанавливается с помощью отображения μ, сопоставляющего классу вычетов $[a] = a + J \in A\ /\ J$ элемент $\varphi(a)$. Отображение μ определено корректно: если $[b]$ тот же класс вычетов. что и $[a]$, то $b = a + c$ для некоторого $c \in J$ и

$$\varphi(b) = \varphi(a + c) = \varphi(a) + \varphi(c) = \varphi(a),$$

---

[27] ***Эварист Галуа*** (25.10.1811 − 31.05.1832) − французский математик, основатель современной высшей алгебры, вышел на такие фундаментальные понятия, как группа (первым использовал этот термин, активно изучая симметрические группы) и поля (конечные поля носят его имя). Открытия Галуа произвели огромное впечатление и положили начало новому направлению — теории абстрактных алгебраических структур. Радикальный революционер-республиканец, погиб на дуэли в возрасте двадцати лет.

так что значение $\mu([a])$ определено однозначно. Далее, если $[a] \neq [b]$, то $\mu([a]) \neq \mu([b])$, поскольку в противном случае приходим к противоречию:

$$\varphi(a) = \varphi(b) \Longrightarrow \varphi(a) - \varphi(b) = 0 \Longrightarrow \varphi(a-b) = 0 \Longrightarrow a - b \in J \Rightarrow [a] = [b].$$

Следовательно, μ – инъекция. Поскольку φ – сюръекция, т.е. $\varphi(A) = B$, то для любого $b \in B$ найдётся $a \in A$ такой, что $\varphi(a) = b$. Отсюда следует, что и μ – сюръекция, но тогда μ − биекция. Кроме того, для любых $[a], [b] \in A / J$ имеем

$$\mu([a] + [b]) = \mu([a + b]) = \varphi(a + b) = \varphi(a) + \varphi(b) = \mu([a]) + \mu([b])$$

и, аналогично, $\mu([a] \cdot [b]) = \mu([a]) \cdot \mu([b])$. Следовательно, μ – изоморфизм.

2) Для любых $a,\ b \in A$ имеем $\psi(a + b) = [a + b] = [a] + [b] = \psi(a) + \psi(b)$ и, аналогично, $\psi(a \cdot b) = \psi(a) \cdot \psi(b)$. Следовательно, ψ – гомоморфизм, очевидно, сюръективный. Так как $a \in J \Longrightarrow \psi(a) = [0]$ и $a \notin J \Longrightarrow \psi(a) \neq [0]$, то $Ker\ \psi = J$. □

§ 37. Характеристика кольца *(поля)*

Определение. *Характеристикой* кольца R называется наименьшее $n \in \mathbb{N}$, при котором $n \cdot x = 0$ для любого $x \in \mathbb{N}$. Если такое n существует, то кольцо R называется *кольцом положительной характеристики* n. Если же такое n не существует, то говорят, что *характеристика кольца R равна нулю*, а само R называют *кольцом нулевой характеристики.*

Характеристика кольца R обозначается как $Char\ R$.

Примеры. 1) $\mathbb{Z}$ – кольцо, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ – поля нулевой характеристики. 2) $\mathbb{Z}_n$, где $n \in \mathbb{N}$, – конечное кольцо положительной характеристики n.

Если R – кольцо с единицей, то значение характеристики кольца полностью определяется аддитивными свойствами единицы: если $n \cdot 1 \neq 0$ при любом $n \in \mathbb{N}$, то $Char\ R = 0$; если же существуют n, при которых $n \cdot 1 = 0$, то $Char\ R = n_0$, где n_0 − наименьшее из таких n, поскольку $n \cdot 1 = 0 \Longrightarrow n \cdot x = (n \cdot 1) \cdot x = 0$.

37.1. ***Теорема.*** *Характеристика любого ненулевого кольца R с единицей и без делителей нуля равна либо нулю, либо некоторому простому числу p.*

Доказательство. Случай $Char\ R = 0$ возможен. Пусть $Char\ R = p > 0$. Так как R содержит не менее двух элементов, то $p \geq 2$. Допустим на минутку, что $p -$ составное число, т.е. $p = ab$, где $0 < a, b < p -$ некоторые целые. Тогда из $p \cdot 1 = (a \cdot 1)(b \cdot 1) = 0$ следует, что или $(a \cdot 1) = 0$, или $(b \cdot 1) = 0$ (либо и то, и другое). Пусть, для определённости, $(a \cdot 1) = 0$, но тогда $Char\ R \leq a < p$, что противоречит выбору числа p. Значит, $p -$ простое число. □

37.2. ***Теорема*** (Равенство Шёнемана [28]). *В коммутативном кольце R простой характеристики $p > 0$ имеет место тождество* $(x \pm y)^{p^n} = x^{p^n} \pm y^{p^n}$ *для всех* $x,y \in R$ *и* $n \in \mathbb{N}$.

Доказательство. Так как $\binom{p}{k} \equiv 0\ (mod\ p)$ для любых $0 < k < p$, то

$$(x + y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k = x^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k} + y^p = x^p + y^p.$$

Используя индукцию по n, устанавливаем первое тождество: $(x + y)^{p^n} = x^{p^n} + y^{p^n}$, а из него вытекает второе: $x^{p^n} = ((x - y) + y)^{p^n} = (x - y)^{p^n} + y^{p^n}$. □

37.3. ***Следствие.*** *При тех же предположениях имеем* $(x_1 + \cdots + x_m)^{p^n} = {x_1}^{p^n} + \cdots + {x_m}^{p^n}$ *для всех* $x_1,\ldots,x_m \in R$ *и* $n, m \in \mathbb{N}$.

Определение. *Подполем* $\mathcal{P}$ поля $\mathcal{F}$ называется подкольцо в $\mathcal{F}$, само являющееся полем.

Например, $\mathbb{Q} -$ поле рациональных чисел $-$ является подполем поля $\mathbb{R}$ вещественных чисел, которое, в свою очередь, является подполем поля $\mathbb{C}$ комплексных чисел.

Если $\mathcal{P} \subset \mathcal{F}$, то говорят, что поле $\mathcal{F}$ является *расширением* своего подполя $\mathcal{P}$ (или *надполем* по отношению к $\mathcal{P}$). Из определения подполя следует, что нуль и единица поля $\mathcal{F}$ лежат в $\mathcal{P}$ и также являются для $\mathcal{P}$ нулём и единицей.

37.4. ***Теорема.*** *Пересечение подполей* ${\mathcal{P}}_1$ *и* ${\mathcal{P}}_2$ *поля* $\mathcal{F}$ *является подполем в* $\mathcal{F}$.

---

[28] ***Теодор Шёнеман*** (4.04.1812 – 16.01.1868) $-$ немецкий математик. Получил ряд важных результатов в теории чисел, касающихся теории сравнений по простому модулю.

Доказательство. Достаточно проверить выполнимость аксиом поля для $\mathcal{P}_0 = \mathcal{P}_1 \cap \mathcal{P}_2$. □

Определение. Поле называется *простым*, если оно не содержит никаких подполей, отличных от него самого.

Пример. 1) Поле $\mathbb{Z}_p$ – простое поле для любого простого числа p. Это следует из того, что аддитивная группа $(\mathbb{Z}_p, +)$ имеет простой порядок и по теореме Лагранжа не имеет собственных подгрупп. 2) $\mathbb{Q}$ – простое поле. В данном случае, наряду с числом 1, простое подполе поля $\mathbb{Q}$ должно содержать все кратные ему, а также все дроби. Но это и будет множество $\mathbb{Q}$.

Отметим, что других простых полей, по существу отличающихся от указанных в примере, нет, о чём свидетельствует следующая

37.4. ***Теорема.*** *Каждое поле $\mathcal{F}$ содержит только одно простое поле $\mathcal{P}_0$, причём $\mathcal{P}_0 \cong \mathbb{Q}$, если $Char\ \mathcal{F} = 0$, и $\mathcal{P}_0 \cong \mathbb{Z}_p$, если $Char\ \mathcal{F} = p > 0$.*

Доказательство. Допуская существование двух простых подполей $\mathcal{P}_1$ и $\mathcal{P}_2$ поля $\mathcal{F}$, мы неизбежно придём к противоречию, поскольку их пересечение $\mathcal{P}_0 = \mathcal{P}_1 \cap \mathcal{P}_2$ содержится как в $\mathcal{P}_1$, так и в $\mathcal{P}_2$, отлично от них и является подполем поля $\mathcal{F}$. Значит, простое поле $\mathcal{P}_0 \subset \mathcal{F}$ единственно.

Уточним структуру поля $\mathcal{P}_0$. Это поле, как всякое подполе поля $\mathcal{F}$, содержит единицу $e = 1$ поля $\mathcal{F}$. Элементы вида $n \cdot 1$, $n \in \mathbb{Z}$, с операциями $m \cdot 1 + n \cdot 1 = (m + n) \cdot 1$, $(m \cdot 1)(n \cdot 1) = (mn) \cdot 1$, $m,n \in \mathbb{Z}$, образуют коммутативное кольцо A, являющееся подкольцом поля $\mathcal{P}_0$. Рассмотрим отображение $\psi : \mathbb{Z} \longrightarrow A$, определяемое правилом $\psi(n) = n \cdot 1$. Это отображение является сюръективным гомоморфизмом кольца $\mathbb{Z}$ на кольцо A с ядром $Ker\ \psi = p\mathbb{Z} = (p)$. По теореме о гомоморфизмах колец $A \cong \mathbb{Z} / p\mathbb{Z}$. Возможны два случая:

1. $p = 0$. В этом случае ядро тривиально, т.е. $Ker\ \psi = \{0\}$. Следовательно, ψ – изоморфизм ($A \cong \mathbb{Z}$) и дроби $\frac{m \cdot 1}{n \cdot 1}$, имеющие смысл в $\mathcal{F}$ (поскольку $\mathcal{F}$ – поле), образуют поле, изоморфное $\mathbb{Q}$. Оно и будет простым подполем в $\mathcal{F}$.

2. $p > 0$. Поскольку $p = Char\ \mathcal{F}$ – простое число, то $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$ – поле. Так что $A \cong \mathbb{Z}_p$ – поле. Поскольку $A \subset \mathcal{P}_0$, то на самом деле $\mathcal{P}_0 = A \cong \mathbb{Z}_p$. □

§ 38. Кольцо многочленов от одной переменной

Пусть $\mathcal{R}$ – коммутативное кольцо с единицей 1.

Определение. *Многочленом* (или *полиномом*) над кольцом $\mathcal{R}$ называется формальное выражение вида

$$a(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n,$$

где a_0, …, a_n – элементы кольца $\mathcal{R}$, называемые *коэффициентами* многочлена, $n \in \mathbb{Z}$, $n \geq 0$, x – некоторый (формальный) символ, не принадлежащий кольцу $\mathcal{R}$, называемый *переменной* (или *неизвестной*).

Замечание. Данное определение на самом деле не является достаточно строгим. В нём есть одно сомнительное место, касающееся связи коэффициентов a_i и посторонней переменной x. Этого вопроса обычно избегают. Однако можно дать совершенно безукоризненное определение многочлена как элемента кольца многочленов. Изложим его вкратце.

Рассмотрим множество S всех бесконечных последовательностей $f = (a_0,a_1,a_2,\dots)$, $a_i \in \mathcal{R}$, у которых все a_i, кроме конечного числа, равны нулю. Для $f = (a_0,a_1,a_2,\dots)$ и $g = (b_0,b_1,b_2,\dots) \in S$ определим сумму $f + g$ и произведение $f \cdot g$, полагая

$$f + g = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots),$$
$$f \cdot g = (c_0,c_1,c_2,\dots),$$

где

$$c_n = a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0 = \sum_{i=0}^{n} a_i b_{n-i},\ n = 0, 1, 2, \dots$$

Относительно этих операций S является коммутативным кольцом с единицей $\mathbf{1} = (1,0,0,\dots)$. Действительно, сложение и умножение двух последовательностей с конечным числом ненулевых членов даёт снова аналогичную последовательность. Сложение последовательностей ассоциативно и коммутативно. Нулём в S является нулевая последовательность $\mathbf{0} = (0,0,0,\dots)$, противоположным для $f = (a_0,a_1,a_2,\dots)$ является элемент $g = (-a_0,-a_1,-a_2,\dots)$. Умножение в S ассоциативно: пусть $f = (a_0,a_1,a_2,\dots)$, $g = (b_0,b_1,b_2,\dots)$, $h = (c_0,c_1,c_2,\dots)$ – три произвольных элемента из S; тогда

$$f \cdot g = (d_0,d_1,d_2,\dots),\ (f \cdot g) \cdot h = (e_0,e_1,e_2,\dots),$$

где

$$d_m = \sum_{\substack{0\le i,j\le m\\ i+j=m}} a_i b_j, \quad e_n = \sum_{\substack{0\le m,k\le n\\ m+k=n}} d_m c_k = \sum_{\substack{0\le m,k\le n\\ m+k=n}} c_k \sum_{\substack{0\le i,j\le m\\ i+j=m}} a_i b_j = \sum_{\substack{0\le i,j,k\le n\\ i+j+k=n}} a_i b_j c_k.$$

Вычисление $f \cdot (g \cdot h)$ даёт тот же результат. Поскольку умножение в исходном кольце $\mathcal{R}$ коммутативно, то оно коммутативно и в S. Наконец, в S выполняется дистрибутивный закон: $f \cdot (g + h) = f \cdot g + f \cdot h$. Значит, $S -$ коммутативное кольцо с единицей.

Множество $\mathcal{P}$ последовательностей $(a_0,0,0,\dots)$, у которых лишь первая компонента может быть ненулевой, образует в S подкольцо, изоморфное $\mathcal{R}$ (изоморфизм задаётся соответствием $(a_0,0,0,\dots) \longmapsto a_0$). Отождествляя $\mathcal{P}$ и $\mathcal{R}$, можно считать, что $\mathcal{R} -$ подкольцо в S, а $S -$ расширение кольца $\mathcal{R}$. Обозначим через X последовательность $(0,1,0,0,\dots)$ и назовём X *переменной* (или *неизвестной*) над $\mathcal{R}$. Легко проверить, что $X^n = (0,\dots,0,1,0,\dots)$ для всех $n \in \mathbb{N}$, где 1 является $(n+1)$-ой компонентой. Если, кроме того, положить $X^0 = (1,0,0,\dots) = 1$, то для любой последовательности $f = (a_0,a_1,a_2,\dots) \in S$ имеем:

$$(a_0, a_1, a_2,\dots) = (a_0,0,0,\dots) + (0,a_1,0,\dots) + (0,0,a_2,0,\dots) + \cdots$$
$$= (a_0,0,\dots)(1,0,0,\dots) + (a_1,0,0,\dots)(0,1,0,\dots) + (a_2,0,\dots)(0,1,\dots) + \cdots$$
$$= a_0\,(1,0,0,\dots) + a_1(0,1,0,\dots) + a_2\,(0,0,1,\dots) + \cdots$$
$$= a_0 + a_1X + a_2X^2 + \cdots + a_nX^n + \cdots$$

Таким образом, если $a_n -$ последний ненулевой элемент в f, то в новых обозначениях $f = f(X) = a_0 + a_1X + \cdots + a_nX^n$. Такое представление f единственно. Действительно, если допустить, что $g = b_0 + b_1X + \cdots + b_nX^n$ – другое представление f, то $f - g = (0,0,0,\dots) = (a_0 - b_0) + (a_1 - b_1)X + \cdots + (a_n - b_n)X^n = (a_0 - b_0,\dots,a_n - b_n,0,\dots)$, откуда следует, что $a_n = b_n,\dots,a_0 = b_0$.

Определение. Введённое кольцо S обозначается через $\mathcal{R}[X]$ и называется *кольцом многочленов над $\mathcal{R}$ от одной переменной X*, а его элементы $-$ *многочленами* (или *полиномами*).

Замечание об обозначениях. Присвоение последовательности названия переменной или неизвестной не более чем терминологическая условность. Для обозначения этой переменной используется заглавная буква X (или другая буква Y, Z,...), чтобы отличить специально выделенный многочлен $f = X$ от теоретико-функциональной переменной x, пробегающей некоторое множество значений. В следующих разделах будем придерживаться таких обозначений. В тех случаях, когда из контекста ясно, какая переменная имеется в виду, для обозначения многочлена $f(X)$ используется символ f.

Многочлены над кольцом обычно определяют как формальные выражения вида (см. начало данного раздела) $f(X) = a_0 + a_1X + \cdots + a_nX^n$, где a_i – элементы кольца $\mathcal{R}$, а X – некоторый символ, не принадлежащий кольцу $\mathcal{R}$. Основным доводом в пользу используемого здесь определения многочленов $f(X)$ над $\mathcal{R}$ является прояснение связи между элементами $a \in \mathcal{R}$ и новым элементом X. Переход от кольца $\mathcal{R}$ к кольцу S называется *кольцевым присоединением элемента* X к кольцу $\mathcal{R}$. Кольцо $\mathcal{R}[X]$ является подкольцом кольца $\mathcal{R}[[X]]$ формальных степенных рядов. □

Пусть $f(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathcal{R}[X]$ – многочлен над кольцом $\mathcal{R}$. Элементы a_i называют *коэффициентами* многочлена f. Если все коэффициенты равны нулю, то многочлен f называют *нулевым* и пишут $f = 0$. Коэффициент a_0 при X^0 называют *постоянным членом*. Если f – ненулевой многочлен, то наибольшее n, для которого $a_n \neq 0$, называют *степенью* многочлена и пишут $n = deg\, f$ или $deg\, f\,(X)$; при этом a_n называют *старшим коэффициентом* многочлена f. Нулевому многочлену приписывают степень $-\infty$ (при этом $-\infty + (-\infty) = -\infty$, $-\infty + n = -\infty$, $-\infty < n$ для каждого $n \in \mathbb{N}$).

В записи многочлена члены a_iX^i с $a_i = 0$ можно опускать, но можно и добавлять. В частности, многочлен $f(X)$ можно записать в эквивалентной форме

$$f(X) = a_0 + a_1X + \cdots + a_nX^n + 0 \cdot X^{n+1} + \cdots + 0 \cdot X^{n+h},$$

где $h \in \mathbb{N}$ – любое число. Поэтому при сравнении двух многочленов $f(X)$ и $g(X)$ над $\mathcal{R}$ можно предполагать, что они содержат одни и те же степени переменной. Многочлен вида a_iX^i называют *одночленом*, или *мономом*. Многочлены

$$f(X) = a_0 + a_1X + \cdots + a_nX^n \quad \text{и} \quad g(X) = b_0 + b_1X + \cdots + b_nX^n$$

над $\mathcal{R}$ считаются *равными* тогда и только тогда, когда $a_i = b_i$ для всех $0 \leq i \leq n$.

Многочлены степени ≤ 0 называют *постоянными* многочленами, или *константами*. Если кольцо $\mathcal{R}$ имеет единицу (1) и если старший коэффициент многочлена f равен 1, то многочлен f называется *нормированным* (его также называют *приведённым* или *унитарным*).

Вычисление старших коэффициентов в сумме и произведении двух многочленов приводит к следующему утверждению:

38.1. ***Теорема.*** *Пусть* $f, g \in \mathcal{R}[X]$. *Тогда*

$$deg\,(f + g) \leq max\,(deg\, f, deg\, g),$$
$$deg\,(f \cdot g) \leq deg\, f + deg\, g.$$

Если $\mathcal{R}$ – целостное кольцо, то

$$deg\,(f \cdot g) = deg\,f + deg\,g.$$

Некоторые свойства кольца $\mathcal{R}$ наследуются кольцом $\mathcal{R}[X]$. В частности, имеет место

38.2. ***Теорема.*** *Кольцо $\mathcal{R}[X]$ является целостным кольцом тогда и только тогда, когда $\mathcal{R}$ – целостное кольцо.*

38.3. ***Теорема.*** *Пусть $\mathcal{K}$ – коммутативное кольцо, содержащее кольцо $\mathcal{R}$ в качестве подкольца. Тогда для каждого элемента $\beta \in \mathcal{K}$ существует единственный гомоморфизм колец*

$$\varphi_\beta : \mathcal{R}[X] \to \mathcal{K}$$

такой, что

$$\varphi_\beta(a) = a \text{ для всех } a \in \mathcal{R} \text{ и } \varphi_\beta(X) = \beta. \qquad (1)$$

Доказательство. Допустим вначале, что указанный гомоморфизм φ_β существует. Поскольку $\varphi_\beta(a_i) = a_i$ для каждого коэффициента многочлена $f = a_0 + a_1X + \cdots + a_nX^n$ и $\varphi_\beta(X^k) = \beta^k$, то

$$\varphi_\beta(f) = \varphi_\beta(a_0 + a_1X + \cdots + a_nX^n) = a_0 + a_1\beta + \cdots + a_n\beta^n, \qquad (2)$$

т.е. гомоморфизм определён однозначно и выражается формулой (2). Ясно, что отображение (1) удовлетворяет условию (2). Остаётся показать, это отображение можно взять в качестве искомого, т.е. оно является гомоморфизмом. Пусть $f(X) = a_0 + a_1X + \cdots + a_mX^m$ и $g(X) = b_0 + b_1X + \cdots + b_nX^n$ – любые многочлены из $\mathcal{R}[X]$. Тогда

$$\varphi_\beta(f + g) = (a_0 + b_0) + (a_1 + b_1)\beta + (a_2 + b_2)\beta^2 + \cdots$$
$$= \varphi_\beta(f) + \varphi_\beta(g),$$

$$\varphi_\beta(f \cdot g)$$
$$= \varphi_\beta(a_0b_0 + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2 + \cdots + a_mb_nX^{m+n})$$
$$= a_0b_0 + (a_0b_1 + a_1b_0)\beta + (a_0b_2 + a_1b_1 + a_2b_0)\beta^2 + \cdots + a_mb_n\beta^{m+n}$$
$$= \varphi_\beta(f) \cdot \varphi_\beta(g).$$

Другими словами, отображение (2) – кольцевой гомоморфизм. □

Результат применения отображения φ_β, определяемого формулой (2), к многочлену $f = f(X)$ называется *подстановкой* β в f, или *значением* f при $X = \beta$. При этом многочлену

$$f(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathcal{R}[X]$$

сопоставляется значение

$$f(\beta) = a_0 + a_1\beta + \cdots + a_n\beta^n \in \mathcal{K}.$$

Если $g(X)$ – любой другой (или тот же многочлен), то все соотношения между $f(X)$ и $g(X)$, основанные на сложении и умножении,

остаются в силе при замене X на любой элемент $\beta \in \mathcal{K}$. Другими словами,

$$f(X) + g(X) = r(X),\ f(X) \cdot g(X) = s(X) \Longrightarrow f(\beta) + g(\beta) = r(\beta),\ f(\beta) \cdot g(\beta) = s(\beta).$$

Гомоморфизмы φ_β – связующее звено между алгебраической и функциональной точками зрения на многочлены.

§ 39. Деление многочленов над целостным кольцом

Пусть $\mathcal{K}$ – целостное кольцо.

39.1. ***Теорема*** (Об однозначности деления с остатком). *Пусть $g \in \mathcal{K}[X]$ – многочлен с обратимым старшим коэффициентом. Тогда любому многочлену $f \in \mathcal{K}[X]$ сопоставляется одна и только одна пара многочленов q, r, для которых $f = qg + r, \deg r < \deg g$.*

Доказательство. Пусть

$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0,$

$g(X) = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_0,$

где $a_n\, b_m \neq 0$ и существует b_m^{-1} – обратный элемент для b_m. Применим индукцию по n. Если $n = 0$ и $m = \deg r > \deg f$, то положим $q = 0, r = f$; если $n = m = 0$, то положим $q = a_n\, b_m^{-1}, r = 0$. Допустим, что утверждение теоремы доказано для всех многочленов f степени $< n$ $(n > 0)$. Можно считать, что $n \geq m$, поскольку в противном случае $q = 0, r = f$. Коль скоро это так, то $f = a_n\, b_m^{-1} X^{n-m} g + f_1$, где $\deg f < n$. По предположению индукции существуют q_1 и r_1 такие, что $f_1 = q_1 g + r_1$, $\deg r_1 < m = \deg g$. Положив $q = a_n\, b_m^{-1} X^{n-m} + q_1$ и $r = r_1$, получим искомую пару многочленов.

Для доказательства единственности q и r предположим, что $f = qg + r = q'g + r'$. Тогда $(q - q')g = r' - r$. Так как $\mathcal{K}[X]$ – целостное кольцо, то $\deg(q - q') + \deg(g) = \deg(r' - r)$. Но это возможно только при $q = q'$ и $r = r'$. □

Многочлены q и r называют соответственно *частным* и *остатком* при делении f на g. Если $r = 0$, то говорят, что f *делится на* g, или f *кратно* g, и пишут $g \mid f$. Если $r \neq 0$, то пишут $g \nmid f$. Операции вычисления частного и остатка обозначим как $\boldsymbol{div}$ и $\boldsymbol{mod}$, так что $q = f\ div\ g$ и $r = f\ mod\ g$. Сам процесс вычисления частного и остатка q и r называют *евклидовым делением*. Если $\mathcal{K} = \mathcal{F}$ – поле, то деление на g всегда возможно, поскольку в поле все ненулевые элементы обратимы.

39.2. ***Следствие***. *В кольце* $\mathcal{F}[X]$ *многочленов над полем* $\mathcal{F}$ *все идеалы главные.*

Доказательство. Пусть J – любой ненулевой идеал в $\mathcal{F}[X]$. Выберем в J ненулевой многочлен g минимальной степени, и пусть f – любой другой многочлен из J. Разделим f на g, т.е. представим его в виде $f = qg + r,\ deg\, r < deg\, g$. Так как $r = f - qg \in J$ и $deg\, r < deg\, g$, то ввиду выбора g заключаем, что $r = 0$ – нулевой многочлен. Отсюда следует, что множество J состоит в точности из многочленов, кратных g. Значит, J – главный идеал. □

Замечание. Для колец многочленов от нескольких переменных данное утверждение неверно. Идеалы в $\mathcal{F}[X, Y, \ldots]$ не исчерпываются главными.

Пример. См. [16], с. 217. □

НОД *и* НОК *в кольце* $\mathcal{F}[X]$*, где* $\mathcal{F}$ *– поле.*

Определение. Пусть $f,\ g \in \mathcal{F}[X]$ – многочлены, не являющиеся одновременно нулевыми. Многочлен $d \in \mathcal{F}[X]$ наибольшей степени такой, что $d \mid f$ и $d \mid g$, называется *наибольшим общим делителем* многочленов f и g, и обозначается через НОД (f, g).

Отметим следующие свойства, используя которые нетрудно получить алгоритм вычисления d = НОД (f, g):

1) НОД $(f, g) = (g, f)$;

2) НОД $(f, 0) = f$;

3) если $deg\, g \le deg\, f$, то НОД $(f, g) =$ НОД (r, g), где $r = f\ mod\ g$.

Алгоритм Евклида вычисления d = НОД (f, g)

```
while deg f ≥ 0 and deg g ≥ 0 do
    if deg f ≥ deg g then f ← f mod g else g ← g mod f;
d ← f + g.
```

По аналогии с НОД (f, g) вводится дуальное понятие – *наименьшее общее кратное* $m =$ НОК $[f, g]$, где $fg \neq 0$, – многочлен наименьшей степени такой, что $f \mid m$ и $g \mid m$.

Замечание. Если НОД (a, b) целых чисел $a,\ b$ определён однозначно, то $d(X) =$ НОД $(f(X), g(X))$ для многочленов f и g определён с точностью до умножения на ненулевой элемент c поля $\mathcal{F}$. Иными словами, наряду с $d(X)$ многочлен $cd(X)$ также является наибольшим общим делителем многочленов f и g. Чтобы устранить неоднозначность, выберем среди многочленов $cd(X)$ унитарный, т.е.

тот, у которого старший коэффициент равен единице. Такое же уточнение сделаем и относительно наименьшего общего кратного. □

Если НОД $(f, g) = 1$, то многочлены f и g будем называть *взаимно простыми*.

Рассмотрим множество многочленов $J = \{af + bg \mid a, b \in \mathcal{F}[X]\}$. Нетрудно проверить, что $J -$ идеал в $\mathcal{F}[X]$. Согласно следствию 32.9, $J -$ главный идеал, т.е. $J = (d)$ для некоторого многочлена $d = af + bg \in \mathcal{F}[X]$. Используя алгоритм деления, запишем многочлен f в виде $f = qd + r$, где $deg\, r < deg\, d$. Ввиду $f, qd \in J$ имеет место включение

$$r = f - qd = f - q(af + bg) = (1 - qa)f + (-b)g \in J.$$

Отсюда следует, что $r = 0$, и, следовательно, $d \mid f$. Аналогично доказывается, что $d \mid g$. Пусть теперь $d' -$ любой делитель многочленов f и g. Тогда $d' \mid af, d' \mid bg \implies d' \mid (af + bg) \implies d' \mid d$. Очевидно, что d обладает всеми свойствами наибольшего общего делителя многочленов f и g. Значит, $d =$ НОД $(f,g) = af + bg$. Таким образом, доказана следующая

39.3. ***Теорема***. НОД $(f, g) = af + bg$ *для некоторых многочленов* $a, b \in \mathcal{F}[X]$.

Определение. Многочлен $f \in \mathcal{F}[X]$ степени $deg\, f > 0$ называется *неприводимым в* $\mathcal{F}[X]$ (или *неприводимым над полем* $\mathcal{F}$), если он не делится ни на какой многочлен $g(X) \in \mathcal{F}[X]$ степени $0 < deg\, g < deg\, f$.

39.4. ***Теорема***. *Множество унитарных неприводимых многочленов над любым полем* $\mathcal{F}$ *бесконечно.*

Доказательство. Это утверждение доказывается так же, как и соответствующее утверждение о бесконечности множества простых чисел в кольце $\mathbb{Z}$. □

Так как множество многочленов заданной степени над конечным полем конечно, то справедливо следующая

39.5. ***Теорема***. *Над конечным полем существуют неприводимые многочлены сколь угодно высокой степени.*

Замечание. На самом деле над конечным полем существуют неприводимые многочлены любой степени. Это же справедливо и для поля $\mathbb{Q}$ рациональных чисел. С другой стороны, над полем $\mathbb{R}$ вещественных чисел существуют неприводимые многочлены только первой и второй степени, а над полем $\mathbb{C}$ комплексных чисел $-$ неприводимые многочлены только первой степени. □

Неприводимые многочлены играют важную роль в кольце $\mathcal{F}[X]$, такую же, как и простые числа в кольце $\mathbb{Z}$.

39.6. ***Лемма***. *Пусть p,f,g − многочлены над полем $\mathcal{F}$. Тогда, если p − неприводимый над $\mathcal{F}$ многочлен и $p \mid fg$, то либо $p \mid f$, либо $p \mid g$* (*либо и то, и другое*).

39.7. ***Теорема*** (Основная теорема арифметики кольца $\mathcal{F}$[X] об однозначности разложения на неприводимые сомножители). *Пусть $\mathcal{F}$ − поле. Каждый многочлен $f \in \mathcal{F}[X]$ положительной степени может быть представлен в виде произведения*

$$f = ap_1^{e_1} \dots p_k^{e_k},$$

где $a \in \mathcal{F}$, $p_1, \dots, p_k$ − различные унитарные неприводимые многочлены из $\mathcal{F}[X]$, а $e_1, \dots, e_k$ − натуральные числа. Такое представление однозначно с точностью до порядка сомножителей. Оно называется каноническим разложением многочлена f в кольце $\mathcal{F}[X]$.

Доказательства утверждений 39.6 и 39.7 опускаются. Они аналогичны доказательствам соответствующих утверждений 6.4 и 6.5 о разложении чисел на простые множители в кольце $\mathbb{Z}$. □

Если $f = ap_1^{\alpha_1} \dots p_k^{\alpha_k}$, $g = bp_1^{\beta_1} \dots p_k^{\beta_k}$, где $a,b \in \mathcal{F}$, $ab \neq 0$; $p_1,\dots$, p_k − различные унитарные неприводимые в $\mathcal{F}$[X] многочлены; $\alpha_1,\dots,\alpha_k$, $\beta_1,\dots,\beta_k$ − неотрицательные целые числа, то

$$\text{НОД}\,(f, g) = p_1^{\gamma_1} \dots p_k^{\gamma_k}, \quad \text{НОК}\,[f, g] = p_1^{\delta_1} \dots p_k^{\delta_k},$$

где $\gamma_i = min\,\{\alpha_i, \beta_i\}$, $\delta_i = max\,\{\alpha_i, \beta_i\}$, $i = 1, 2, \dots, k$. Отсюда следует, что

$$a \cdot b \cdot \text{НОД}\,(f, g) \cdot \text{НОК}\,[f, g] = f \cdot g.$$

39.8. ***Теорема***. *Пусть $f \in \mathcal{F}[X]$. Факторкольцо $K = \mathcal{F}[X] / (f)$ является полем тогда и только тогда, когда f − неприводимый многочлен над полем $\mathcal{F}$.*

Доказательство. Элементами кольца K являются классы вычетов $[g] = g + (f)$, где $g \in \mathcal{F}[X]$. Классы вычетов $[g]$ и $[h]$ совпадают тогда и только тогда, когда $g - h \in (f)$, т.е. g и h при делении на f дают один и тот же остаток. Поэтому различные элементы в K можно описать явно, а именно это те классы $g + (f)$, где g пробегает множество многочленов из $\mathcal{F}[X]$ степени $< n = deg\,f$. Роль нуля и единицы в K играют классы вычетов $[0]$ и $[1]$, где 0 и 1 − нуль и единица поля $\mathcal{F}$.

Предположим, что f не является неприводимым многочленом. Тогда $f = ab$ для некоторых многочленов a, $b \in \mathcal{F}[X]$ степени

$0 < deg\, a,\ deg\, b < n$. Так как $[a]$ и $[b] \neq 0$ и $[a] \odot [b] = [f] = [0]$, то K не может быть полем, поскольку содержит делители нуля.

Теперь предположим, что f – неприводимый над $\mathcal{F}$ многочлен степени n. Пусть $c \in \mathcal{F}[X]$ – любой ненулевой многочлен степени $< n$ (так что $[c]$ – произвольный элемент кольца K). Многочлены f и c, очевидно, взаимно просты. Согласно теореме **39.3**
НОД $(f, g) = 1 = af + bc$ для некоторых $a, b \in \mathcal{F}[X]$. Но тогда

$$[1] = [af + bc] = ([a] \odot [f]) \oplus ([b] \odot [c]) =$$
$$([a] \odot [0]) \oplus ([b] \odot [c]) = [b] \odot [c],$$

т.е. элемент $[c]$ имеет обратный, а именно $[b]$. Значит, K – поле. □

§ 40. Корни многочленов

Пусть A – подкольцо с единицей целостного кольца B.

Определение. Элемент $\beta \in B$ называется *корнем* (или *нулём*) многочлена $f(x) \in A[x]$, если $f(\beta) = 0$. (Говорят также, что β – корень уравнения $f(x) = 0$.)

Замечание. Переход от кольца A к кольцу B (для которого A является собственным подкольцом) обычно обусловлен следующим обстоятельством. Многочлен $f(x) \in A[x]$ может не иметь корней в A. С другой стороны, ввиду $A[x] \subset B[x]$, многочлен $f(x)$ можно рассматривать как элемент кольца $B[x]$. При этом $f(x)$ может иметь корни в B. Например, многочлен $x^2 + 1$ не имеет корней в $\mathbb{R}$, но имеет два корня в $\mathbb{C}$ (именно: i и $-i$, где $i = \sqrt{-1}$). Как бы там ни было, мы рассмотрим сначала случай $B = A$. □

40.1. ***Теорема*** Безу [29]. *Элемент $\alpha \in A$ является корнем многочлена $f(x) \in A[x]$ тогда и только тогда, когда $f(x)$ делится на $x - \alpha$.*

Доказательство. Многочлен $f(x)$ может быть записан в виде $f(x) = q(x)(x - \alpha) + r(x)$, $deg\ r(x) < deg\ (x - \alpha) = 1$. Так как $f(\alpha) = r(\alpha)$, то $f(\alpha) = 0$ тогда и только тогда, когда $r(x)$ – нулевой многочлен. □

Определение. Элемент $\alpha \in A$ называется *корнем кратности e* (или *e-кратным корнем*) многочлена $f(x) \in A[x]$, если $f(x)$ делится

---

[29] ***Этьен Безу*** (31.03.1730 – 27.09.1783) – французский математик, член Французской академии наук (1758).

на $(x-\alpha)^e$, но не делится на $(x-\alpha)^{e+1}$. При $e=1$ корень α называется *простым*, а при $e>1$ *e-кратным*.

Очевидно, что $\alpha \in A$ является e- кратным корнем многочлена $f(x) \in A[x]$ тогда и только тогда, когда $f(x)=(x-\alpha)^e g(x)$, где $g(x) \in A[x]$ и $g(\alpha) \neq 0$. Так как $A[x]$ – целостное кольцо, то $deg\ f = e + deg\ g$.

40.2. ***Теорема***. *Если $\alpha_1, \dots, \alpha_s$ – различные корни ненулевого многочлена $f(x) \in A[x]$ кратностей $e_1, \dots, e_s$ соответственно, то*

$$f(x) = (x-\alpha_1)^{e_1} \dots (x-\alpha_s)^{e_s} g(x) \quad (1)$$

для некоторого многочлена $g(x)$ такого, что $g(\alpha_i) \neq 0$, $i = 1,\dots, s$. При этом

$$e_1 + \dots + e_s = deg\ f - deg\ g \leq deg\ f. \quad (2)$$

Доказательство. Применим индукцию по s. При $s=1$ доказывать нечего. Пусть доказано, что $f(x) = (x-\alpha_1)^{e_1} \dots (x-\alpha_r)^{e_r} h(x)$ для некоторых $r < s$ и многочлена $h(x) \in A[x]$ такого, что $h(\alpha_i) \neq 0$, $i = 1,\dots, r$. Подстановка $x = \alpha_{r+1}$ даёт $0 = f(\alpha_{r+1}) = (\alpha_{r+1} - \alpha_1)^{e_1} \dots (\alpha_{r+1} - \alpha_r)^{e_r} h(\alpha_{r+1})$. Так как A – целостное кольцо и $\alpha_{r+1} - \alpha_i \neq 0$, $i = 1,\dots, r$, то $h(\alpha_{r+1}) = 0$. Пусть $h(x) = (x - \alpha_{r+1})^t u(x)$, где $u(\alpha_{r+1}) \neq 0$ (и, очевидно, $u(\alpha_i) \neq 0$, $i = 1,\dots, r$). Тогда

$f(x) = (x-\alpha_{r+1})^{e_{r+1}} v(x) = (x-\alpha_1)^{e_1} \dots (x-\alpha_r)^{e_r} (x-\alpha_{r+1})^t u(x)$,

где $v(\alpha_{r+1}) \neq 0$. Допустим, что $t < e_{r+1}$. Тогда, используя закон сокращения в целостном кольце, получаем $(x-\alpha_{r+1})^{e_{r+1}-t} v(x) = (x-\alpha_1)^{e_1} \dots (x-\alpha_r)^{e_r} u(x)$, что, однако, невозможно ввиду $0 = (\alpha_{r+1} - \alpha_{r+1})^{e_{r+1}-t} = (\alpha_{r+1} - \alpha_1)^{e_1} \dots (\alpha_{r+1} - \alpha_r)^{e_r}$ и $(\alpha_{r+1}) \neq 0$.
Следовательно, $t \geq e_{r+1}$. Аналогично доказываем, что $t \leq e_{r+1}$. Поэтому $t = e_{r+1}$ и $f(x) = (x-\alpha_1)^{e_1} \dots (x-\alpha_{r+1})^{e_{r+1}} u(x)$, где $u(\alpha_i) \neq 0$, $i = 1,\dots, r+1$. Это и требовалось показать. Наконец, неравенство (2) непосредственно вытекает из (1). □

Замечание. Без предположения о целостности кольца A теорема неверна. Например, если $f(x) = x^3 \in \mathbb{Z}_8[x]$ (где $\mathbb{Z}_8$ – кольцо целых чисел по модулю 8), то $f(0) = f(2) = f(4) = f(6) = 0$; разложение $f(x)$ также неоднозначно: $x^3 = x(x-4)(x+4) = (x-2)(x^2+2x+4) = (x+2)(x^2-2x+4)$. □

Из теоремы 40.2 вытекает

40.3. ***Следствие***. *Ненулевой многочлен $f(x) \in A[x]$ степени n имеет, самое большее, n корней. Два многочлена $g, h \in A[x]$ степени*

n, принимающие одинаковые значения при подстановке $n+1$ различных элементов из A, равны: $g = h$.

Доказательство. Если допустить, что многочлен f имеет не менее $n+1$ корней, то возникает противоречие с неравенством в (2). Если $g \neq h$, то многочлен $f = g - h$ имеет степень $\leq n$, но не менее $n+1$ корней, что невозможно. □

§ 41. Производные многочленов. Характеризация корней многочленов

Пусть $\mathcal{F}$ – поле. Для характеризации корней многочленов от одной переменной над полем полезны производные и гиперпроизводные, определяемые ниже.

Определение. *Производной* многочлена

$$f(x) = \sum_{\nu=0}^{n} a_\nu x^\nu = a_0 + a_1 x + \cdots + a_n x^n \in \mathcal{F}[x]$$

называется многочлен

$$f'(x) = \sum_{\nu=0}^{n} \nu a_\nu x^\nu = a_1 + 2a_2 x + \cdots + n a_n x^{n-1} \in \mathcal{F}[x]. \qquad (1)$$

Отметим следующие свойства производной:

$$(af + bg)' = af' + bg', \qquad (2)$$

$$(fg)' = f'g + fg', \qquad (3)$$

которые имеют место для любых $a, b \in \mathcal{F}$ и $f, g \in \mathcal{F}[x]$. Соотношение (2) вытекает из определения производной, а доказательство (3) сводится к рассмотрению случая $f = x^m$, $g = x^n$: $(x^{m+n})' = (m+n)x^{m+n-1} = (m\,x^{m-1})x^n + x^m\,(nx^{n-1}) = (x^m)'x^n + x^m(x^n)'$.

Применяя индукцию по m соотношение (3) можно обобщить следующим образом:

$$(f_1 \cdots f_m)' = \sum_{i=1}^{m} f_1 \cdots f_{i-1} f_i' f_{i+1} \cdots f_m.$$

В частности, $(f^m)' = m f^{m-1} f'$.

Определение. *Производная порядка* m (кратко: m-ая *производная*) $f^{(m)}$ многочлена $f(x)$ определяется как $f^{(0)} = f$; $f^{(m)} = (f^{(m-1)})'$ для $m = 1, 2, \ldots$

Формула Лейбница. Применяя индукцию по m и учитывая соотношение

$$\binom{m}{s-1}+\binom{m}{s}=\binom{m+1}{s}$$

для биномиальных коэффициентов, получаем формулу, обобщающую соотношение (3) на случай m- ых производных:

$$(fg)^{(m)}=\sum_{s=0}^{m}\binom{m}{s}f^{(s)}g^{(m-s)} \quad \text{для } m=1,2,\dots$$

Если $\mathcal{F}-$ поле характеристики нуль, то $deg\ f'=(deg\ f)-1$. Для поля характеристики $p>0$ это, вообще говоря, неверно. Например, если многочлен $f\in\mathcal{F}[x]$ имеет вид

$$f=\sum_{\mu}b_{\mu}x^{p\mu}\in\mathcal{F}[x^{p}],$$

то $f'-$ нулевой многочлен, поскольку $(x^{p\mu})'=p\mu x^{p\mu-1}=0$, и $deg\ f'=-\infty$; в остальных случаях $f'-$ ненулевой многочлен, но $0\le deg\ f'\le(deg\ f)-1$ (более точно: если $f=\sum_{\nu}a_{\nu}x^{\nu}$, то $deg\ f'=m-1$, где m равно наибольшему ν, при котором $a_{\nu}\neq 0$ и $p\nmid\nu$). Относительно m-ых производных отметим, что $f^{(m)}=0$ при $m\ge(deg\ f)+1$, а если при этом $Char\ \mathcal{F}=p>0$, то и $f^{(m)}=0$ при $m\ge p$, и, следовательно, при $m\ge min\{p,(deg\ f)+1\}$.

§ 42. Интерполяционная формула Ньютона и гиперпроизводные Хассе

Пусть $\mathcal{F}-$ поле.

42.1. ***Теорема***. *Пусть $g_1,\dots,g_{s+1}\in\mathcal{F}[X]-$ любые (необязательно различные) многочлены со степенями $n_i=deg\ g_i\ge 1$. Тогда для любого многочлена $f\in\mathcal{F}[X]$, степень которого не превосходит $n=n_1+\cdots+n_{s+1}$, существуют однозначно определённые многочлены $r_0,\dots,r_s\in\mathcal{F}[X]$ такие, что $deg\ r_i<deg\ g_{i+1}$, $0\le i\le s$, и*

$$f=r_0+r_1g_1+r_2g_1g_2+\cdots+r_sg_1g_2\dots g_s. \qquad (1)$$

Доказательство. *Существование.* Если $deg\ f<deg\ g_1$, то возьмём $r_0=f$ и $r_i=0$ для $i>0$. Предположим, что $deg\ f\ge deg\ g_1$. Представим f в виде

$$f=r_0+f_1g_1,\ deg\ r_0<deg\ g_1 \qquad (2)$$

(r_0- остаток, а f_1- частное от деления f на g_1). Так как $deg\ f_1<deg\ f-deg\ g_1$, то по предположению индукции существуют многочлены $r_1,\dots,r_s\in\mathcal{F}[X]$ такие, что $deg\ r_i<deg\ g_{i+1}$, $1\le i\le s$, и

$$f_1=r_1+r_2g_2+\cdots+r_sg_2\dots g_s. \qquad (3)$$

Подставляя (3) в (2), получим искомое разложение (1).

Единственность. Допустим, что существуют два разложения, удовлетворяющие условиям теоремы:

$$r_0 + r_1 g_1 + r_2 g_1 g_2 + \cdots + r_s g_1 g_2 \ldots g_s = \rho_0 + \rho_1 g_1 + \rho_2 g_1 g_2 + \cdots + \rho_s g_1 g_2 \ldots g_s.$$

Тогда

$$0 = (r_0 - \rho_0) + (r_1 - \rho_1) g_1 + (r_2 - \rho_2) g_1 g_2 + \cdots + (r_s - \rho_s) g_1 g_2 \ldots g_s.$$

Очевидно, что g_1 делит $r_0 - \rho_0$, а так как $deg\ (r_0 - \rho_0) < deg\ g_1$, то $r_0 = \rho_0$. Разделив наше равенство на g_1, аналогично установим, что $r_1 = \rho_1$. Продолжая этот процесс, получим $r_2 = \rho_2, \ldots, r_s = \rho_s$. Это доказывает единственность разложения (1). □

42.2. *Следствие.* *Пусть $\alpha_1, \ldots, \alpha_n \in \mathcal{F}$ — любые элементы. Тогда любой многочлен $f \in \mathcal{F}[X]$ степени $\leq n$ представим в виде*

$$f(X) = \beta_0 + \sum_{\nu=1}^{n} \beta_\nu (X - \alpha_1) \ldots (X - \alpha_\nu) \qquad (4)$$

для однозначно определяемых констант $\beta_0, \ldots, \beta_n \in \mathcal{F}$.

Если $\alpha_1, \ldots, \alpha_n \in \mathcal{F}$ — различные элементы, то формула (1) называется *интерполяционной формулой Ньютона*, где коэффициенты последовательно определяются путём подстановки значений $x = \alpha_1, \ldots, x = \alpha_n$. Представление (4), где $g_1 = \cdots = g_{s+1} = g$ называется g-*адическим разложением* многочлена f. Если $g = x$, то g-адическое разложение совпадает с обычной записью многочлена f. Рассмотрим более подробно случай $g(X) = x - \alpha$, $\alpha \in \mathcal{F}$, уточняя значения коэффициентов $\beta_0, \ldots, \beta_n$ в разложении

$$f(X) = \beta_0 + \sum_{\nu=1}^{n} \beta_\nu (X - \alpha)^\nu. \qquad (5)$$

Определение. Для многочлена

$$f(X) = \sum_{\nu=0}^{n} a_\nu X^\nu \in \mathcal{F}[X]$$

определим его *гиперпроизводную порядка* m (кратко: m-*ую* гиперпроизводную) равенством

$$f^{[m]}(X) = \sum_{\nu=0}^{n} \binom{\nu}{m} a_\nu X^{\nu - m} \in \mathcal{F}[X], \qquad m = 0, 1, 2, \ldots$$

Стандартное соглашение о биномиальных коэффициентах, согласно которому $\binom{\nu}{m} = 0$ при $\nu < m$, гарантирует, что m-ая гиперпроизводная является многочленом над полем $\mathcal{F}$.

Гиперпроизводные обладают свойством линейности относительно поля $\mathcal{F}$:

$$(af + bg)^{[m]} = af^{[m]} + bg^{[m]}$$

для всех $a, b \in \mathcal{F}$ и $f, g \in \mathcal{F}[X]$.

42.3. ***Лемма.***

$$((X-\alpha)^e)^{[m]} = \binom{e}{m}(X-\alpha)^{e-m},\ m = 0,1,2,\ldots$$

Доказательство. Имеем

$$(X-\alpha)^e = \sum_{\nu=0}^{e}\binom{e}{\nu}(-\alpha)^{e-\nu}x^{\nu},$$

$$((X-\alpha)^e)^{[m]} = \sum_{\nu=m}^{e}\binom{\nu}{m}\binom{e}{\nu}(-\alpha)^{e-\nu}x^{\nu-m}$$

$$= \sum_{\nu=m}^{e}\binom{e}{m}\binom{e-m}{e-\nu}(-\alpha)^{e-\nu}x^{\nu-m}$$

$$= \binom{e}{m}\sum_{\mu=0}^{e-m}\binom{e-m}{e-m-\mu}(-\alpha)^{e-m-\mu}x^{\mu} = \binom{e}{m}(X-\alpha)^{e-m}. \quad \square$$

42.4. ***Теорема.*** *Для любого элемента $\alpha \in \mathcal{F}$ и любого многочлена $f \in \mathcal{F}[X]$ вида* (5) *имеет место следующее разложение в ряд Тейлора*:

$$f(X) = f^{[0]}(\alpha) + \sum_{\nu=1}^{n} f^{[\nu]}(\alpha)(X-\alpha)^{\nu}.$$

Доказательство. Учитывая лемму 42.3, имеем

$$f^{[m]}(X) = \sum_{\nu=0}^{n}\beta_\nu((X-\alpha)^\nu)^{[m]} = \beta_m + \sum_{\nu=m+1}^{n}\beta_\nu\binom{\nu}{m}(X-\alpha)^{\nu-m},$$

откуда следует, что $\beta_m = f^{[m]}(\alpha)$, $m = 0, 1, 2,\ldots$ $\square$

42.5. ***Следствие.*** *Элемент $\alpha \in \mathcal{F}$ является в точности e-кратным корнем многочлена $f \in \mathcal{F}[X]$ тогда и только тогда, когда $f^{[m]}(\alpha) = 0$ для $m = 0, 1, \ldots, e-1$, но $f^{[e]}(\alpha) \neq 0$.*

Доказательство. Если α – e-кратный корень, то из теоремы 42.4 следует, что $f^{[m]}(\alpha) = 0$ для $m = 0,1,\ldots, e-1$. При этом $f^{[e]}(\alpha) \neq 0$, так как в противном случае α будет $(e+1)$- кратным корнем. $\square$

Замечание. Идея использовать гиперпроизводные для исследования функций над полями ненулевой характеристики принадлежит Хассе, а также Тайхмюллеру [30] (1936), который исследовал основные свойства гиперпроизводных (см. [**24**], с.372, 405). Обычные производные $f^{(m)}$ и гиперпроизводные $f^{[m]}$ связаны соотношением: $f^{(m)}(x) = m!\, f^{[m]}(x)$, которое имеет место, если $Char\ \mathcal{F} = 0$ или $Char\ \mathcal{F} = p > 0$, но при этом $m < p$. Для данного случая следствие можно сформулировать так:

42.6. ***Следствие.*** *Пусть e – неотрицательное целое число, причём любое, если $Char\ \mathcal{F} = 0$, и $e < p$, если $Char\ \mathcal{F} = p > 0$. Элемент $\alpha \in \mathcal{F}$ является в точности e-кратным корнем многочлена $f \in \mathcal{F}[X]$ тогда и только тогда, когда $f^{(m)}(\alpha) = 0$ для $m = 0,1,\ldots, e-1$, но $f^{(e)}(\alpha) \neq 0$.*

§ 43. Интерполяционные формулы

43.1. ***Теорема*** (Интерполяционная формула Лагранжа). *Пусть $n \geq 1$; $a_0, a_1,\ldots,a_{n-1}$ – различные, и $b_0,b_1,\ldots,b_{n-1}$ – любые элементы поля $\mathcal{F}$. Тогда существует в точности один многочлен $f \in \mathcal{F}[X]$ степени $< n$ такой, что $f(a_i) = b_i$ для $i = 0, 1,\ldots, n-1$. Этот многочлен имеет вид*

$$f(X) = \sum_{i=0}^{n-1} b_i \chi_i(X), \quad \text{где } \chi_i(X) = \prod_{\substack{k=0 \\ k\neq i}}^{n-1} \frac{(X - a_k)}{(a_i - a_k)}.$$

Доказательство. Так как $\chi_i(a_j) = 0$ при $j \neq i$ и $\chi_i(a_i) = 1$, то $f(a_i) = b_i$ для $0 \leq i < n$. Пусть $g(X)$ – другой многочлен, обладающий теми же свойствами, что и $f(X)$. Тогда многочлен $h(X) = f(X) - g(X)$ степени $< n$ имеет n корней. Значит, $h(X)$ – нулевой многочлен, и $f(X)$ – единственный многочлен с требуемыми свойствами. □

---

[30] ***Пауль Юлиус Освальд Тайхмюллер*** (18.06.1913 – 11.09.1943) – немецкий математик, ученик Х. Хассе. "Заблудившийся гений". Сторонник рассистских взлядов и Третьего рейха. Погиб на Восточном фронте на Днепре под Полтавой.

Другие формулы. Пусть $f(X)$ – тот же многочлен, что и в теореме 43.1. Если $\mathcal{F} = \mathbb{F}_q$ – конечное поле, то

$$f(X) = \sum_{i=0}^{n-1} b_i(1-(X-a_i)^{q-1}) \, mod \, h(X), \quad \text{где } h(X) = \prod_{i=0}^{n-1}(X-a_i).$$

Обратное дискретное преобразование Фурье [31]. Пусть $\alpha \in \mathbb{F}_q$ – элемент порядка n, $n \mid q-1$; $a_i = \alpha^i$, $f(a_i) = b_i$, $i = 0, 1, \ldots, n-1$. Тогда

$$f(X) = \frac{1}{n}\sum_{i=0}^{n-1}\left(\sum_{j=0}^{n-1} b_j \alpha^{-ji}\right)X^i.$$

§ 44. Элементарные симметрические многочлены и степенные суммы. Формулы Ньютона

Пусть $f(x) = (x-x_1)(x-x_2)\ldots(x-x_n) \in \mathbb{F}_q[x\,]$. Тогда

$f(x) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \cdots + (-1)^{n-1}\sigma_{n-1}x^1 + (-1)^n\sigma_n$,

где

$$\sigma_k = \sigma_k(x_1, x_2, \ldots, x_n) = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} x_{i_1}x_{i_2}\ldots x_{i_k}, k = 1,2,\ldots,n\,.$$

Многочлены

$\sigma_1 = x_1 + x_2 + \cdots + x_n$,

$\sigma_2 = x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + x_2x_n + \cdots + x_{n-1}x_n$,

$\ldots$

$\sigma_n = x_1x_2\ldots x_n$

остаются неизменными при любой перестановке переменных x_1, $x_2, \ldots, x_n$. Каждый из них однороден (σ_k – сумма слагаемых, каждое из которых произведение k переменных). Многочлены σ_k называют *элементарными симметрическими многочленами* от переменных x_1, $x_2, \ldots, x_n$ над полем $\mathbb{F}_q$. Название многочленов σ_k элементарными

---

[31] ***Жан-Батист Жозеф Фурье*** (21.03.1768 – 16.05.1830) – французский математик и физик.

обусловлено следующим утверждением (доказательство см. в [**22**, § 52]):

44.1. ***Теорема*** (Основная теорема о симметрических многочленах). *Для каждого многочлена* $f(x_1, x_2, \dots, x_n)$ *над полем* $\mathcal{F}$ *существует единственный многочлен* $g \in \mathcal{F}[x_1, x_2, \dots, x_n]$, *такой, что* $f(x_1, x_2, \dots, x_n) = g(\sigma_1, \sigma_2, \dots, \sigma_n)$.

Установим связь между $\sigma_1, \sigma_2, \dots, \sigma_n$ и $s_1, s_2, \dots, s_n$, где

$$s_k = \sum_{i=1}^{n} x_i^k, k \in \mathbb{N},$$

– степенные суммы.

44.2. ***Теорема*** (Формулы Ньютона). *Пусть* $\sigma_1, \sigma_2, \dots, \sigma_n$ *– элементарные симметрические многочлены от переменных* $x_1, x_2, \dots, x_n$; $s_1, s_2, \dots, s_n$ *– степенные суммы тех же переменных. Тогда при* $k \geq 1$ *имеют место формулы*

$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 - \dots + (-1)^{k-1}s_1\sigma_{k-1} + (-1)^k k\sigma_k = 0;$

$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 - \dots + (-1)^{n-1}s_{k-n+1}\sigma_{n-1} + (-1)^n s_{k-n}\sigma_n = 0,$

справедливые соответственно при $k \leq n$ *и* $k > n$.

Доказательство. Отметим, что $\sigma_1 = s_1$. Для произведения

$$ax_1^{k_1}x_2^{k_2} \dots x_n^{k_n} \qquad (1)$$

неизвестных $x_1, x_2, \dots, x_n$, где некоторые показатели k_j могут равняться нулю, обозначим через $S(ax_1^{k_1}x_2^{k_2} \dots, x_n^{k_n})$ сумму всех членов, получающихся из (1) при всевозможных перестановках неизвестных. Например, $S(x_1x_2) = \sigma_2$, $S(x_1^2) = s_2$ и т.д. Если $k \leq n$, то нетрудно убедиться в справедливости следующих равенств:

$s_{k-1}\sigma_1 = s_k + S\left(x_1^{k-1}x_2\right),$

$s_{k-2}\sigma_2 = S\left(x_1^{k-1}x_2\right) + S\left(x_1^{k-2}x_2x_3\right),$

……

$s_{k-i}\sigma_i = S\left(x_1^{k-i+1}x_2 \dots x_i\right) + S\left(x_1^{k-i}x_2 \dots x_ix_{i+1}\right),$

$2 \leq i \leq k-2,$

……

$s_1\sigma_{k-1} = (x_1^2x_2 \dots x_{k-1}) + k\sigma_k.$

Складывая эти равенства и умножая их на чередующиеся знаки $-$ и $+$, затем, перенося все члены в левую часть, получаем требуемую формулу (6).

При $k > n$ система равенств выглядит следующим образом:

$s_{k-1}\sigma_1 = s_k + S\left(x_1^{k-1}x_2\right),$

$$s_{k-2}\sigma_2 = S\left(x_1^{k-1}x_2\right) + S\left(x_1^{k-2}x_2x_3\right),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$s_{k-i}\sigma_i = S\left(x_1^{k-i+1}x_2 \ldots x_i\right) + S\left(x_1^{k-i}x_2 \ldots x_ix_{i+1}\right), \quad 2 \le i \le n-1,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$s_{k-n}\sigma_n = \left(x_1^{k-n+1}x_2 \ldots x_n\right),$$

откуда аналогично получаем формулу (7). □

§ 45. Поле отношений (вкратце)

Имеется много общих свойств между кольцами $\mathbb{Z}$ и $\mathcal{k}[X]$. Наша дальнейшая цель – вложить $\mathcal{k}[X]$ в поле, так же, как $\mathbb{Z}$ вкладывается в $\mathbb{Q}$.

Пусть A – целостное кольцо. Рассмотрим множество пар $(a, b) \in A \times A^*$, где $A^* = A / \{0\}$. Пары (a, b) будем называть *дробями* и обозначать через $\frac{a}{b}$, что более привычно. На множестве дробей определим отношение равенства:

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc.$$

Данное отношение обладает следующими свойствами (рефлексивность, симметричность и транзитивность):

1) $\frac{a}{b} = \frac{a}{b}$;
2) $\frac{a}{b} = \frac{c}{d} \Longrightarrow \frac{c}{d} = \frac{a}{b}$;
3) $\frac{a}{b} = \frac{c}{d}$ и $\frac{c}{d} = \frac{e}{f} \Longrightarrow \frac{a}{b} = \frac{e}{f}$.

Первые два свойства очевидны. Докажем третье свойство:

$$\frac{a}{b} = \frac{c}{d} \text{ и } \frac{c}{d} = \frac{e}{f} \Longrightarrow ad = bc \text{ и } cf = de \Longrightarrow$$
$$adcf = bcde \Longrightarrow af = be \Longrightarrow \frac{a}{b} = \frac{e}{f}.$$

Таким образом, отношение равенства является отношением эквивалентности на множестве $A \times A^*$ и, следовательно, определяет разбиение этого множества на непересекающиеся классы. Класс эквивалентности, содержащий дробь $\frac{a}{b}$, обозначим через $\left[\frac{a}{b}\right]$. Так что

$$\left[\frac{a}{b}\right] = \left\{\frac{c}{d} \,\middle|\, \frac{c}{d} = \frac{a}{b}, c \in A, d \in A^*\right\}.$$

На множество классов, которое обозначим через $Q(A)$, можно перенести обычные операции сложения и умножения:

$$\left[\frac{a}{b}\right]+\left[\frac{c}{d}\right]=\left[\frac{ad+bc}{bd}\right];\quad \left[\frac{a}{b}\right]\cdot\left[\frac{c}{d}\right]=\left[\frac{ac}{bd}\right].$$

Нетрудно показать, что эти операции определены корректно, т.е. не зависят от выбора представителей классов, а именно:

$$\left[\frac{a_1}{b_1}\right]=\left[\frac{a_2}{b_2}\right] \text{ и } \left[\frac{c_1}{d_1}\right]=\left[\frac{c_2}{d_2}\right] \Rightarrow \left[\frac{a_1}{b_1}\right]+\left[\frac{c_1}{d_1}\right]=\left[\frac{a_2}{b_2}\right]+\left[\frac{c_2}{d_2}\right]$$
$$\text{и } \left[\frac{a_1}{b_1}\right]\cdot\left[\frac{c_1}{d_1}\right]=\left[\frac{a_2}{b_2}\right]\cdot\left[\frac{c_2}{d_2}\right].$$

Также нетрудно установить, что множество $Q(A)$ относительно введённых операций сложения и умножения дробей образует поле. Чтобы оно содержало кольцо A, нужно отождествить некоторые дроби с элементами из A. Это достигается следующим образом. Элементу $a \in A$ отнесём дроби $\left[\frac{ab}{b}\right]$, где $b -$ любой элемент из A^* (на самом деле элементу a будет отнесена одна дробь, поскольку все дроби $\frac{ab}{b}$ равны). Далее квадратные скобки в записи $\left[\frac{a}{b}\right]$ будем опускать.

Поле $(Q(A), +, \cdot)$ называется *полем отношений*, или *полем частных* кольца A. Таким образом, доказано существование объемлющего поля для целостного кольца. Заметим, что кольцо могло и не содержать единицу, а в поле частных она появится. (Пример: $A = m\mathbb{Z}$, где $m \in \mathbb{N}, m > 1$.)

Конструкция полей отношений часто используется в математике. Например, поле рациональных чисел $\mathbb{Q}$ есть не что иное, как поле отношений $Q(\mathbb{Z})$ кольца $\mathbb{Z}$. Нетрудно установить также, что $Q(A) \cong A$, если $A -$ поле.

Другой важный пример полей отношений даёт кольцо $A = \Bbbk[X]$, где $\Bbbk -$ поле (в более общем случае $A = \Bbbk[X_1,\ldots,X_n] -$ кольцо многочленов от n переменных). Поле отношений $Q(\Bbbk[X])$ кольца $\Bbbk[X]$ называется *полем рациональных дробей* от переменной X с коэффициентами в $\Bbbk$ и обозначается через $\Bbbk(X)$ (квадратные скобки меняются на круглые).

Поле $\Bbbk(X)$ бесконечно и имеет характеристику, совпадающую с характеристикой поля $\Bbbk$. Каждая рациональная дробь записывается в виде $\frac{f}{g}$, где $f, g -$ многочлены из $\Bbbk[X]$, $g -$ ненулевой многочлен; f называется *числителем*, а $g -$ *знаменателем* дроби $\frac{f}{g}$. Дробь не меня-

ется, если числитель и знаменатель умножить на один и тот же ненулевой многочлен или сократить на общий множитель. Значение $deg\ \frac{f}{g} = deg\ f - deg\ g$ не зависит от представления дроби $\frac{f}{g}$ в виде отношения (частного) двух многочленов f и g. Рациональная дробь называется *несократимой*, если её числитель взаимно прост со знаменателем. Любая рациональная дробь $\frac{f}{g}$ однозначно представляется несократимой дробью $\frac{f_1}{g_1}$, где f_1 и g_1 − частные от деления f и g на их наибольший общий делитель НОД (f, g). Старший коэффициент знаменателя можно вынести и его обратное значение присоединить к числителю. Несократимая дробь со знаменателем, являющимся унитарным многочленом, называется *нормализованной*. Если $deg\ \frac{f}{g} < 0$, т.е. степень числителя меньше степени знаменателя, то несократимая дробь называется *правильной*.

45.1. ***Теорема.*** *Каждая рациональная дробь из $k(X)$ представима в виде суммы многочлена и правильной лроби.*

Доказательство. Использовать теорему о делении с остатком. □

Определение. Правильная рациональная дробь $\frac{f}{g}$ из $k(X)$ называется *простейшей*, если $g = p^n$, $n \geq 1$, где $p \in k[X]$ − неприводимый многочлен, и $deg\ f < deg\ p$.

45.2. ***Теорема.*** *Каждая правильная рациональная дробь $\frac{f}{g}$ из $k(X)$ может быть разложена в сумму простейших дробей, причём единственным способом.*

Конкретно, если $g = p_1^{\alpha_1} \dots p_k^{a_k}$ − каноническое разложение многочлена g в произведение неприводимых сомножителей $p_1, \dots, p_k$, где $g, p_1, \dots, p_k$ − унитарные многочлены, то

$$\frac{f}{g} = \sum_{i=1}^{k} \sum_{j=1}^{a_i} \frac{f_{ij}}{p_i^j}$$

для некоторых $f_{ij} \in k[X]$, $deg\ f_{ij} < deg\ p_i$.

Доказательство. Опускается. См. [**22**], § 25; [**23**], § V.5. □

§ 46. Элементы теории полей

Если $\Bbbk$ – подполе поля K, то K называют *расширением* (или *надполем*) поля $\Bbbk$. Далее запись $K\ /\ \Bbbk$ означает, что K – расширение поля $\Bbbk$. Если $\Bbbk$ – подполе поля $\mathcal{F}$, а $\mathcal{F}$ – подполе поля K, т.е. $\Bbbk \subset \mathcal{F} \subset K$, то $\mathcal{F}$ называют *промежуточным* полем расширения $K\ /\ \Bbbk$. Цепочку расширений $\Bbbk = \mathcal{F}_1 \subset \mathcal{F}_2 \subset \cdots \subset \mathcal{F}_n = K$, где $\mathcal{F}_i$ – промежуточное поле расширения $\mathcal{F}_{i-1}\ /\ \mathcal{F}_{i+1}$, $1 < i < n$, называют n-*этажной башней* полей.

Любое расширение $K\ /\ \Bbbk$ можно рассматривать как векторное пространство над полем $\Bbbk$ (относительно сложения в K и умножения на элементы поля $\Bbbk$). Размерность $dim_{\Bbbk}K$ этого пространства называют *степенью* расширения $K\ /\ \Bbbk$ и обозначают $[K\colon \Bbbk]$. Если эта степень конечна, то расширение называют *конечным*, в противном случае – *бесконечным*. Всякий базис поля K как векторного пространства над $\Bbbk$ называют *базисом расширения* $K\ /\ \Bbbk$.

46.1. ***Теорема.*** *Пусть $\mathcal{F}$ – промежуточное поле расширения $K\ /\ \Bbbk$. Расширение $K\ /\ \Bbbk$ конечно тогда и только тогда, когда конечны расширения $K\ /\ \mathcal{F}$ и $\mathcal{F}\ /\ \Bbbk$. В случае их конечности*

$$[K\colon \Bbbk] = [K\colon \mathcal{F}][\mathcal{F}\colon \Bbbk],$$

причём если $\alpha_1, \ldots, \alpha_m$ – базис расширения $K\ /\ \mathcal{F}$ и $\beta_1, \ldots, \beta_n$ – базис расширения $\mathcal{F}\ /\ \Bbbk$, то элементы $\alpha_i\beta_j$, $1 \le i \le m$, $1 \le j \le n$, составляют базис расширения $K\ /\ \Bbbk$.

Доказательство. Предположим вначале, что расширения $K\ /\ \mathcal{F}$ и $\mathcal{F}\ /\ \Bbbk$ конечны. Тогда любой элемент $\gamma \in K$ записывается в виде

$$\gamma = \sum\nolimits_i a_i\alpha_i\,,\ a_i \in \mathcal{F}.$$

В свою очередь,

$$a_i = \sum\nolimits_j b_{ij}\beta_j\,, b_{ij} \in \Bbbk.$$

Следовательно,

$$\gamma = \sum\nolimits_i \sum\nolimits_j b_{ij}\alpha_i\beta_j,$$

т.е. γ – линейная комбинация над $\Bbbk$ элементов $\alpha_i\beta_j$. Предположим, что элементы $\alpha_i\beta_j$ линейно зависимы над $\Bbbk$, т.е. $\sum_i \sum_j c_{ij}\alpha_i\beta_j = 0$ при некоторых $c_{ij} \in \Bbbk$, не равных нулю одновременно. Тогда

$$0 = \sum\nolimits_i \left(\sum\nolimits_j c_{ij}\beta_j\right)\alpha_i \Longrightarrow \sum\nolimits_j c_{ij}\beta_j = 0 \Longrightarrow c_{ij} = 0$$

для всех $1 \le i \le m$, $1 \le j \le n$, поскольку элементы $\alpha_1,\ldots,\alpha_m$ линейно независимы над $\mathcal{F}$, а элементы $\beta_1,\ldots,\beta_n$ линейно независимы над $\Bbbk$. Другими словами, элементы $\alpha_i\beta_j$ составляют базис расширения $K \,/\, \Bbbk$ и $[K:\Bbbk] = mn = [K:\mathcal{F}][\mathcal{F}:\Bbbk]$.

Обратно, если $[K:\Bbbk] < \infty$, то и $[\mathcal{F}:\Bbbk] < \infty$, поскольку $\mathcal{F}/\Bbbk$ – подпространство в $K \,/\, \Bbbk$. Если $\gamma_1,\ldots, \gamma_s$ – базис пространства K над $\Bbbk$, то произвольный элемент $\gamma \in K$ будет линейной комбинацией элементов $\gamma_1,\ldots, \gamma_s$ с коэффициентами из $\Bbbk$ и, ввиду $\Bbbk \subset \mathcal{F}$, тем более с коэффициентами из $\mathcal{F}$. Поэтому $[K:\mathcal{F}] \le s < \infty$. □

Определение. Пусть K – расширение поля $\Bbbk$. Элемент $\alpha \in K$ называется *алгебраическим* над (относительно) $\Bbbk$, если он является корнем некоторого ненулевого многочлена $f(x) \in \Bbbk[x]$. Элемент α, не являющийся алгебраическим над $\Bbbk$, называется *трансцендентным* над $\Bbbk$. Расширение $K \,/\, \Bbbk$ называется *алгебраическим*, если всякий элемент из K алгебраичен над $\Bbbk$.

46.2. ***Теорема.*** *Всякое конечное расширение $K \,/\, \Bbbk$ алгебраично над $\Bbbk$.*

Доказательство. Пусть $[K:\Bbbk] = n$. Тогда степени 1, α^1, α^2,..., α^n любого элемента $\alpha \in K$ линейно зависимы над $\Bbbk$, т.е.

$$f_0 \cdot 1 + f_1\alpha^1 + f_2\alpha^2 + \cdots + f_n\alpha^n = 0$$

при некоторых $f_i \in \Bbbk$, не равных нулю одновременно. Так что α – корень некоторого ненулевого многочлена $f(x) = f_0 + f_1x^1 + f_2x^2 + \cdots + f_nx^n \in \Bbbk[x]$. Значит, α – алгебраический элемент над $\Bbbk$. □

Определение. Пусть K – расширение поля $\Bbbk$ и $\alpha \in K$ – алгебраический элемент над $\Bbbk$. Выберем среди всех ненулевых многочленов $f(x) \in \Bbbk[x]$, для которых $f(\alpha) = 0$, нормированный многочлен $\mu(x) = \mu_{\alpha,\,\Bbbk}(x)$ наименьшей степени. Он называется *минимальным многочленом элемента* α относительно поля $\Bbbk$. Под *степенью элемента* α над полем $\Bbbk$ понимается степень его минимального многочлена.

Отметим следующие свойства минимального многочлена $\mu(x)$:

1) если $f(x) \in \Bbbk[x]$ и $f(\alpha) = 0$, то $\mu(x) \mid f(x)$;

2) $\mu(x)$ – неприводимый в $\Bbbk[x]$ многочлен.

Действительно, 1) если $\mu(x) \nmid f(x)$, то $r(x)$ – остаток от деления $f(x)$ на $\mu(x)$ – имел бы α своим корнем, что противоречит выбору $\mu(x)$, так как в этом случае $r(x)$ – ненулевой многочлен и $deg\ r(x) < deg\ \mu(x)$. Далее, 2) если допустить, что $\mu(x) = g(x)h(x)$, где $g(x), h(x) \in \Bbbk[x]$ и $1 \le deg\ g(x), deg\ h(x) < deg\ \mu(x)$, то α являет-

ся корнем либо $g(x)$, либо $h(x)$, что также противоречит выбору $\mu(x)$.

Определение. Пусть $\Bbbk -$ подполе поля K и $S -$ любое подмножество в K. Определим поле $\Bbbk(S)$ как пересечение всех подполей поля K, содержащих одновременно $\Bbbk$ и S; оно называется *расширением поля $\Bbbk$, полученным присоединением элементов множества S*. Если $S = \{\alpha_1,..., \alpha_n\} -$ конечное множество, то будем писать $\Bbbk(S) = \Bbbk(\alpha_1,..., \alpha_n)$. Если S состоит из одного элемента α, то поле $\Bbbk(\alpha)$ называется *простым расширением* поля $\Bbbk$, а $\alpha -$ *образующим* (или *порождающим*) *элементом* этого расширения.

46.3. ***Теорема.*** *Пусть A, $B -$ любые подмножества расширения K поля $\Bbbk$. Тогда $\Bbbk(A \cup B) = k(A)(B)$.*

Доказательство. Поле $\Bbbk(A \cup B)$ содержит поле $\Bbbk(A)$ и множество B, а следовательно, и поле $\Bbbk(A)(B)$. Обратно, поле $\Bbbk(A)(B)$ содержит множество $\Bbbk \cup (A \cup B)$, а следовательно, поле $\Bbbk(A \cup B)$. □

46.4. ***Следствие.*** *Пусть $\alpha_1,...,\alpha_n \in K \,/\, \Bbbk$. Тогда* $\Bbbk(\alpha_1,..., \alpha_n) = \Bbbk(\alpha_1) ... (\alpha_n)$.

Замечание. Отметим, что поле $\Bbbk(\alpha_1,...,\alpha_n)$ образовано в точности дробями $\frac{f(\alpha_1,...,\alpha_n)}{g(\alpha_1,...,\alpha_n)}$, где $f, g -$ многочлены от n переменных с коэффициентами из поля $\Bbbk$ и $g(\alpha_1,...,\alpha_n) \neq 0$. Уместно пояснить также, что записи $\Bbbk(\alpha_1,...,\alpha_n)$ и $\Bbbk[\alpha_1,...,\alpha_n]$ отличаются тем, что круглые скобки обозначают всегда расширение до поля, т.е. образование всех рациональных выражений (дробей), а квадратные обозначают расширение до кольца, т.е. образование всех целых выражений $f(\alpha_1,\ldots,\alpha_n)$. □

Изучим строение простых расширений поля $\Bbbk$. Далее два расширения K и K' поля $\Bbbk$ будем называть *эквивалентными* (относительно $\Bbbk$), если существует изоморфизм $K \cong K'$, переводящий элементы поля $\Bbbk$ в себя.

46.5. ***Теорема.*** *Пусть $K -$ расширение поля $\Bbbk$, содержащее трансцендентный элемент α относительно поля $\Bbbk$. Тогда поле $\Bbbk(\alpha)$ эквивалентно полю $\Bbbk(x)$ рациональных дробей от переменной x с коэффициентами в $\Bbbk$.*

Доказательство. Напомним, что элементами поля $\Bbbk(x)$ являются дроби $\frac{f(x)}{g(x)}$, где $f(x), g(x) \in \Bbbk[x]$ и $g(x) -$ ненулевой многочлен. При этом дроби $\frac{f_1(x)}{g_1(x)}$ и $\frac{f_2(x)}{g_2(x)}$ являются равными, т.е. представляют

один и тот же элемент поля $\Bbbk(x)$, если $f_1g_2 - f_2g_1$ – нулевой многочлен. Поскольку $g(\alpha) \neq 0$ для ненулевых многочленов, то для дроби $\frac{f(x)}{g(x)}$ имеет смысл значение $\frac{f(\alpha)}{g(\alpha)}$. Разные дроби (как разные элементы поля $\Bbbk(x)$) имеют разные значения в K. Действительно, если $\frac{f_1(\alpha)}{g_1(\alpha)} = \frac{f_2(\alpha)}{g_2(\alpha)}$, то $f_1(\alpha)g_2(\alpha) - f_2(\alpha)g_1(\alpha) = 0$, откуда следует, что $f_1g_2 - f_2g_1$ – нулевой многочлен, и дроби $\frac{f_1(x)}{g_1(x)}$ и $\frac{f_2(x)}{g_2(x)}$ представляют один и тот же элемент поля $\Bbbk(x)$. Таким образом, между дробями $\frac{f(x)}{g(x)} \in \Bbbk(x)$ и значениями $\frac{f(\alpha)}{g(\alpha)} \in K$ можно установить взаимно однозначное соответствие. Оно сохраняется и при операциях сложения и умножения:

$$\frac{f_1(x)}{g_1(x)} + \frac{f_2(x)}{g_2(x)} = \frac{f(x)}{g(x)} \Leftrightarrow \frac{f_1(\alpha)}{g_1(\alpha)} + \frac{f_2(\alpha)}{g_2(\alpha)} = \frac{f(\alpha)}{g(\alpha)},$$
$$\frac{f_1(x)}{g_1(x)} \cdot \frac{f_2(x)}{g_2(x)} = \frac{f(x)}{g(x)} \Leftrightarrow \frac{f_1(\alpha)}{g_1(\alpha)} \cdot \frac{f_2(\alpha)}{g_2(\alpha)} = \frac{f(\alpha)}{g(\alpha)}.$$

Поскольку поле $\Bbbk(\alpha)$ состоит в точности из элементов $\frac{f(x)}{g(x)}$, где $f, g \in \Bbbk[x]$ и g – ненулевой многочлен, то поля $\Bbbk(x)$ и $\Bbbk(\alpha)$ изоморфны. Установленный изоморфизм переводит элементы поля $\Bbbk$ в себя. Поэтому поля $\Bbbk(x)$ и $\Bbbk(\alpha)$ эквивалентны. □

46.6. ***Теорема.*** *Пусть K – расширение поля $\Bbbk$, содержащее алгебраический элемент α над $\Bbbk$, и пусть $\mu(x) \in \Bbbk[x]$ – минимальный многочлен элемента α степени n. Тогда*:

1) *простое алгебраическое расширение $\Bbbk(\alpha)$ эквивалентно факторкольцу $\Bbbk[x] / \mu(x)$;*

2) *$[\Bbbk(\alpha):\Bbbk] = n$ и $\{1,\alpha,\ldots,\alpha^{n-1}\}$ – базис векторного пространства $\Bbbk(\alpha)$ над $\Bbbk$;*

3) *каждый элемент $\beta \in \Bbbk(\alpha)$ алгебраичен над $\Bbbk$, и его степень d – делитель числа n.*

Доказательство. 1) Рассмотрим отображение $\psi: \Bbbk[x] \longrightarrow \Bbbk(\alpha)$, определяемое следующим образом: $\psi(f) = f(\alpha)$ для любого $f \in \Bbbk[x]$. Очевидно, что ψ является гомоморфизмом колец, и $Ker\ f = \{f \in \Bbbk[x] \mid f(\alpha) = 0\} = (\mu)$. Пусть $S = Im\ f$ – образ отображения ψ, т.е. множество значений многочленов $g(x) \in \Bbbk[x]$ при $x = \alpha$. Отметим, что $\Bbbk \subseteq S = \Bbbk[\alpha] \subseteq \Bbbk(\alpha)$ и $\alpha \in S$. Согласно теореме о гомоморфиз-

мах колец имеем $S \cong \mathbb{k}[x] / (\mu)$. Так как $\mathbb{k}[x] / (\mu)$ – поле, то и S – поле, но тогда, по определению простого расширения, $S = \mathbb{k}(\alpha) \cong \mathbb{k}[x] / (\mu)$. Очевидно, что поля $\mathbb{k}(\alpha)$ и $\mathbb{k}[x] / (\mu)$ не только изоморфны, но и эквивалентны.

2) Так как $\mathbb{k}(\alpha) = \mathbb{k}[\alpha]$, то любой элемент $\beta \in \mathbb{k}(\alpha)$ можно записать в виде $\beta = f(\alpha)$ для некоторого $f(x) \in \mathbb{k}[x]$. Пусть $r(x)$ – остаток от деления $f(x)$ на $\mu(x)$. Тогда $\beta = f(\alpha) = r(\alpha)$. Так как $deg\, r(x) < n$, то β является линейной комбинацией элементов $1, \alpha, ..., \alpha^{n-1}$ с коэффициентами из $\mathbb{k}$. Остаётся показать, что элементы $1, \alpha, ..., \alpha^{n-1}$ линейно независимы над $\mathbb{k}$. Для этого предположим противное: пусть $a_0 \cdot 1 + a_1\alpha^1 + \cdots + a_{n-1}\alpha^{n-1} = 0$, где $a_i \in \mathbb{k}$ и не все $a_i = 0$. Полагая $a(x) = a_0 + a_1x^1 + \cdots + a_{n-1}x^{n-1}$, имеем: $a(x)$ – ненулевой многочлен, $deg\, a(x) < n$ и $a(\alpha) = 0$, но это противоречит выбору минимального многочлена $\mu(x)$. Следовательно, элементы $1, \alpha, ..., \alpha^{n-1}$ линейно независимы над $\mathbb{k}$ и $[\mathbb{k}(\alpha) : \mathbb{k}] = n$.

3) Так как $\mathbb{k}(\alpha)$ – конечное расширение поля $\mathbb{k}$, то любой элемент $\beta \in \mathbb{k}(\alpha)$ алгебраичен над $\mathbb{k}$. Пусть d – степень элемента β над $\mathbb{k}$. Тогда, учитывая теорему 46.1 и тот факт, что $\mathbb{k}(\beta)$ – подполе поля $\mathbb{k}(\alpha)$, имеем

$$n = [\mathbb{k}(\alpha) : \mathbb{k}] = [\mathbb{k}(\alpha) : \mathbb{k}(\beta)][\mathbb{k}(\beta) : \mathbb{k}] = [\mathbb{k}(\alpha) : \mathbb{k}(\beta)]d,$$

откуда следует, что $d \mid n$. □

46.7. ***Теорема.*** *Пусть $K / \mathbb{k}$ и $K' / \mathbb{k}$ – два расширения поля $\mathbb{k}$, и пусть $\alpha \in K$ и $\beta \in K'$ – алгебраические над полем $\mathbb{k}$ элементы, имеющие один и тот же минимальный многочлен $\mu(x)$ степени n. Тогда отображение*

$$a_0 + a_1\alpha^1 + \cdots + a_{n-1}\alpha^{n-1} \longrightarrow a_0 + a_1\beta^1 + \cdots + a_{n-1}\beta^{n-1}$$

где $a_0, \ldots, a_{n-1} \in \mathbb{k}$ – произвольные элементы, является изоморфизмом поля $\mathbb{k}(\alpha)$ на поле $\mathbb{k}(\beta)$, причём единственным, при котором $\alpha \longrightarrow \beta$ и $a \longrightarrow a$, если $a \in \mathbb{k}$.

Доказательство. Утверждение вполне очевидно. □

В теоремах 46.5 и 46.6 мы предполагали, что задано надполе K, содержащее поле $\mathbb{k}$ и элемент α, и исследовали строение поля $\mathbb{k}(\alpha)$ внутри K. Это было необходимо, чтобы выражения, содержащие α, имели смысл. Теперь поставим задачу иначе. Пусть задано поле $\mathbb{k}$. Требуется найти его расширение $K = \mathbb{k}(\alpha)$ такое, что либо (задача 1) элемент α трансцендентен над $\mathbb{k}$, либо (задача 2) элемент α – корень любого наперёд заданного неприводимого многочлена в $\mathbb{k}[x]$.

Первая задача решается просто: в качестве α берём неизвестное x, образуем кольцо многочленов $\Bbbk[x]$ и его поле $\Bbbk(x)$ рациональных дробей. Из теоремы 46.5 следует, что все простые трансцендентные расширения поля $\Bbbk$ эквивалентны, так как каждое из них эквивалентно полю $\Bbbk(x)$. Стало быть имеет место

46.8. ***Теорема.*** *Поле $\Bbbk(x)$ является единственным, с точностью до эквивалентности расширений, простым трансцендентным расширением поля $\Bbbk$.*

Рассмотрим вторую задачу.

46.9. ***Теорема.*** *Пусть $\Bbbk$ – поле, а $\mu(x)$ – любой неприводимый многочлен из кольца $\Bbbk[x]$. Тогда существует конечное расширение $K / \Bbbk$ степени $n = deg\,\mu(x)$, в котором многочлен $\mu(x)$ имеет корень. С точностью до эквивалентности, расширение $K / \Bbbk$ единственно. Если $\mu(\alpha) = 0$, $\alpha \in K$, то $K = \Bbbk(\alpha)$.*

Доказательство. Согласно теореме 46.6 искомое поле K должно быть изоморфно факторкольцу $K' = \Bbbk[x] / (\mu)$. Его элементами являются классы вычетов $[f] = f + (\mu)$, где $f \in \Bbbk[x]$. Определим отображение $\psi : \Bbbk[x] \longrightarrow K'$, сопоставляющее многочлену $f \in \Bbbk[x]$ класс вычетов $[f] \in K'$. Нетрудно установить, что это гомоморфизм колец. Отметим, что классы вычетов f_1 и f_2 совпадают тогда и только тогда, когда $f_1(x) - f_2(x) \equiv 0\ (mod\ \mu(x))$. Поскольку $a = 0$ – единственный элемент поля $\Bbbk$, для которого $a \equiv 0\ (mod\ \mu(x))$, то $[a_1] \neq [a_2]$ для различных элементов a_1 и a_2 поля $\Bbbk$. Отсюда следует, что отображение ψ задаёт изоморфизм поля $\Bbbk$ на некоторое подполе $\Bbbk'$ поля K'. Поэтому поле $\Bbbk'$ можно отождествить с полем $\Bbbk$, заменяя классы вычетов $[a]$ на соответствующие им элементы a из $\Bbbk$. Тем самым получим поле K, содержащее $\Bbbk$ и изоморфное K'.

Для любого многочлена $a(x) = a_0 + a_1x^1 + \cdots + a_mx^m \in \Bbbk[x]$ в соответствии с правилами операций с классами вычетов и с учётом отождествления $[a] = a$ для $a \in \Bbbk$ получаем

$$[a] = [a_0 + a_1x^1 + \cdots + a_mx^m] = a_0 + a_1\alpha^1 + \cdots + a_m\alpha^m,$$

где α обозначает класс вычетов x. Таким образом, каждый элемент поля K может быть записан как многочлен от "переменной" α с коэффициентами из $\Bbbk$. Следовательно, $K = \Bbbk(\alpha)$ – простое расширение поля $\Bbbk$. Если $\mu(x) = b_0 + b_1x^1 + \cdots + b_nx^n$, то $\mu(\alpha) = b_0 + b_1\alpha^1 + \cdots + b_n\alpha^n = [b_0 + b_1x^1 + \cdots + b_nx^n] = [\,\mu(x)] = [0]$.

Значит, α – корень многочлена $\mu(x)$, $\alpha \in K$ – алгебраический элемент над $\Bbbk$, и $K = \Bbbk(\alpha)$ – простое алгебраическое расширение поля $\Bbbk$ степени n. □

§ 47. Поле разложения

Определение. Пусть $f \in \Bbbk[X]$ – унитарный многочлен степени n. Расширение $K \,/\, \Bbbk$ поля $\Bbbk$ называется *полем разложения* многочлена f, если

1) f разлагается в $K[X]$ на линейные множители, т.е. $f(X) = (X - \alpha_1)\ldots(X - \alpha_n)$, $\alpha_1,\ldots,\alpha_n \in K$;

2) $K = \Bbbk(\alpha_1,\ldots, \alpha_n)$, т.е. K получается из $\Bbbk$ присоединением корней $\alpha_1,\ldots, \alpha_n$ многочлена f;

3) K – минимальное поле, в котором f разлагается на линейные множители.

Заметим, что условие унитарности многочлена f (равенство старшего коэффициента единице) на самом деле не существенно и используется только для удобства.

47.1. ***Теорема.*** (Существование поля разложения). *Для всякого многочлена $f \in \Bbbk[X]$ степени $n > 1$ существует поле разложения K, причём степень $[K:\Bbbk]$ расширения $K \,/\, \Bbbk$* поля $\Bbbk$ не превосходит $n!$.

Доказательство. Пусть

$$f(X) = ap_1(X) \ldots p_s(X),\ a \in \Bbbk,$$

– разложение f на неприводимые множители в $\Bbbk[X]$. Присоединяя к полю $\Bbbk$ корень α_1 неприводимого многочлена $p_1(X)$, мы получим поле $\Bbbk_1 = \Bbbk(\alpha_1)$, над которым от p_1, а, следовательно, от f можно отделить множитель $(X - \alpha_1)$, т.е. $f(X) = (X - \alpha_1)f_1(X)$, где $f_1(X) \in \Bbbk_1[X]$.

Повторяя этот приём к многочлену f_1 и его корню α_2, мы построим поле $\Bbbk_2 = \Bbbk_1(\alpha_2)$. Продолжая так шаг за шагом, мы придём к полному разложению f на линейные множители над некоторым расширением $\Bbbk_n$ поля $\Bbbk$. Либо $\Bbbk_n$, либо его некоторое подполе будет полем разложения для f.

Так как $[\Bbbk_i:\Bbbk_{i-1}] \le n + 1 - i$, то

$$[K:\Bbbk] \le \prod_{i=1}^{n} [\Bbbk_i:\Bbbk_{i-1}] \le n! \quad \square$$

В доказательстве теоремы слишком много произвола, чтобы можно было говорить о единственности поля разложения. Этот вопрос рассмотрен в следующем параграфе. Правда, в дальнейшем факт единственности поля разложения не используется. Нам будет достаточно того, что существует расширение поля $\Bbbk$, в котором лежат все корни многочлена f.

§ 48. Теорема Кронекера

48.1. ***Теорема*** Кронекера. *Пусть* $f(X) = f_0 + f_1X + \cdots + f_nX^n \in \Bbbk[X]$ *– неприводимый многочлен над полем* $\Bbbk$ *степени* $deg\ f = n > 0$. *Тогда существует простое алгебраическое расширение* $\mathcal{K}$ *поля* $\Bbbk$, *образующим элементом которого является некоторый корень многочлена* f.

Доказательство. Рассмотрим факторкольцо $\mathcal{K} = \Bbbk[X]/(f)$, которое по теореме 39.8 является полем. Элементами кольца $\mathcal{K}$ являются классы вычетов $[h] = h + (f)$, где $h \in \Bbbk[X]$. Для каждого $a \in \Bbbk$ можно построить класс вычетов $[a]$. Если $a, b \in \Bbbk$ и $a \neq b$, то $[a] \neq [b]$, поскольку $deg\ f > 0$. Отображение $a \longrightarrow [a]$ является изоморфизмом поля $\Bbbk$ на некоторое подполе $\mathcal{K}'$ поля $\mathcal{K}$, так что поле $\mathcal{K}'$ можно отождествить с полем $\Bbbk$. Другими словами, поле $\mathcal{K}$ можно рассматривать как расширение поля $\Bbbk$. Для каждого многочлена $h(X) = a_0 + a_1X + \cdots + a_mX^m \in \Bbbk[X]$ в соответствии с правилами операций над классами вычетов и с учётом отождествления $[a_i] = a_i$, для $a_i \in \Bbbk$, получаем $[h] = [a_0 + a_1X + \cdots + a_mX^m] = [a_0] + [a_1X] + \cdots + [a_mX^m] = a_0 + a_1[X] + \cdots + a_m[X^m]$.

Таким образом, каждый элемент поля $\mathcal{K}$ может быть записан как многочлен от переменной $[X]$ с коэффициентами из $\Bbbk$. Иными словами, поле $\mathcal{K}$ является простым расширением поля $\Bbbk$, получаемым присоединением элемента $[X]$. Так как $f([X]) = f_0 + f_1[X] + \cdots + f_n[X]^n] = [f_0 + f_1X + \cdots + f_nX^n] = [f(X)] = [0]$, то $[X]$ – корень многочлена f. Отсюда следует, что поле $\mathcal{K}$ является простым расширением поля $\Bbbk$, получаемым присоединением некоторого корня многочлена f. □

48.2. ***Теорема.*** *Пусть* α *и* β *– два корня многочлена* $f(X) \in \Bbbk[X]$, *который неприводим над полем* $\Bbbk$. *Тогда простые расширения* $\Bbbk(\alpha)$ *и* $\Bbbk(\beta)$ *изоморфны, причём изоморфизм осуществляется отображением, которое переводит элемент* α *в элемент* β *и оставляет неизменными элементы поля* $\Bbbk$.

Доказательство. Обозначим $A = \{a_0 + a_1X + \cdots + a_{n-1}X^{n-1} \in \Bbbk[X]\}$, где $n = deg\, f$. Поле $\Bbbk(\alpha)$ образовано элементами вида $a(\alpha)$, где $a(X) \in A$, а поле $\Bbbk(\beta)$ – элементами вида $a(\beta)$, где $a(X) \in A$. Если $a(X), b(X) \in A$, то $a(\alpha) \cdot b(\alpha) = c(\alpha)$, $a(\beta) \cdot b(\beta) = c(\beta)$, где $c(X) = a(X) \cdot b(X)\ mod\ f(X)$ (т.е. $c(X)$ – остаток от деления $a(X) \cdot b(X)$ на $f(X)$).

Пусть τ: $\Bbbk(\alpha) \longrightarrow \Bbbk(\beta)$ – отображение, определяемое правилом:

$$\tau(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) = a_0 + a_1\beta + \cdots + a_{n-1}\beta^{n-1}.$$

Поскольку элементы 1, α,..., α^{n-1} и 1, β,..., β^{n-1} линейно независимы над полем $\Bbbk$, то отображение τ взаимно однозначно. Кроме того,

$$\tau(a(\alpha) + b(\alpha)) = \tau(a(\alpha)) + \tau(b(\alpha)) = a(\beta) + b(\beta);$$
$$\tau(a(\alpha) \cdot b(\alpha)) = \tau(c(\alpha)) = c(\beta) = a(\beta) \cdot b(\beta).$$

Другими словами, τ – изоморфизм, указанный в формулировке теоремы. □

48.3. ***Теорема.*** (Существование и единственность поля разложения). *Для любого многочлена f над полем $\Bbbk$ положительной степени существует поле разложения. Любые два поля разложения многочлена f изоморфны, и соответствующий изоморфизм оставляет неизменными элементы поля $\Bbbk$ и осуществляет некоторую перестановку корней многочлена f.*

Доказательство. Повторным применением теоремы Кронекера можно получить первую часть данного утверждения. Вторая часть является обобщением предыдущей теоремы. □

§ 49. Строение конечных полей

Число элементов конечного поля. Напомним определение векторного пространства над полем.

Определение. *Векторное пространство над полем $\mathcal{F}$* – это аддитивно записанная абелева группа $\mathcal{V}$, в которой определено умножение на скаляры, т.е. отображение

$$\mathcal{F} \times \mathcal{V} \to \mathcal{V}\colon (a, \boldsymbol{v}) \longrightarrow a\boldsymbol{v},$$

удовлетворяющее следующим аксиомам, где $\boldsymbol{v}, \boldsymbol{w} \in \mathcal{V}$; $a, b \in \mathcal{F}$, 1 – единица в $\mathcal{F}$:

1) $a(\boldsymbol{v} + \boldsymbol{w}) = a\boldsymbol{v} + a\boldsymbol{w}$);
2) $(a + b)\boldsymbol{v} = a\boldsymbol{v} + b\boldsymbol{v}$;
3) $(ab)\ \boldsymbol{v} = a(b\boldsymbol{v})$;
4) $1 \cdot \boldsymbol{v} = \boldsymbol{v}$.

Элементы векторного пространства называют *векторами*, а элементы поля $\mathcal{F}$ – *скалярами*. Из аксиом 1) – 4) вытекают следующие свойства векторного пространства ($\mathbf{0}$, 0 – нули в $\mathcal{V}$ и $\mathcal{F}$ соответственно): $a \cdot \mathbf{0} = \mathbf{0}$, $0 \cdot \boldsymbol{v} = \mathbf{0}$, $(-1) \cdot \boldsymbol{v} = -\boldsymbol{v}$.

Пусть $\mathcal{B} = \{\boldsymbol{v}_i | \, i \in I\}$ – произвольное множество векторов из $\mathcal{V}$. *Линейной комбинацией* векторов $\boldsymbol{v}_i \in \mathcal{B}$ называется вектор, определённый формулой

$$\boldsymbol{v} = \sum_{i \in I} c_i \boldsymbol{v}_i, \quad c_i \in \mathcal{F},$$

в которой лишь конечное число коэффициентов c_i отлично от нуля. Линейная комбинация называется *тривиальной*, если все коэффициенты c_i равны нулю.

Множество $\mathcal{B}$ называется *линейно независимым множеством*, если все нетривиальные комбинации векторов из $\mathcal{B}$ отличны от нуля. Любое линейно независимое множество содержится в некотором *максимальном* линейно независимом множестве $\mathcal{B}_0$, которое перестаёт быть линейно независимым после присоединения к нему любого элемента из $\mathcal{V}$.

Каждый вектор $\boldsymbol{v} \in \mathcal{V}$ может быть однозначно представлен в виде линейной комбинацией векторов $\boldsymbol{v}_i \in \mathcal{B}_0$:

$$\boldsymbol{v} = \sum_{i \in I} c_i \boldsymbol{v}_i, \quad \boldsymbol{v}_i \in \mathcal{B}_0.$$

В связи с этим максимальное линейно независимое множество называют *базисом*. Все базисы имеют одинаковую мощность, которая называется *размерностью* векторного пространства и обозначается $dim\, \mathcal{V}$. Если данная мощность конечна, пространство называется *конечномерным*; в противном случае – *бесконечномерным.* Конечномерное векторное пространство с базисом из n элементов называется n*- мерным пространством*.

49.1. ***Теорема.*** *Пусть $\mathbb{F}_q$ – конечное поле характеристики p, содержащее q элементов. Тогда $q = p^m$ для некоторого $m \in \mathbb{N}$.*

Доказательство. Поле $\mathbb{F}_q$ можно рассматривать как векторное пространство над простым полем $\mathbb{F}_p$. В этом нетрудно убедиться, проверяя выполнимость аксиом 1) – 4). Пусть $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ – базис $\mathbb{F}_q$ над $\mathbb{F}_p$. Тогда произвольный элемент $\boldsymbol{a} \in \mathbb{F}_q$ представим в виде линейной комбинации $\boldsymbol{a} = c_1\boldsymbol{a}_1 + \cdots + c_m\boldsymbol{a}_m$, где $c_1, \ldots, c_m \in \mathbb{F}_p$. Очевидно, что число элементов поля $\mathbb{F}_q$ равно числу всевозможных

наборов $(c_1,\ldots, c_m) \in \mathbb{F}_p^n$. Поскольку поле $\mathbb{F}_p$ содержит p элементов, то общее число таких наборов равно p^m. □

49.2. ***Теорема.*** *Для любого простого числа p и любого натурального $m \in \mathbb{N}$ существует поле $\mathbb{F}_q$, содержащее $q = p^m$ элементов.*

Доказательство. Рассмотрим многочлен $f(X) = X^q - X \in \mathbb{F}_p[X]$. По теореме 47.1 существует поле разложения многочлена f. Обозначим это поле через $\mathcal{F}$. Очевидно, что $Char\ \mathcal{F} = p$. Так как $f' = -1$ и НОД $(f, f') = 1$, то многочлен f не имеет кратных корней, и поле $\mathcal{F}$ содержит q различных элементов, удовлетворяющих уравнению $X^q - X = 0$ (или, что то же самое, $X^q = X$). Остаётся показать, что соответствующее множество элементов, которое мы обозначим через A_q, и является искомым полем $\mathbb{F}_q$. Отметим предварительно, что в поле характеристики p для любых элементов имеет место тождество $(a + b)^q = a^q + b^q$, если $q = p^m$. Кроме того, нуль и единица поля $\mathcal{F}$ лежат в множестве A_q.

Пусть $a, b \in A_q$. Тогда, учитывая, что $a^q = a$ и $b^q = b$, имеем:

$(a + b)^q = a^q + b^q = a + b \Longrightarrow a + b \in A_q$;

$(ab)^q = a^q b^q = ab \Longrightarrow ab \in A_q$;

$a \neq 0, (a^{-1})^q = (a^q)^{-1} = a^{-1} \Longrightarrow a^{-1} \in A_q$.

Другими словами, множество A_q замкнуто относительно сложения и умножения, а также относительно взятия обратного элемента. Отсюда следует, что A_q – поле. Очевидно, что в данном случае $\mathcal{F} = A_q = \mathbb{F}_q$. □

49.3. ***Следствие.*** (Малая теорема Ферма для поля $\mathbb{F}_q$). *Каждый элемент β поля $\mathbb{F}_q$ удовлетворяет тождеству $\beta^q = \beta$, или, что эквивалентно, является корнем уравнения $X^q - X = 0$. Таким образом, в поле $\mathbb{F}_q$ имеет место разложение*

$$X^q - X = \prod_{\alpha \in \mathbb{F}_q} (X - \alpha) = X \sum_{\alpha \in \mathbb{F}_q^*} (X - \alpha).$$

49.4. ***Теорема.*** *Мультипликативная группа $\mathbb{F}_q^*$ ненулевых элементов поля $\mathbb{F}_q$ циклическая.*

Доказательство. Напомним, что мультипликативный порядок $ord\ \alpha$ элемента $\alpha \in \mathbb{F}_q^*$ определяется как наименьшее $\delta \in \mathbb{N}$, при котором $\alpha^\delta = 1$. Пусть θ – элемент с наибольшим порядком среди элементов $\alpha \in \mathbb{F}_q^*$, $m = ord\ \theta$. Тогда $m \mid q - 1$, а по следствию 21.10 порядок любого элемента $\alpha \in \mathbb{F}_q^*$ является делителем числа m. Следова-

тельно, любой элемент $\alpha \in \mathbb{F}_q^*$ является корнем уравнения $X^m - 1 = 0$. Это возможно лишь в том случае, если $m = q - 1$. Таким образом, $ord\ \theta = q - 1$, и $\mathbb{F}_q^* = \{\theta^0 = 1, \theta^1, \ldots, \theta^{q-2}\} = <\theta> -$ циклическая группа. □

Следующее утверждение является обращением теоремы Ферма:

49.5. ***Теорема*** (Люка,1876). *Натуральное число n является простым тогда и только тогда, когда существует число b такое, что*

$$b^{n-1} \equiv 1\ (mod\ n), \qquad (1)$$

но

$$b^{(n-1)/q} \not\equiv 1\ (mod\ n) \text{ для любого простого делителя } q \qquad (2)$$

числа $n - 1$.

Доказательство. Если $n -$ простое число, то $\mathbb{Z}_n -$ простое поле, а $\mathbb{Z}_n^* -$ циклическая группа, порождающий элемент которой является искомым числом b. Обратно, если имеет место (1), и $ord\ b = m$, то $m \mid n - 1$. Но тогда из условия (2) следует, что $m = n - 1$. Следовательно, $\varphi(n) = n - 1$ и $n -$ простое число. □

Теорему Люка можно использовать для проверки числа n на простоту, если известно разложение числа $n - 1$ на простые множители. Соответствующий алгоритм основан на переборе возможных значений $b \in \mathbb{Z}_n$, взаимно простых с n, с проверкой выполнения условий (1) и (2).

Определение. Элемент θ порядка $q - 1$ называется *примитивным* элементом поля $\mathbb{F}_q$, или *образующим* элементом группы $\mathbb{F}_q^*$. Очевидно, что θ является первообразным корнем $(q - 1)$-ой степени из единицы поля $\mathbb{F}_q$.

Примитивным элементом поля $\mathbb{F}_q$ является также любой элемент θ^d, если d взаимно просто с $(q - 1)$. Всего имеется $\varphi(q - 1)$ таких элементов, где $\varphi -$ функция Эйлера.

Из теоремы 48.1 непосредственно вытекает

49.6. ***Следствие***. *Поле $\mathbb{F}_q$ с $q = p^m$ элементами является простым алгебраическим расширением поля $\mathbb{F}_p$, т.е. $\mathbb{F}_q = \mathbb{F}_p(\theta)$, где $\theta -$ любой первообразный корень уравнения $X^{q-1} - 1 = 0$.*

49.7. ***Лемма.*** *Если $d, m \geq 1$; $n \geq 2$, то $(n^d - 1) \mid (n^m - 1)$ тогда и только тогда, когда $d \mid m$. Аналогично, в произвольном поле $X^m - 1$ делится на $X^d - 1$ без остатка тогда и только тогда, когда $d \mid m$.*

Доказательство. Представим число m в виде $m = td + r$, где $0 \leq r < d$. Тогда $n^m - 1 = n^r(n^{td} - 1) + (n^r - 1)$. Число $n^{td} -$

1 всегда делится на $n^d - 1$, а последнее слагаемое меньше $n^d - 1$ и, следовательно, является остатком от деления $n^m - 1$ на $n^d - 1$, который равен нулю тогда и только тогда, когда $r = 0$. Так же доказывается второе утверждение леммы (с заменой n на X). □

49.8. ***Теорема.*** *Пусть* $q = p^m$. *Тогда каждое подполе поля* $\mathbb{F}_q$ *имеет порядок* p^d, где $d \mid m$. *Обратно, если* $d \mid m$, *то существует ровно одно подполе* $\mathbb{F}_{p^d}$ *поля* $\mathbb{F}_q$.

Доказательство. Пусть $\mathbb{F}$ − подполе поля $\mathbb{F}_q$. Тогда $\mathbb{F} = \mathbb{F}_{p^d}$ для некоторого d. Очевидно, $Char\ \mathbb{F}_{p^d} = Char\ \mathbb{F}_q = p$. Порядок примитивного элемента ξ поля $\mathbb{F}_{p^d}$, равный $p^d - 1$, является делителем числа $q - 1 = p^m - 1$. Тогда по лемме 49.7. $d \mid m$. Поле $\mathbb{F}_{p^d}$ образуют элементы 0, ξ, ξ^2,…, ξ^{p^d-1}, являющиеся корнями многочлена $X^{p^d} - X$. Отметим попутно, что $\xi = \theta^s$, где θ − примитивный элемент поля $\mathbb{F}_{p^m}$, $s = \frac{p^m-1}{p^d-1}$.

Обратно, если $d \mid m$, то число $p^d - 1$ делит число $p^m - 1$. Это означает, что многочлен $X^{p^d} - X$ делит многочлен $X^{p^m} - X$. Следовательно, корни многочлена $X^{p^d} - X$ являются корнями многочлена $X^{p^m} - X$ и принадлежат полю $\mathbb{F}_{p^m}$. С другой стороны, множество корней многочлена $X^{p^d} - X$ само образует поле из p^d элементов, являющееся, естественно, подполем в $\mathbb{F}_{p^m}$. Единственность подполя $\mathbb{F}_{p^d}$ вытекает из того факта, что в любом поле $\mathbb{F}$ порядка p^d выполняется тождество $a^{p^d} = a$ и поэтому $\mathbb{F}$ состоит исключительно из корней многочлена $X^{p^d} - X$. □

§ 50. Корни из единицы. Круговые многочлены

Определение. Элемент x поля $\mathcal{F}$ называется *корнем из единицы*, если существует натуральное число n, для которого $x^n = 1$. Всякий элемент x, для которого $x^n = 1$ называется *корнем n-ой степени* из единицы.

Определение. Для натурального числа n поле разложения многочлена $x^n - 1$ над произвольным полем $\mathcal{F}$ называется *n-круговым* (или *n-циклотомическим*) *полем* над $\mathcal{F}$ и обозначается $\mathcal{F}^{(n)}$**.** Множество корней n-ой степени из единицы обозначим E_n.

Если $\mathcal{F}$ – поле рациональных чисел $\mathbb{Q}$, то $\mathcal{F}^{(n)}$ – подполе поля $\mathbb{C}$ комплексных чисел. Хотя нас больше интересуют конечные поля, свойства корней из единицы полезно установить без предположения о конечности поля $\mathcal{F}$. Следующее утверждение показывает, что структура множества E_n определяется соотношением между числом n и характеристикой p поля $\mathcal{F}$.

50.1. ***Теорема***. *Пусть* $\nu \in \mathbb{N}$ *и* $char\ \mathcal{F} = p$. *Тогда*

1) *Если* $p \nmid \nu$, *то* E_ν – *циклическая подгруппа мультипликативной группы поля* $\mathcal{F}^{(n)}$. *В частности, мультипликативная группа конечного поля* $\mathbb{F}_q$ *является циклической*.

2) *Если* $p \mid \nu$ *и* $\nu = np^m$, *причем* $p \nmid n$, *то* $\mathcal{F}^{(\nu)} = \mathcal{F}^{(n)}$, $E_\nu = E_n$, *а корнями многочлена* $x^\nu - 1$ *являются* n *элементов множества* E_n, *каждый из которых имеет кратность* p^m.

Доказательство. 1) Отметим, что E_ν – конечная мультипликативная абелева группа. Пусть m – максимальный порядок среди её элементов, т.е. $m = max\{ord\ (\xi) \mid \xi \in E_\nu\}$. Тогда порядок любого элемента $\xi \in E_\nu$ является делителем числа m, причем $m \mid \nu$. Следовательно, любой элемент $\xi \in E_\nu$ является корнем многочлена $x^m - 1$. Отсюда следует, что $m = \nu$.

2) Утверждение вытекает из равенств $x^\nu - 1 = x^{np^m} - 1 = (x^n - 1)^{p^m}$. □

Определение. Пусть $\mathcal{F}$ – поле характеристики p, $p \nmid n$. Образующий элемент циклической подгруппы E_n поля $\mathcal{F}$ называется *первообразным* (или *примитивным*) *корнем* n*-ой степени из единицы* поля $\mathcal{F}$.

Если $p \nmid n$, то E_n содержит $\varphi(n)$ различных первообразных корней n*-ой* степени из единицы поля $\mathcal{F}$. Если ζ – один из них, то все другие первообразные корни n-ой степени из единицы поля $\mathcal{F}$ имеют вид ζ^k, где $1 \le k \le n$, НОД $(k, n) = 1$.

Определение. Пусть $\mathcal{F}$ – поле характеристики p, $p \nmid n$ и ζ – первообразный корень n*-ой* степени из единицы поля $\mathcal{F}$. Тогда многочлен

$$Q_n(x) = \prod_{\substack{k=1,\dots,n,\\ \text{НОД}\ (k,n)=1}} (x - \zeta^k)$$

называется n*-круговым* (или n*-циклотомическим*) *многочленом* над полем $\mathcal{F}$.

Очевидно, что многочлен $Q_n(x)$ не зависит от выбора элемента ζ.

50.2. ***Теорема***. Пусть $\mathcal{F}$ – поле характеристики p, $p \nmid n$. Тогда

$$x^n - 1 = \prod_{d|n} Q_d(x). \qquad (1)$$

Доказательство. Каждый корень n-ой степени из единицы поля $\mathcal{F}$ является первообразным корнем d-ой степени из единицы поля $\mathcal{F}$ ровно для одного делителя d числа n. Формула (1) получается из формулы

$$x^n - 1 = \prod_{k=1}^{n} (x - \zeta^k)$$

собиранием тех множителей $(x - \zeta^k)$, для которых ζ^k является первообразным корнем n-ой степени из единицы поля $\mathcal{F}$ для каждого натурального делителя d числа n. □

50.3. ***Теорема***. Коэффициенты n-кругового многочлена $Q_n(x)$ принадлежат простому подполю поля $\mathcal{F}$, если $p > 0$, или кольцу $\mathbb{Z}$, если $p = 0$.

Доказательство **(**индукция по n). Имеем $Q_1(x) = x - 1$. При $n \geq 2$ имеем

$$Q_n(x) = \frac{(x^n - 1)}{f(x)},$$

где

$$f(x) = \prod_{d|n, d<n} Q_d(x).$$

Поскольку многочлены $Q_d(x)$ нормированные и их коэффициенты принадлежат простому подполю поля $\mathcal{F}$ (при $p > 0$) или кольцу $\mathbb{Z}$ (при $p = 0$), то при делении углом коэффициенты многочлена $Q_n(x)$ будут также принадлежать простому подполю поля $\mathcal{F}$ или кольцу $\mathbb{Z}$ соответственно при $p > 0$ и $p = 0$. □

Пример. Пусть p – простое число. Тогда

$$Q_{p^k}(x) = \frac{\left(x^{p^k} - 1\right)}{Q_1(x)Q_p(x) \ldots Q_{p^{k-1}}(x)} = \frac{\left(x^{p^k} - 1\right)}{\left(x^{p^{k-1}} - 1\right)}$$
$$= 1 + x^{p^{k-1}} + x^{2p^{k-1}} \ldots + x^{(p-1)p^{k-1}}.$$

В частности,

$$Q_p(x) = 1 + x + x^2 \ldots + x^{p-1}. \square$$

Более общее утверждение дает следующая

50.4. ***Теорема***.

$$Q_n(x) = \prod_{d|n} (x^n - 1)^{\mu(n/d)} = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)}.$$

Доказательство. Достаточно применить мультипликативный вариант (теорема 13.3) формулы обращения Мёбиуса к равенству (1). □

50.5. ***Теорема***. Пусть d − собственный делитель натурального числа n. Тогда $Q_n(x)$ делит многочлен $(x^n - 1)/\,(x^d - 1)$.

Доказательство. Ввиду теоремы 50.2 многочлен $Q_n(x)$ делит многочлен $x^n - 1 = (\,x^d - 1)((x^n - 1)/\,(x^d - 1))$. Так как d − собственный делитель числа n, то, согласно той же теореме, многочлены $Q_n(x)$ и $x^d - 1$ не имеют общих корней. Значит, НОД $(\,Q_n(x), x^d - 1) = 1$, и, следовательно, $Q_n(x)$ делит $(x^n - 1)/\,(x^d - 1)$. □

§ 51. Теорема Веддербёрна о коммутативности конечных тел

Определение. *Нормализатором* непустого подмножества S группы G называется множество

$$N(S) = \{a \in G \mid aSa^{-1} = S\}.$$

Если $S = \{b\}$, то $N(\{b\})$ называется *нормализатором элемента* $b \in G$ и обозначается как $N(b)$. Для любого фиксированного элемента $a \in G$ множества S и aSa^{-1} называются *сопряженными*.

51.1. ***Теорема***. *Для любого непустого подмножества S группы G нормализатор $N(S)$ является подгруппой группы G, причем можно установить взаимно однозначное соответствие между левыми смежными классами группы G по подгруппе $N(S)$ и различными множествами aSa^{-1}, сопряженными с S.*

Доказательство. Пусть $a, b \in N(S)$. Тогда $aS = Sa$, $Sb^{-1} = b^{-1}S$. Отсюда следуют равенства $ab^{-1}S = aSb^{-1} = Sab^{-1}$ и включение $ab^{-1} \in N(S)$. Так как $e \in N(S)$, и $a, b \in N(S) \Longrightarrow a^{-1}, ab \in N(S)$, то $N(S)$ − подгруппа группы G. Далее, из цепочки соотношений

$$aSa^{-1} = bSb^{-1} \Leftrightarrow a^{-1}bSb^{-1}a = a^{-1}bS(a^{-1}b)^{-1} \Leftrightarrow$$
$$a^{-1}b \in N(S) \Leftrightarrow b \in aN(S)$$

следует, что сопряженные с S множества aSa^{-1} и bSb^{-1} совпадают тогда и только тогда, когда элементы a и b принадлежат одному и тому же левому смежному классу группы G по подгруппе N(S). Это доказывает вторую часть утверждения теоремы. □

Все элементы группы G, сопряженные с фиксированным элементом a, образуют множество, которое называют *классом сопряженности* группы G, содержащим элемент a. Некоторые классы сопряженности состоят из одного элемента. Таким свойством обладают элементы центра, причем только они.

Определение. *Центром* группы G называется её подмножество

$$C(G) = \{c \in G \mid ca = ac \text{ для всех } a \in G\}$$

Нетрудно проверить, что центр – нормальная подгруппа группы G. Группа G является абелевой (т.е. с коммутативным умножением) тогда и только тогда, когда она совпадает со своим центром, т.е. $C(G) = G$.

51.2. ***Теорема*** (Уравнение классов сопряженности). *Пусть G – конечная группа с центром C. Тогда*

$$| G | = | C | + \sum_{i=1}^{k} n_i, \qquad (1)$$

где $n_1, \dots, n_k$ – мощности классов сопряженности группы G, содержащих более одного элемента, т.е. $n_i \geq 2$, причем каждое число n_i делит порядок группы G.

Доказательство. Отношение сопряженности является отношением эквивалентности на G. Поэтому различные классы сопряженности группы G образуют разбиение множества G, и порядок группы G равен сумме мощностей различных классов сопряженности. При этом имеется | C | одноэлементных классов сопряженности, соответствующих элементам центра. Число n_i элементов, сопряженных с некоторым элементом $a_i \in G$, согласно предыдущей теореме равно числу левых смежных классов группы G по подгруппе $N(a_i)$. По теореме Лагранжа индекс нормализатора $N(a_i)$ является делителем порядка $| G |$ группы G. Отсюда следует, что числа n_i являются делителями числа $| G |$. □

Пусть K – конечное тело, а F – его коммутативное подтело (F будем называть подполем тела K). Тело K можно рассматривать как

(левое) векторное пространство W над полем F [32]. Если $F = \mathbb{F}_q$, а тело K имеет конечную размерность n, то K состоит из q^n элементов. Мультипликативную группу ненулевых элементов тела K обозначим через K^*. Из теоремы 51.1 следует, что если G – конечная группа, то число элементов в классе сопряженных с b элементов группы G равно индексу $| G |/N(b)$ нормализатора $N(b)$ в группы G.

51.3. ***Теорема*** Веддербёрна. *Каждое конечное тело является полем.*

Доказательство. Пусть $K -$ конечное тело, и $C = \{c \in K \mid ca = ac$ для всех $a \in K\} -$ его центр. Нетрудно показать, что $C = \mathbb{F}_q -$ поле, где q – степень некоторого простого числа p. Тогда, как отмечено выше, $| K |= q^n$. Покажем, что $K = C$, т.е. $n = 1$.

Допустим противное, т.е. что $n > 1$. Пусть $a \in K$, $N_a = \{b \in K \mid ab = ba\}$. Тогда $N_a -$ тело, содержащее C, и поэтому состоит q^r из элементов. Так как $N_a^* -$ подгруппа группы K^*, то $q^r - 1 \mid q^n - 1$. Последнее возможно лишь тогда, когда r делит n.

Рассмотрим уравнение классов сопряженности (1) для группы K^*. Центром группы K^* является группа C^* порядка $q - 1$. Если $a \in K^*$, то N_a^* – нормализатор элемента a в группе K^*. Поэтому любой класс сопряженности группы K^*, содержащий более одного элемента, состоит из $(q^n - 1)/(q^r - 1)$ элементов, где r – собственный делитель числа n. Уравнение классов сопряженности в этом случае имеет вид

$$q^n - 1 = q - 1 + \sum_{i=1}^{k} \frac{q^n - 1}{q^{r_i} - 1}, \qquad (2)$$

где $1 \le r_1, \ldots, r_k < n -$ собственные делители числа n.

Рассмотрим n-круговой многочлен Q_n над полем рациональных чисел. Согласно теоремам 50.3 и 50.5 $Q_n(q) -$ целое число, которое делит $\frac{q^n-1}{q^{r_i}-1}$ при любом i.

---

[32] Это означает, что $(W, +) -$ абелева группа и что определено умножение её элементов на элементы (скаляры) F: $a\xi \in W, a(b)\xi = (ab)\xi, (a + b)\xi = a\xi + b\xi, a(\xi + \eta) = a\xi + a\eta, 1\xi = \xi$ для всех $a, b \in F$ и $\xi, \eta \in W$.

Поэтому из (2) следует, что $Q_n(q)$ делит $q-1$. Но это приводит к противоречию. Действительно, по определению

$$Q_n(x) = \prod_{\substack{s=1,\\ \text{НОД}\,(s,n)=1}}^{n} (x-\zeta^s),$$

где ζ – первообразный корень n-ой степени из единицы поля $\mathbb{Q}$ рациональных чисел. (Например, $\zeta = cos\frac{2\pi}{n} + i\, sin\frac{2\pi}{n}$.) Переходя к модулю комплексного числа $Q_n(q)$, получаем

$$|\, Q_n(q)\,| = \prod_{\substack{s=1,\\ \text{НОД}\,(s,n)=1}}^{n} |\, q-\zeta^s\,| > \prod_{\substack{s=1,\\ \text{НОД}\,(s,n)=1}}^{n} (q-1) \geq q-1,$$

так как $n>1, q\geq 2$. Неравенство $|\, Q_n(q)\,| > q-1$ противоречит тому, что $Q_n(q)$ делит $q-1$. Полученное противоречие означает, что $n=1$ и $K=C=\mathbb{F}_q$. □

§ 52. Следы, нормы и базисы

Определение. *След элемента* $\alpha \in \mathbb{F}_{q^m}$ *относительно поля* $\mathbb{F}_q$ определяется равенством

$$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}}. \qquad (1)$$

Пусть $f(x) \in \mathbb{F}_q[x]$ – минимальный многочлен элемента α. Если $deg\, f(x) = d$, то $f(x) \mid x^{q^d} - x$ и $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$ – все корни $f(x)$. Они будут повторяться $\frac{m}{d}$ раз в последовательности $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$. Поэтому

$$\begin{aligned} f(x)^{\frac{m}{d}} &= x^m + a_{m-1}x^{m-1} + \cdots + a_0 \\ &= (x-\alpha)(x-\alpha^q)\ldots\left(x-\alpha^{q^{m-1}}\right). \end{aligned} \qquad (2)$$

Из сравнения коэффициентов следует, что

$$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = -\,a_{m-1} \in \mathbb{F}_q.$$

52.1. ***Теорема*** **(**Свойства следа**).** *Для любых* $\alpha, \beta \in \mathbb{F}_{q^m}$, $a, c \in \mathbb{F}_q$ *имеют место равенства*:

$$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha+\beta) = Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) + Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta), \qquad (3)$$

$$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c\alpha) = cTr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha), \qquad (4)$$

$$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a) = ma, \qquad (5)$$

$$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a^q) = Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a). \qquad (6)$$

Доказательство. Свойства (3)−(6) непосредственно вытекают из определения следа (1). □

Определение. Отображение $f\colon \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$ называется *линейным отображением из* $\mathbb{F}_{q^m}$ *в* $\mathbb{F}_q$, если оно удовлетворяет следующим условиям:

1) $f(\alpha+\beta) = f(\alpha) + f(\beta), \forall \alpha, \beta \in \mathbb{F}_{q^m}$;

2) $f(c\alpha) = cf(\alpha), \forall \alpha \in \mathbb{F}_{q^m}, c \in \mathbb{F}_q$.

52.2. ***Теорема.*** *Линейные отображения из* $\mathbb{F}_{q^m}$ *в* $\mathbb{F}_q$ *исчерпываются отображениями*

$$L_b\colon x \longrightarrow Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(bx), \ \ \forall b \in \mathbb{F}_q, x \in \mathbb{F}_{q^m}, \qquad (7)$$

причем $L_b \neq L_c$, *если* $b \neq c$.

Доказательство. Тот факт, что отображение (7) является линейным, очевиден ввиду свойств функции следа, отмеченных выше. При этом, если $b \neq c$, то $L_b(x) - L_c(x) = Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}((b-c)x) \not\equiv 0$ и, следовательно, $L_b \neq L_c$. Заметим, что имеется q^m отображений вида (7). С другой стороны, выбирая определенный базис $\{\alpha_1, \alpha_2, \dots, \alpha_m\}$ векторного пространства $\mathbb{F}_{q^m}$ над полем $\mathbb{F}_q$ и отображая базисные элементы α_j, $j = 1, \dots, m$, в произвольные элементы поля $\mathbb{F}_q$, можно получить любое линейное отображение из $\mathbb{F}_{q^m}$ в $\mathbb{F}_q$. Это можно сделать в точности q^m различными способами. Следовательно, любое линейное отображение из $\mathbb{F}_{q^m}$ в $\mathbb{F}_q$ есть отображение вида (7). □

52.3. ***Теорема*** [33]**.** *Для* $\alpha \in \mathbb{F}_{q^m}$ *равенство* $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = 0$ *выполняется тогда и только тогда, когда* $\alpha = \beta^q - \beta$ *для некоторого* $\beta \in \mathbb{F}_{q^m}$.

Доказательство. Достаточность условия очевидна. Докажем его необходимость.

Допустим, что $\alpha \in \mathbb{F}_{q^m}$ − такой элемент, для которого $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = 0$, β − корень уравнения $x^q - x - \alpha = 0$ в некотором расширении поля $\mathbb{F}_{q^m}$. Тогда

---

[33] Это утверждение – частный случай теоремы 90 Гильберта о следе, см. [**23**, гл. VIII, §6].

$$0 = Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta^q - \beta)$$
$$= (\beta^q - \beta) + (\beta^q - \beta)^q + \cdots + (\beta^q - \beta)^{q^{m-1}}$$
$$= (\beta^q - \beta) + \left(\beta^{q^2} - \beta^q\right) + \cdots + \left(\beta^{q^m} - \beta^{q^{m-1}}\right)$$
$$= \beta^{q^m} - \beta.$$

Другими словами, $\beta \in \mathbb{F}_{q^m}$. □

52.4. ***Теорема*** (Транзитивность следа).

$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(Tr_{\mathbb{F}_{q^{nm}}/\mathbb{F}_{q^m}}(\alpha)\right) = Tr_{\mathbb{F}_{q^{nm}}/\mathbb{F}_q}(\alpha), \forall \alpha \in \mathbb{F}_{q^{nm}}$.

Доказательство. Имеем

$$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(Tr_{\mathbb{F}_{q^{nm}}/\mathbb{F}_{q^m}}(\alpha)\right) = \sum_{i=0}^{m-1}\left(Tr_{\mathbb{F}_{q^{nm}}/\mathbb{F}_{q^m}}(\alpha)\right)^{q^i}$$

$$= \sum_{i=0}^{m-1}\left(\sum_{j=0}^{n-1}\alpha^{q^{jm}}\right)^{q^i} = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\alpha^{q^{jm+i}} = \sum_{k=0}^{mn-1}\alpha^{q^k} = Tr_{\mathbb{F}_{q^{nm}}/\mathbb{F}_q}(\alpha).$$ □

Определение. *Норма* $N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ элемента $\alpha \in \mathbb{F}_{q^m}$ над $\mathbb{F}_q$ определяется равенством

$$N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \alpha \cdot \alpha^q \cdot \alpha^{q^2} \cdot \ldots \cdot \alpha^{q^{m-1}} = \alpha^{(q^m-1)/(q-1)}.$$

Из соотношения (2) следует, что $N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = a_0 \in \mathbb{F}_q$.

52.5. ***Теорема*** (Свойства нормы). *Для любых* $\alpha, \beta \in \mathbb{F}_{q^m}$, $a \in \mathbb{F}_q$, $\delta \in \mathbb{F}_q^*$ *имеют место равенства*:

$$N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha \cdot \beta) = N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) \cdot N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta); \quad (8)$$

$$N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\delta) \in \mathbb{F}_q^*; \quad (9)$$

$$N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a) = a^m; \quad (10)$$

$$N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha^q) = N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha). \quad (11)$$

Доказательство. Свойства (8) − (11) непосредственно вытекают из определения нормы. □

52.6. ***Теорема*** (Транзитивность нормы). *Для любого* $\alpha \in \mathbb{F}_{q^{nm}}$ *имеет место равенсто*

$N_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(N_{\mathbb{F}_{q^{nm}}/\mathbb{F}_{q^m}}(\alpha)\right) = N_{\mathbb{F}_{q^{nm}}/\mathbb{F}_q}(\alpha), \forall \alpha \in \mathbb{F}_{q^{nm}}$.

Доказательство.

$$N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(N_{\mathbb{F}_{q^{nm}}/\mathbb{F}_{q^m}}(\alpha) = N_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(\alpha^{(mn-1)/(q^m-1)}\right)$$

$$= \left(\alpha^{(mn-1)/(q^m-1)}\right)^{(q^m-1)/(q-1)} = N_{\mathbb{F}_{q^{nm}}/\mathbb{F}_q}(\alpha). \quad \square$$

52.7. ***Теорема*** [34]**.** *Пусть* $\alpha \in \mathbb{F}_{q^m}$. *Равенство* $N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = 1$ *выполняется тогда и только тогда, когда* $\alpha = \beta^{q-1}$ *для некоторого* $\beta \in \mathbb{F}_{q^m}^*$.

Доказательство. Пусть $\alpha = \zeta^i$, где $\zeta -$ примитивный элемент поля $\mathbb{F}_{q^m}$. Имеем $\zeta^{i\frac{q^m-1}{q-1}} = 1 \Leftrightarrow i\frac{q^m-1}{q-1} \equiv 0\ (mod\ q^m - 1) \Leftrightarrow i \equiv 0\ (mod\ q - 1)$. Отсюда следует утверждение теоремы. $\square$

Определение. Поле $\mathbb{F}_{q^m}$ может иметь над $\mathbb{F}_q$ много базисов, но имеются два особо важных типа базисов: 1) *степенной* базис $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$, образованный степенями образующего элемента поля $\mathbb{F}_{q^m}$ (как простого расширения поля $\mathbb{F}_q$; в качестве α обычно берется примитивный элемент поля $\mathbb{F}_{q^m}$); 2) другим типом базиса является *нормальный* базис $\{1, \alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$, состоящий из подходящим образом выбранного элемента α и сопряженных с ним элементов α^{q^i}, $i = 1, 2, \ldots, m-1$.

Приведем без доказательств некоторые утверждения о базисах (см., например, [**24**, гл. 2, § 3; **26**, гл. 4, §§ 4.6–4.9]). Они могут быть полезны при реализации вычислений над конечными полями.

52.8. ***Теорема*** (О нормальном базисе). *Для каждого поля* $\mathbb{F}_q$ *и каждого его расширения* $\mathbb{F}_{q^m}$ *существует нормальный базис поля* $\mathbb{F}_{q^m}$ *над полем* $\mathbb{F}_q$.

52.9. ***Теорема.*** *Элементы* $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ *поля* $\mathbb{F}_{q^m}$ *образуют базис этого поля над* $\mathbb{F}_q$ *тогда и только тогда, когда*

$$det(A) = \begin{vmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_m \\ \alpha_1^q & \alpha_2^q & & \alpha_m^q \\ \vdots & & \ddots & \vdots \\ \alpha_1^{q^{m-1}} & \alpha_2^{q^{m-1}} & \cdots & \alpha_m^{q^{m-1}} \end{vmatrix} \neq 0.$$

---

[34] Это утверждение – частный случай теоремы 90 Гильберта о норме, см. [**23**, гл. VIII, § 6].

52.10. ***Теорема.*** *Нормальный базис* $\{1, \alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$ *поля* $\mathbb{F}_{q^m}$ *над полем* $\mathbb{F}_q$ *существует тогда и только тогда, когда многочлены* $x^m - 1$ *и* $\alpha x^{m-1} + \alpha^q x^{m-2} + \cdots + \alpha^{q^{m-2}} x + \alpha^{q^{m-1}}$ *взаимно просты.*

52.11. ***Теорема*** Дэвенпорта [35]**.** *Для каждого поля* $\mathbb{F}_{q^m}$ *характеристики* p *существует нормальный базис этого поля над его простым подполем* $\mathbb{F}_p$*, который состоит из примитивных элементов поля* $\mathbb{F}_{q^m}$.

§ 53. Некоторые результаты о многочленах над конечными полями

53.1. ***Теорема***. *Если* β *– корень многочлена* $f(X) \in \mathbb{F}_q[X]$*, то* β^q *также является корнем многочлена* $f(X)$.

Доказательство. Пусть $f(X) = f_0 + f_1 X + \cdots + f_n X^n$. Тогда $0 = [f(\beta)]^q = f_0{}^q + f_1{}^q \beta^q + f_n{}^q \beta^{nq} = f_0 + f_1 \beta^q + \cdots + f_n \beta^{nq} = f(\beta^q)$. □

53.2. ***Теорема***. *Каждый многочлен* $f(X) \in \mathbb{F}_q[X]$ *степени* m*, неприводимый над* $\mathbb{F}_q$*, является делителем многочлена* $X^{q^m} - X$.

Доказательство. Если $f(X) = X$, то теорема верна. Пусть $f(X) \neq X$ и α – корень многочлена $f(X)$ в расширении $\mathbb{F}_q[X] / (f)$. Это расширение является полем $\mathbb{F}_{q^m}$ и совокупность его ненулевых элементов образует группу порядка $q^m - 1$. Поэтому порядок элемента α должен быть делителем $q^m - 1$, а сам элемент α – корнем многочлена $X^{q^m-1} - 1$. Многочлен $f(X)$ является минимальным многочленом элемента α, но тогда $f(X)$ является делителем многочлена $X^{q^m} - X$. □

53.3. ***Теорема***. *Каждый делитель* $f(X) \in \mathbb{F}_q[X]$ *многочлена* $X^{q^m} - X$*, неприводимый над* $\mathbb{F}_q$*, имеет степень, равную* m *или меньше* m.

---

[35] ***Гарольд Дэвенпорт*** (1907—1969) — английский математик, ученик Литтлвуда. Внёс значительный вклад в алгебраическую теорию чисел. Доказательство теоремы о нормальном базисе над простым полем получено им в работе: ***H. Davenpor*t**. Bases for finite fields. J. London Math. Soc. 43 (1968), pp. 21-39.

Доказательство. Пусть $deg\ f(X) = k$. Рассмотрим расширение $\mathbb{F}_q[X]\ /\ (f)$ поля $\mathbb{F}_q$. Это поле из q^k элементов, каждый из которых может быть представлен в виде линейной комбинации $\beta = a_0 + a_1\alpha + \cdots + a_{k-1}\alpha^{k-1}$, где α − корень $f(X)$, а a_0, a_1,…, $a_{k-1} \in \mathbb{F}_q$. Тогда

$$\beta^{q^m} = a_0 + a_1\alpha^{q^m} + \cdots + a_{k-1}\alpha^{(k-1)q^m}.$$

Но α − корень многочлена $X^{q^m} - X$, и поэтому $\alpha^{q^m} = \alpha$. Отсюда следует, что $\beta^{q^m} = a_0 + a_1\alpha + \cdots + a_{k-1}\alpha^{k-1} = \beta$, т.е. β − корень многочлена $X^{q^m} - X$. Так как число элементов β равно q^k, а число корней многочлена $X^{q^m} - X$ равно q^m, то $q^m \geq q^k$ и, следовательно, $m \geq k$. □

53.4. ***Теорема***. *Пусть β − элемент некоторого расширения поля $\mathbb{F}_q$, и пусть $\mu(X)$ − минимальный многочлен над $\mathbb{F}_q$ элемента β. Тогда, если $deg\ \mu(X) = m$, то порядок элемента β является делителем числа $q^m - 1$, но не является делителем никакого меньшего числа вида $q^k - 1$.*

Доказательство. По теореме 53.2 $\mu(X)$ является делителем многочлена $X^{q^m-1} - 1$, а β − корнем этого многочлена. Поэтому порядок β является делителем числа $q^m - 1$. Предположим, что $q^k - 1$ делится на порядок β при $k < m$. Тогда β является корнем многочлена $X^{q^k} - X$, а $\mu(X)$ − делителем этого многочлена. Но тогда по теореме 53.3 степень многочлена $\mu(X)$ не превосходит k, что противоречит $deg\ \mu(X) = m > k$. □

53.5. ***Теорема***. *Пусть $f(X) \in \mathbb{F}_q[X]$ − многочлен степени m, неприводимый над $\mathbb{F}_q$, и пусть β − корень этого многочлена в некотором расширении поля $\mathbb{F}_q$. Тогда β, β^q,…, $\beta^{q^{m-1}}$ образуют совокупность всех корней многочлена $f(X)$.*

Доказательство. По теореме 53.1 элементы β, β^q,…, $\beta^{q^{m-1}}$ являются корнями многочлена $f(X)$. Покажем, что все эти элементы различны. Допустим на минутку, что это не так и $\beta^{q^i} = \beta^{q^j}$ при $0 \leq i < j \leq m - 1$. Тогда $\beta = \beta^{q^m} = (\beta^{q^j})^{q^{m-j}} = (\beta^{q^i})^{q^{m-j}} = \beta^{q^{m+i-j}}$, $1 = \beta^{q^{m+i-j}-1}$.

Получается, что порядок β является делителем числа $q^{m+i-j} - 1$. С другой стороны, $f(X)$ отличается от минимального многочлена для β разве что на постоянный множитель $a \in \mathbb{F}_q$. Поэтому по теореме

53.4 порядок β является делителем числа $q^m - 1$, но не является делителем никакого числа меньше $q^{m+i-j} - 1$. Полученное противоречие означает, что все элементы $\beta, \beta^q, \ldots, \beta^{q^{m-1}}$ на самом деле различны. Других корней у многочлена $f(X)$ нет, поскольку число корней не может быть больше, чем степень многочлена. □

53.6. ***Теорема***. *Все корни неприводимого многочлена имеют один и тот же порядок*.

Доказательство. Пусть $\beta -$ один из корней многочлена. По теореме 53.5 любой из остальных корней может быть представлен в виде β^{q^j} при некотором j. Пусть e и $e' -$ порядки этих корней. Тогда из соотношений

$$\left(\beta^{q^j}\right)^e = \beta^{eq^j} = (\beta^e)^{q^j} = 1^{q^j} = 1,$$

$$\beta^{e'} = \left(\beta^{q^m}\right)^{e'} = \beta^{q^j q^{m-j} e'} = \left(\left(\beta^{q^j}\right)^{e'}\right)^{q^{m-j}} = 1^{q^{m-j}} = 1$$

следует, что $e' \mid e$ и $e \mid e'$. Но тогда $e = e'$. □

Определение. Порядок корней неприводимого многочлена называется *показателем*, которому данный многочлен принадлежит.

Если неприводимый многочлен принадлежит показателю e, то он является делителем многочлена $X^e - 1$, но не является делителем многочлена $X^n - 1$ при $n < e$. Неприводимый многочлен степени m над полем $\mathbb{F}_q$ называется *примитивным*, если его корнем является примитивный элемент поля $\mathbb{F}_{q^m}$. Тогда этот корень и, следовательно, все корни имеют порядок $q^m - 1$, и все они $-$ примитивные элементы. Неприводимый многочлен степени m является примитивным тогда и только тогда, когда он принадлежит показателю $q^m - 1$. Наконец, неприводимый многочлен степени m является примитивным тогда и только тогда, когда он не является делителем многочлена $X^n - 1$ ни при каких при $n < q^m - 1$.

Число неприводимых многочленов заданной степени над конечным полем.

Обозначим через $\Phi_m(q)$ число унитарных неприводимых многочленов степени m над полем $\mathbb{F}_q$.

53.7. ***Теорема***.

$$\Phi_m(q) = \frac{1}{m} \sum_{d \mid m} \mu\left(\frac{m}{d}\right) q^d,$$

где $\mu -$ *функция Мёбиуса*.

Доказательство. Пусть $f(X) \in \mathbb{F}_q[X]$ – один из унитарных неприводимых многочленов степени d над $\mathbb{F}_q$, $q = p^n$. Его поле разложения изоморфно факторкольцу $\mathbb{F}_q[X] / (f)$. Если $f(X)$ и $X^{q^d} - X$ имеют общий корень, то $X^{q^d} - X$ делится на $f(X)$. Многочлен $X^{q^d} - X$ является делителем многочлена $X^{q^m} - X$, если $m = dr$. Так как многочлен $X^{q^m} - X$ не имеет кратных корней, то в его разложение входят все унитарные неприводимые многочлены

$$f_{d,1}(X), f_{d,2}(X), \ldots, f_{d,\Phi_d(q)}(X)$$

любой степени $d \mid m$, причём ровно по одному разу. Поэтому

$$X^{q^m} - X = \prod_{d \mid m} \left\{ \prod_{k=1}^{\Phi_d(q)} f_{d,k}(X) \right\}.$$

Вычисляя степени многочленов в обеих частях этого равенства, получаем соотношение:

$$q^m = \sum_{d \mid m} d\, \Phi_d(q),$$

из которого, применяя формулу обращения Мёбиуса, получаем выражение для $\Phi_m(q)$. □

Из предыдущих результатов следует, что для любого m существует по меньшей мере один неприводимый многочлен степени m над полем $\mathbb{F}_q$. Это же подтверждает и следующая оценка величины $\Phi_m(q)$:

$$\Phi_m(q) = \frac{1}{m} \sum_{d \mid m} \mu\left(\frac{m}{d}\right) q^d \geq \frac{1}{m}\left(q^m - \sum_{d=1}^{m-1} q^d\right)$$

$$= \frac{1}{m}\left(q^m + 1 - \frac{q^m - 1}{q - 1}\right) > 0.$$

§ 54. Критерий неприводимости многочленов над конечным полем и их разложение на неприводимые сомножители

Любой многочлен над конечным полем можно разложить в произведение неприводимых многочленов. (Напомним, что многочлен $f(x) \in \mathbb{F}_q[x]$ степени n называется *неприводимым*, если он не делится ни на какой многочлен $h(x) \in \mathbb{F}_q[x]$ степени m при $0 < m < n$.) Наличие соответствующих алгоритмов разложения особенно важно

для теории кодирования, для изучения линейных рекуррентных соотношений и вычисления корней многочленов, а также при решении других задач алгебры и теории чисел.

Неприводимый многочлен $f(x) \in \mathbb{F}_q[x]$ степени n обязательно является делителем многочлена $x^{q^n} - x$. Следующее утверждение дает критерий неприводимости многочлена над простым полем:

54.1. ***Теорема*** [**52, 14**]. *Пусть p – простое число. Многочлен $f(x) \in \mathbb{F}_p[x]$ степени $n > 1$ такой, что $f(0) \neq 0$, является неприводимым над полем $\mathbb{F}_p$ тогда и только тогда, когда*

$$\text{НОД}\,(f(x), x^{p^i-1} - 1) = 1 \text{ для } i = 1, 2, \ldots, \left[\frac{n}{2}\right],$$

где $\left[\frac{n}{2}\right]$ – целая часть числа n.

Так как $x \nmid f(x)$, то

$$\text{НОД}\,(f(x), x^{p^i-1} - 1) = \text{НОД}\left(f(x),\ x^{p^i} mod\ f(x) - x\right).$$

Наибольший общий делитель многочленов $f(x)$ и $g(x)$ вычисляется согласно алгоритму Евклида:

Вход: многочлены $f, g \in \mathbb{F}_q[x]$.
while $(f \not\equiv 0)\ and\ (g \not\equiv 0)$ ***do***
if $deg\ f > deg\ g$ ***then*** $f := f\ mod\ g$ ***else*** $g := g\ mod\ f$;
$h := f + g$;
нормировать многочлен $h = h_0 + h_1 x + \cdots + h_k x^k$, умножая его на h_k^{-1}.
Выход: $h = \text{НОД}\,(f, g)$.

Вычисление $d(x) = (g(x))^s\ mod\ f(x)$ основано на использовании соотношения:

$$d(x) = \begin{cases} ((d^2\ mod\ f))^{s/2} mod\ f, & \text{если } s \text{ четно;} \\ (((d^2\ mod\ f))^{[s/2]}\ mod\ f) \cdot g\ mod\ f, & \text{если } s \text{ нечетно.} \end{cases}$$

Это дает следующую схему вычислений $(g(x))^s\ mod\ f(x)$:

Вход: многочлены $f, g \in \mathbb{F}_q[x]$.
$d := 1$; $t := s$;
while $t > 0$ ***do***{
if t нечетно ***then*** $d := d \cdot g\ mod\ f$;
$g := g^2\ mod\ f$;
$t := t\ div\ 2$
}.

Выход: $d = g^s mod\ f$.

Очевидно, если НОД $(f(x), x^{p^i-1} - 1) = d(x) \neq 1$ при некотором $i \leq \left[\frac{n}{2}\right]$, то $d(x)$ делит $f(x)$, т.е. $f(x)$ разложим. Однако существуют более эффективные алгоритмы проверки многочленов на неприводимость и их разложения на неприводимые сомножители в $\mathbb{F}_q[x]$.

54.2. ***Теорема*** Батлера [36] [**44**]. *Многочлен* $f(x) \in \mathbb{F}_q[x]$ *степени* $n > 1$ *неприводим над полем* $\mathbb{F}_q$ *тогда и только тогда, когда выполняются следующие условия*:

a) НОД $\left(f(x),\ f'(x)\right) = 1$, *т.е.* $f(x)$ *не имеет кратных корней*;

b) *уравнение*

$$x^q - x = 0 \qquad (1)$$

имеет в кольце $R = \mathbb{F}_q[x]/(f(x))$ *в точности* q *решений.*

Доказательство. *Необходимость*. Пусть многочлен $f(x)$ неприводим. Тогда R есть поле $\mathbb{F}_q$. Требование о выполнении *условия* НОД $\left(f(x),\ f'(x)\right) = 1$, необходимо, так как неприводимый многочлен над конечным полем не может иметь кратных корней. Константы (постоянные многочлены) a поля $\mathbb{F}_q$ (их ровно q) являются различными корнями многочлена $x^q - x$. Других корней у этого многочлена нет. Следовательно, условия теоремы выполняются.

Достаточность [37]. Пусть выполняются условия a) и b). Элементами кольца R являются классы вычетов, каждый из которых образован многочленами $g(x)$, сравнимыми между собой по модулю $f(x)$. Уравнение (1) не имеет решений, кроме элементов множества $\mathcal{F} = \{[a] \mid a \in \mathbb{F}_q\} \cong \mathbb{F}_q$. (Здесь $[a] = \left\{g(x) \in \mathbb{F}_q[x] \,\middle|\, g(x) \equiv a\ mod\ f(x)\right\}$ – элемент кольца R, $\mathcal{F}$ – подполе кольца R.) Предположим на минутку, что многочлен $f(x)$ приводим над полем $\mathbb{F}_q$, т.е. существуют многочлены $f_1(x), f_2(x) \in \mathbb{F}_q[x]$ такие, что

$$f(x) = f_1(x) \cdot f_2(x),\ \ 1 \leq deg\ f_1(x), deg\ f_2(x) < n.$$

---

[36] ***М. Батлер*** – современный американский математик.

[37] Приведенное доказательство достаточности условий теоремы Батлера почерпнуто нами из книги [11]. Как сообщают авторы, оно предложено А.В. Куприяновым.

Покажем, что уравнение (1) имеет в этом случае решение в $R\backslash\mathcal{F}$, и, тем самым, получим противоречие, что доказывает неприводимость многочлена $f(x)$.

Из условия a) следует, что многочлены $f_1(x)$ и $f_2(x)$ взаимно просты. Поэтому существуют многочлены $u(x), v(x) \in \mathbb{F}_q[x]$, что

$$u(x)\, f_1(x) + v(x) f_2(x) = 1.$$

Можно считать, что $deg\, u(x) \le deg\, f_2(x)$. (В противном случае представим $u(x)$ в виде $u(x) = q(x)\, f_2(x) + r(x)$, где $r(x)$ – остаток от деления $u(x)$ на $f_2(x)$, и получим $r(x) f_1(x) + (q(x) f_1(x) + v(x))\, f_2(x) = 1$.) Очевидно, что $u(x) \neq 0$.

В кольце R имеет место равенство

$$u(x) f_1(x)\ mod\ f(x) = \big(1 - v(x) f_2(x)\big)\ mod\ f(x).$$

Тогда

$$\big(u(x) f_1(x)\big)^2 mod\ f(x) = \big(u(x) f_1(x)\big)\big(1 - v(x) f_2(x)\big)\ mod\ f(x) =$$
$$= \Big(u(x) f_1(x) - u(x) v(x) f_1(x) f_2(x)\Big)\ mod\ f(x) = u(x) f_1(x)\ mod\ f(x).$$

Нетрудно заключить, что $\big(u(x) f_1(x)\big)^q mod\ f(x) = u(x) f_1(x)\ mod\ f(x)$. Другими словами, $u(x) f_1(x)\ mod\ f(x)$ – решение уравнения (1), причем оно не принадлежит $\mathcal{F}$, так как

$$0 < deg\big((x) f_1(x)\ mod\ f(x)\big) < n\ .\ \square$$

Теорема Батлера позволяет сформулировать следующий алгоритм проверки многочлена $f(x) \in \mathbb{F}_q[x]$ на неприводимость над полем $\mathbb{F}_q$:

1) Если НОД $\big(f(x),\ f'(x)\big) \neq 1$, то $f(x)$ приводим. Конец.

2) Если НОД $\big(f(x), f'(x)\big) = 1$, то подсчитаем число решений уравнения (1).

Элементы кольца R представлены многочленами

$$c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in \mathbb{F}_q[x]$$

(с операцией умножения многочленов и возведения многочленов в степень по модулю $f(x)$). Элемент $c(x) \in R$ является корнем уравнения (1) тогда и только тогда, когда $\big(c(x)^q - c(x)\big)\ mod\ f(x) = 0$, что можно записать как

$$\big(c_0^q + c_1^q x^q + \cdots + c_{n-1}^q x^{(n-1)q}\big)\ mod\ f(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1},$$

или, учитывая, что $a^q = a$ для любого $a \in \mathbb{F}_q$,

$$c_1(x^q - x) + c_2(x^{2q} - x^2) + \cdots + c_{n-1}\big(x^{(n-1)q} - x^{n-1}\big) = 0. \quad \big| \quad (2)$$

Вычислим следующие многочлены в кольце $\mathbb{F}_q[x]$:

$$a^{(i)}(x) = a_{0,i} + a_{1,i}x + \cdots + a_{n-1,i}x^{n-1} \equiv x^{iq} - x^i \bmod f(x),$$
$$i = 1, \ldots, n-1,$$

– остатки от деления $x^{iq} - x^i$ на $f(x)$. Тогда равенство (2) можно переписать в виде

$$c_0 \cdot 0 + c_1 a^{(1)}(x) + c_2 a^{(2)}(x) + \cdots + c_{n-1} a^{(n-1)}(x) = 0. \qquad (3)$$

Приравнивая коэффициенты при одинаковых степенях x в левой и правой частях равенства (3), получаем следующую систему линейных уравнений:

$$\begin{cases} 0 \cdot c_0 + a_{0,1}c_1 + a_{0,2}c_2 + \ldots + a_{0,n-1}c_{n-1} = 0, \\ \ldots \\ 0 \cdot c_0 + a_{n-1,1}c_1 + a_{n-1,2}c_2 + \cdots + a_{n-1,n-1}c_{n-1} = 0, \end{cases}$$

или в матричной форме:

$$A_f C = 0, \qquad (4)$$

где

$$A_f = \begin{pmatrix} 0 & a_{0,1} & \cdots & a_{0,n-1} \\ \ldots & \ldots & \ldots & \ldots \\ 0 & a_{n-1,1} & \cdots & a_{n-1,n-1} \end{pmatrix}, \quad C = \begin{pmatrix} c_0 \\ \ldots \\ c_{n-1} \end{pmatrix}, 0 = \begin{pmatrix} 0 \\ \ldots \\ 0 \end{pmatrix}.$$

Число решений уравнения (1) в кольце R равно числу решений системы линейных уравнений (4), т.е. равно $q^{n-rang\, A_f}$. ($rang\, A_f$ – ранг матрицы A_f, т.е. максимальное число линейно независимых строк, – вычисляют обычно путем приведения матрицы к ступенчатому виду с удалением нулевых строк). Согласно теореме Батлера многочлен неприводим, если $n - rang\, A_f = 1$, *т.е.* $rang\, A_f = n - 1$. Таким образом, имеет место

Критерий Батлера. Алгоритм проверки многочлена $\boldsymbol{f(x) \in \mathbb{F}_q[x]}$ ***степени n на неприводимость.***

1. Вычислить $d(x) = \text{НОД}\left(f(x), f'(x)\right)$

2. ***if*** $d(x) \neq 1$ ***then*** $return$ ("$f(x)$ не является неприводимым многочленом")

3. ***if*** $d(x) = 1$ ***then*** вычислить матрицу $\boldsymbol{A_f}$ и её $rang\, \boldsymbol{A_f}$.

4. ***if*** $rang\, \boldsymbol{A_f} = n - 1$ ***then*** $return$ ("$f(x)$ – неприводимый многочлен")

else $return$ ("$f(x)$ не является неприводимый многочленом").

Теорема Батлера позволяет не только проверить многочлен на неприводимость, но и получить в некоторых случаях разложение

многочлена на неприводимые сомножители. Полное (и вполне приемлемое в случае относительно небольших конечных полей) решение вопроса о разложении многочлена на неприводимые сомножители дает приведенная ниже теорема Берлекэмпа [38]. Подход Берлекэмпа является развитием метода Батлера.

Докажем предварительно одно вспомогательное утверждение:

54.3. ***Лемма***. *Пусть* $a_1(x), \dots, a_k(x) \in \mathbb{F}_q[x]$ *– попарно взаимно простые многочлены, т.е. НОД* $(a_i(x), a_j(x)) = 1$ *при* $i \neq j$; $f(x) \in \mathbb{F}_q[x]$ *– унитарный многочлен. Тогда*

$$f(x) \mid \prod_{i=1}^{k} a_i(x) \Rightarrow f(x) = \prod_{i=1}^{k} \text{НОД}\left(f(x), a_i(x)\right) = \text{НОД}\left(f(x), \prod_{i=1}^{k} a_i(x)\right).$$

Доказательство (индукция по k). Пусть $k = 2$. Из условия НОД $(a_1(x), a_2(x)) = 1$ следует равенство

$$\text{НОД}(\text{НОД}(f(x), a_1(x)), \text{НОД}\,(f(x), a_2(x))) = 1.$$

Из последнего равенства и соотношений $\text{НОД}\,(f(x), a_1(x)) \mid f(x)$ и $\text{НОД}\,(f(x),\ a_2(x)) \mid f(x)$ следует, что

$$(\text{НОД}\,(f(x),\ a_1(x))) \cdot (\text{НОД}\,(f(x), a_2(x))) \mid f(x). \tag{5}$$

Пусть

$$\begin{aligned} \text{НОД}\,(f(x), a_1(x)) &= f(x)u_1(x) + a_1(x)v_1(x), \\ \text{НОД}\,(f(x), a_2(x)) &= f(x)u_2(x) + a_2(x)v_2(x). \end{aligned} \tag{6}$$

Перемножая левые и правые части равенств (6) и учитывая условие $f(x) \mid a_1(x)a_2(x)$, получаем, что

$$f(x) \,\Big|\, (\text{НОД}\,(f(x), a_1(x))) \cdot \big(\text{НОД}\,(f(x), a_2(x))\big). \tag{7}$$

Сравнивая (5) и (7) и учитывая, что $f(x)$ – унитарный многочлен, получаем требуемое равенство

$$f(x) = (\text{НОД}\,(f(x), a_1(x))) \cdot \big(\text{НОД}(f(x), a_2(x)\big) =$$

---

[38] ***Элвин Р. Берлекэмп*** (6.09.1940 – 9.04.2019) — американский математик, заслуженный профессор математики, электротехники и компьютерных наук в Университете Калифорнии в Беркли. Широко известен своими работами в области теории кодирования и комбинаторной теории игр.

$$= \text{НОД}\,(f(x), a_1(x)a_2(x)).$$

Далее для завершения доказательства леммы применяем индукцию, переходя от k к $k+1$. □

54.4. ***Теорема*** Берлекэмпа [**40**]. *Пусть* $f(x) \in \mathbb{F}_q[x]$ *– унитарный многочлен степени* n, $R = \mathbb{F}_q[x]/(f(x))$ *и* $c(x) \in R$ *– решение уравнения* (1) *степени* $0 < deg\, c(x) < n$. *Тогда*

$$f(x) = \prod_{\alpha \in \mathbb{F}_q} \text{НОД}\,(f(x), c(x) - \alpha), \tag{8}$$

причем существует такой элемент $\beta \in \mathbb{F}_q$, *что*

$$0 < deg\ \big(\text{НОД}\,(f(x), c(x) - \beta)\big) < n.$$

Доказательство. Имеет место равенство

$$x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha),$$

откуда следует, что

$$c(x)^q - c(x) = \prod_{\alpha \in \mathbb{F}_q} (c(x) - \alpha). \tag{9}$$

Если $\alpha, \beta \in \mathbb{F}_q$ и $\alpha \neq \beta$, то

$$\text{НОД}\,(c(x) - \alpha,\ c(x) - \beta) = 1. \tag{10}$$

По условию теоремы Батлера, $c(x)^q - c(x)\ mod\ f(x) = 0$. Следовательно, $f(x) \mid \big(c(x)^q - c(x)\big)$. Учитывая (9), получаем

$$f(x) \mid \prod_{\alpha \in \mathbb{F}_q} (c(x) - \alpha), \tag{11}$$

Ввиду предыдущей леммы из соотношений (10) и (11) следует требуемое равенство (8). Поскольку $deg\ c(x) > 0$ элемент $\beta \in \mathbb{F}_q$ существует. □

Замечания. 1) Условие унитарности, накладываемое на многочлен $f(x)$ в теореме Берлекэмпа, не является существенным, поскольку любой многочлен можно превратить в унитарный, умножая его на некоторый ненулевой элемент поля $\mathbb{F}_q$. 2) Поиск нужного элемента β осуществляется путем обычного перебора элементов поля $\mathbb{F}_q$.

Алгоритм Батлера-Берлекэмпа разложения многочлена $f(x)$ на неприводимые сомножители в $\mathbb{F}_q[x]$.

***Вход*:** многочлен $f(x) = f_0 + f_1x + \cdots + f_nx^n \in \mathbb{F}_q[x]$, $char\ \mathbb{F}_q = p$.

В алгоритме используются: стек S и список T. Первоначально они пустые, т.е. $S = \emptyset, T = \emptyset$. В стеке S будут храниться промежуточные результаты – многочлены с их кратностями, подлежащие дальнейшему разложению, а в списке T накапливается окончательный результат − неприводимые делители многочлена $f(x) \in \mathbb{F}_q[x]$ с указанием их кратностей.

***Помещаем в стек S многочлен $f(x)$ с кратностью* 1**;

while S* $\neq \emptyset$ *do* { *извлекаем из стека S очередной многочлен $g(x)$ с его кратностью k;

На данном шаге алгоритм реализует один из возможных случаев:

1. ***Случай* $g'(x) = 0$**. Из равенства $g'(x) = \sum_{i=1}^{n} ig_ix^{i-1} = 0$ следует, что $ig_i = 0$ при $i = 1,2, \dots, n$. Поэтому, если $1 \le i \le n$ и $g_i \neq 0$, то $p \mid i$. Следовательно, в этом случае

$g(x) = g_0 + \cdots + g_i\left(x^{i/p}\right)^p + \cdots + g_n\left(x^{n/p}\right)^p$ ($g_i \neq 0, i$ кратно p).

Так как $g_i = \left(g_i^{q/p}\right)^p$, то

$$g(x) = \left(h(x)\right)^p,\ h(x) = g_0^{q/p} + \cdots + g_i^{q/p}x^{i/p} + \cdots + g_n^{q/p}x^{n/p}.$$

Помещаем в стек S многочлен $h(x)$ с кратностью kp.

2. ***Случай* $g'(x) \neq 0, d(x) =$ НОД $\left(g(x), g'(x)\right) \neq 1$**. Здесь $g(x) = d(x)g_1(x)$, где $g_1(x) = \frac{g(x)}{d(x)}$.

Помещаем многочлены $d(x)$ и $g_1(x)$ в стек S с кратностью k

3. ***Случай* $g'(x) \neq 0, d(x) =$ НОД $\left(g(x), g'(x)\right) = 1$**. Если $rang\ A_g = n - 1$, то многочлен $g(x)$ неприводим.

Помещаем в список T многочлен $g(x)$ с его кратностью k.

Если $rang\ A_g < n - 1$, то многочлен $g(x)$ приводим и существует ненулевое решение $c = (c_0, c_1, \dots, c_{n-1})^{\mathrm{T}}$ системы уравнений (4), где $c_i \neq 0$ при некотором $i = 1, \dots, n - 1$. Тогда $c(x) \bmod g(x)$ – решение уравнения (1), где $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$, $0 < deg\ c(x) < n$. Находим многочлен $c(x)$ и элемент $\beta \in \mathbb{F}_q$ такой, что $0 < deg\ \left(\text{НОД}\ (g(x), c(x) - \beta)\right) < n$. Многочлены требуют дальнейшего разложения.

Помещаем в стек S многочлены $h(x) =$ НОД $(g(x), c(x) - \beta)$ и $\frac{g(x)}{h(x)}$ с кратностью k

};

Выход: список T неприводимых делителей многочлена $f(x)$ с указанием их кратностей.

Этот алгоритм эффективен и хорошо работает в случае относительно небольших полей $\mathbb{F}_q$. Но для больших полей, когда q велико, он становится непрактичным, так как работает медленно. Алгоритмы разложения многочлена на неприводимые сомножители в случае больших конечных полей предложены Берлекэмпом [**41**] и Цассенхаузом [**62**]. Вероятностные алгоритмы рассматриваются в [**45, 52**]. См. также [**8**] и [**24**, гл. 4 и комментарии].

§ 55. Перестановочные многочлены в конечных полях

Пусть $S = \{\beta_1, \beta_2, \dots, \beta_m\}$ – произвольное подмножество поля $\mathbb{F}_q$, $m \le q$,

$$\sigma(x) = \prod_{\beta \in S} (x - \beta)\,.$$

Любое отображение $f: S \longrightarrow S$ может быть задано некоторым многочленом $f(x) \in \mathbb{F}_q[x]$. Многочлен $f(x)$ вычисляется, например, либо по интерполяционной формуле Лагранжа, либо по формуле

$$f(x) = \sum_{\beta \in S} f(\beta)(1 - (x - \beta)^{q-1}) \; mod\; \sigma(x),$$

где приведение по модулю $\sigma(x)$ требуется только для того, чтобы степень $f(x)$ не превосходила $m - 1$. Соответствующий многочлен $f(x)$ называется *перестановочным многочленом* для множества S.

55.1. ***Лемма.*** *Многочлен $f(x) \in \mathbb{F}_q[x]$ задаёт отображение множества S в себя тогда и только тогда, когда*

$$\sigma\big(f(x)\big) \equiv 0 \; (mod\; \sigma(x)). \qquad (1)$$

Доказательство. Если имеет место (1), то $\sigma(f(\beta)) = 0$, и, следовательно, $f(\beta) \in S$ для любого $\beta \in S$, т.е. многочлен f задаёт отображение множества S в себя. Обратно, если $f(\beta) \in S$, т.е. $\sigma\big(f(\beta)\big) = 0$ для любого $\beta \in S$, то $\sigma\big(f(x)\big) \equiv 0 \; (mod\; \sigma(x))$ – нулевой многочлен, т.е. имеет место (1). □

55.2. ***Лемма.*** *Пусть $a_0, a_1, \dots, a_{q-1}$ – любые элементы поля $\mathbb{F}_q$. Тогда следующие два условия эквивалентны*:

(a) *все элементы $a_0, a_1, \dots, a_{q-1}$ различны*;

(b) $\sum_{i=0}^{q-1} a_i^t = \begin{cases} 0, & \text{если } t = 0, 1, \dots, .\, q-2; \\ -1, & \text{если } t = q-1. \end{cases}$

Доказательство. Считаем, что $0^0 = 1$. Так как $\mathbb{F}_q = \{0, \zeta^0, \zeta^1, \dots, \zeta^{q-2}\}$, где ζ – примитивный элемент поля $\mathbb{F}_{q,}$, то

$$\sum_{i=0}^{q-1} a_i^t = 0^t + \sum_{i=0}^{q-2} \zeta^{it} = 0^t + \frac{\zeta^{t(q-1)} - 1}{\zeta - 1} = \begin{cases} 0, & \text{если } t = 0, 1, \dots, .q-2; \\ -1, & \text{если } t = q-1. \end{cases}$$

Следовательно, $(a) \Longrightarrow (b)$.

Докажем обратное: $(b) \Longrightarrow (a)$. Рассмотрим многочлены $g_i(x) = 1 - (x - a_i)^{q-1}$, $i = 0, 1, \dots, q-1$. Тогда $g_i(a_i) = 1$ и $g_i(b) = 0$, если $b \in \mathbb{F}_q \setminus \{a_i\}$. Следовательно, многочлен

$$g(x) = \sum_{i=0}^{q-1} g_i(x) = \sum_{i=0}^{q-1} (1 - (x - a_i)^{q-1}) =$$

$$= -\sum_{i=0}^{q-1} \frac{x^q - a_i^q}{x - a_i} = -\sum_{j=0}^{q-1} x^j \sum_{i=0}^{q-1} a_i^{q-1-j}$$

отображает каждый элемент поля $\mathbb{F}_q$ в 1 тогда и только тогда, когда $\{a_0, a_1, \dots, a_{q-1}\} = \mathbb{F}_{q,}$. Так как $deg\ g(x) < q$, то $g(x) \equiv 1$. Другими словами,

$$\sum_{i=0}^{q-1} a_i^{q-1-j} = \begin{cases} 0, & \text{если } j = 1, 2, \dots, .q-1; \\ q - 1 = -1, & \text{если } j = 0, \end{cases}$$

т.е. условие (b) выполняется, и, следовательно, $(b) \Longrightarrow (a)$. □

55.3. ***Теорема*** (Критерий Эрмита [39]–Диксона)**.** *Пусть p – характеристика поля $\mathbb{F}_q$. Многочлен $f(x) \in \mathbb{F}_q[x]$ тогда и только тогда является перестановочным многочленом для множества $S = \mathbb{F}_q$, когда выполняются следующие два условия:*

(a) *многочлен $f(x)$ имеет единственный корень в $\mathbb{F}_q$;*

---

[39] ***Шарль Эрмит*** (24.12.1822 – 14.01.1901) – французский математик, признанный лидер математиков Франции во второй половине XIX века. Член Парижской академии наук с 1856 года, член-корреспондент (1857) и почётный член (1895) Петербургской академии наук, иностранный член Лондонского королевского общества (1873).

(*b*) *для каждого целого* t, *такого, что* $1 \le t \le q-2$ *и* $t \not\equiv 0 \pmod p$, *результат приведения многочлена* $f(x)^t$ *по модулю* $x^q - x$ *имеет степень* $d \le q-2$.

Доказательство. Докажем вначале необходимость условий (*a*) и (*b*). Пусть $f(x)$ – перестановочный многочлен поля $\mathbb{F}_q$. Необходимость условия (*a*) очевидна. Приводя многочлен $f(x)^t$ по модулю $x^q - x$, получаем некоторый многочлен $\sum_{l=0}^{q-1} b_i^{(t)} x^i$. Далее, с учетом леммы 55.2 имеем

$$\sum_{c\in\mathbb{F}_q} f(c)^t = \sum_{c\in\mathbb{F}_q}\sum_{i=0}^{q-1} b_i^{(t)} c^i = \sum_{i=0}^{q-1} b_i^{(t)} \sum_{c\in\mathbb{F}_q} c^i = -\ b_{q-1}^{(t)} \Longrightarrow\ b_{q-1}^{(t)} = 0,$$
$$\forall\ t = 1, 2, \dots, q-2,$$

откуда следует необходимость условия (*b*).

Докажем теперь достаточность условий (*a*) и (*b*). Из условия (*a*) следует, что

$$\sum_{c\in\mathbb{F}_q} f(c)^{q-1} = -1,$$

а из условия (*b*), что

$$\sum_{c\ \in\ \mathbb{F}_q} f(c)^t = 0 \ \text{ для всех } t \not\equiv 0 \pmod p, 1 \le t \le q-2. \qquad (2)$$

Из равенства

$$\sum_{c\in\mathbb{F}_q} f(c)^{tp} = \left(\sum_{c\in\mathbb{F}_q} f(c)^t\right)^p$$

следует, что равенство в (2) имеет место для всех $1 \le t \le q-2$. Для $t = 0$ это очевидно. Тогда из леммы 55.2 следует, что $f(x)$ – перестановочный многочлен поля $\mathbb{F}_q$. □

Замечание. Теорема 55.3 и лемма 55.1 позволяют указать необходимые и достаточные условия, которым должен удовлетворять многочлен $f(x) \in \mathbb{F}_q[x]$, задающий перестановку ρ на множестве S, где S – любое (непустое) подмножество поля $\mathbb{F}_q$. Перестановка ρ может быть продолжена (разными способами) до перестановки τ на множестве $\mathbb{F}_q$. Перестановка τ задается, как и в теореме 55.3, некоторым многочленом $f(x) \in \mathbb{F}_q[x]$, который должен удовлетворять условиям (*a*) и (*b*) этой теоремы. Однако, чтобы обеспечить замкну-

тость действия τ на множестве S, необходимо и достаточно, чтобы выполнялось сравнение (1). □

Пусть $\mathbb{F}_q$ – поле характеристики p, $E_{n,q}$ – подгруппа в $\mathbb{F}_q^*$ порядка n. Так что $n|(q-1)$, $E_{n,q} = \{\zeta^0, \zeta^1, \dots, \zeta^{n-1}\}$, где $\zeta = \alpha^{(q-1)/n}$, α – примитивный элемент поля $\mathbb{F}_q$.

55.4. ***Теорема.*** *Многочлен $f(x) \in \mathbb{F}_q[x]$ является перестановочным многочленом для множества $E_{n,q}$ тогда и только тогда, когда выполнены следующие условия*:

(a) $f(x)^n \equiv 1\ (mod\ x^n - 1)$,

(b) $g_0^{(t)} = \begin{cases} 0, & \text{если } t \in T, \\ 1, & \text{если } t = n, \end{cases}$

где $g_0^{(t)}$ – *свободный член многочлена* $g_t(x) = f(x)^t mod\ (x^n - 1)$ $(g_t(x)$ – *остаток от деления* $f(x)^t$ *на* $(x^n - 1)$, T – *множество чисел* $1,2, \dots, n-1, n+p, n+2p, n+3p, \dots$, *не превосходящих* $q-1$.

Доказательство. Для $t = 1,2, \dots$ положим

$$S_t = \sum_{\xi \in E_{n,q}} f(\xi)^t = \sum_{\xi \in E_{n,q}} g_t(x)$$

и отметим, что

$$S_t = S_{t+q-1};\ S_t = n g_0^{(t)}. \tag{3}$$

Необходимость условий (a) и (b)**.** Если $f(x)$ – перестановочный многочлен на $E_{n,q}$, то условие (a) заведомо выполняется, кроме того,

$$S_t = \sum_{\xi \in E_{n,q}} \xi^t = \begin{cases} 0, & \text{если } t \not\equiv 0\ (mod\ n), \\ n & \text{если } t \equiv n.\ 2n.\ 3n, \dots \end{cases} \tag{4}$$

Сравнивая (3) и (4), заключаем: должно выполняться и условие (b).

Достаточность условий (a) и (b)**.** Пусть выполняются условия (a) и (b). Рассмотрим многочлен

$$\sigma(x) = \prod_{\xi \in E_{n,q}} \big(x - f(\xi)\big) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \dots + (-1)^n \sigma_n$$

и покажем, что $\sigma(x) = x^n - 1$. Это, заметим, равносильно тому, что $f(x)$ – перестановочный многочлен на $E_{n,q}$. Запишем уравнения Ньютона, связывающие элементарные симметрические многочлены σ_i и степенные суммы s_k:

$$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 - \dots + (-1)^{k-1} s_1 \sigma_{k-1} + (-1)^k k \sigma_k = 0, \quad (k \le n); \tag{5}$$

$$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 - \dots + (-1)^{n-1} s_{k-n+1}\sigma_{n-1} + \tag{6}$$

$+(-1)^n s_{k-n}\sigma_n = 0, \quad (k > n).$

Тогда из условия (b) и соотношений (4) следует, что

$s_n = n$, т.е. $s_n \neq 0$; $s_t = 0$ для любого $t \in T$. (7)

Из соотношений (5) следует, что

$\sigma_k = 0$ для любого $k = 1, 2, \dots, n-1, \quad k \not\equiv 0 (mod\ p)$; (8)

$\sigma_n = (-1)^{n-1}$.

Наконец, используя (7) – (8) и последовательно полагая в соотношении (6) $k = n+p, n+2p, n+3p, \dots$, получаем, что $\sigma_k = 0$ для любого $k \equiv 0\ (mod\ p)$, и, следовательно, $\sigma(x) = x^n - 1$. □

Пример. Проиллюстрируем доказательство достаточности условий (a) и (b) теоремы 55.5. Пусть $q = 16, n = 5, p = 2$. Имеем $s_1 = s_2 = s_3 = s_4 = 0, s_5 = 5$. Необходимо доказать, что в этом случае $\sigma(x) = x^5 - 1$. Используя уравнения Ньютона, получаем:

$$\begin{aligned} s_1 - \sigma_1 = 0 \quad &\Longrightarrow \quad \sigma_1 = 0 \\ s_3 - s_2\sigma_1 + s_1\sigma_2 - 3\sigma_3 = 0 \quad &\Longrightarrow \quad \sigma_3 = 0 \\ s_5 - s_4\sigma_1 + s_3\sigma_2 - s_2\sigma_3 + s_1\sigma_4 - 5\sigma_5 = 0 \quad &\Longrightarrow \quad \sigma_5 = 1 \\ s_7 - s_6\sigma_1 + s_5\sigma_2 - s_4\sigma_3 + s_3\sigma_4 - s_2\sigma_5 + s_1\sigma_6 = 0 \quad &\Longrightarrow \quad \sigma_2 = 0 \\ s_9 - s_8\sigma_1 + s_7\sigma_2 - s_6\sigma_3 + s_5\sigma_4 - s_4\sigma_5 + s_3\sigma_6 - s_2\sigma_7 + s_1\sigma_8 = 0 & \\ \Longrightarrow \quad \sigma_4 = 0 & \end{aligned}$$

Так что $\sigma(x) = x^5 - \sigma_5 = x^5 - 1$.

Аналогично доказывается следующее утверждение:

55.5. ***Теорема.*** *Пусть n, p, T – те же, что и в теореме* 55.4, $E_{n,q}^{(0)} = E_{n,q} \cup \{0\}$. *Многочлен $f(x) \in \mathbb{F}_q[x]$, имеющмй корень в $E_{n,q}^{(0)}$, является перестановочным многочленом для $E_{n,q}^{(0)}$ тогда и только тогда, когда выполнены следующие условия*:

(1) $f(x)^{n+1} - f(x) \equiv 0\ (mod\ x^{n+1} - x)$,

(2) $n g_n^{(t)} + (n+1) f(0)^t = \begin{cases} 0, & \text{если } t \in T, \\ n, & \text{если } t = n, \end{cases}$

где $g_n^{(t)}$ – коэффициент при x^n в многочлене $g_t(x) = f(x)^t \ mod\ (x^{n+1} - x)$.

55.6. ***Теорема*** [2]. *Многочлен x^m является перестановочным для множеств $\mathbb{F}_q$ и $\mathbb{F}_q^*$ тогда и только тогда, когда $q-1$ и m* взаимно просты.

55.7. ***Теорема*** [2]. *Если $q = p^u$, где u нечетно, а $p = 5m \pm 2$, то многочлен $5x^5 + 5\nu x^3 + \nu^2 x$ является перестановочным для множеств $\mathbb{F}_q$ и $\mathbb{F}_q^*$ при любом $\nu \in \mathbb{F}_q$.*

55.8. ***Теорема*** [**2**]. *Пусть* $sl = p^t - 1, d = (s, q-1), \quad q = p^u$, $\nu \in \mathbb{F}_q$. *Многочлен* $f(x) = x(x^s - \nu)^l \in \mathbb{F}_q[x]$ *является перестановочным множеств* $\mathbb{F}_q$ *и* $\mathbb{F}_q^*$ *тогда и только тогда, когда* $\nu \notin E_{\frac{q-1}{d},q} = \{\beta^s \mid \beta \in \mathbb{F}_q^*\}$.

55.9. ***Теорема*** [**24**, теорема 7.10]**.** *Пусть* $\mathbb{F}_q$ *– конечное поле,* $r \in \mathbb{N}$, НОД $(r, q-1) = 1$, $f(x) \in \mathbb{F}_q[x]$ *– многочлен, такой, что* $f(x^s)$ *не имеет ненулевых корней в* $\mathbb{F}_q$. *Тогда многочлен* $x^r f(x^s)^{(q-1)/s}$ *является перестановочным многочленом поля* $\mathbb{F}_q$.

55.10. ***Теорема*** ([**24**], теорема 7.24). *Многочлен*

$$\psi(x) = \sum_{i=0}^{m-1} \alpha_i x^{q^i} \in \mathbb{F}_{q^m}[x].$$

Является перестановочным для поля $\mathbb{F}_q$ *тогда и только тогда, когда* $x = 0$ *– единственное решение в* $\mathbb{F}_{q^m}$ *уравнения* $\psi(x) = 0$.

Множество всех перестановок $x \longrightarrow \psi(x)$ *на элементах поля* $\mathbb{F}_{q^m}$ *образует группу, которую называют группой Бетти-Матье. Эта группа изоморфна полной линейной группе* $GL(m, q)$*, образованной всевозможными обратимыми* $(m \times m)$*-матрицами над полем* $\mathbb{F}_q$. *Её порядок равен*$(q^m - 1)(q^m - q) \dots (q^m - q^{m-1})$.

§ 56. Вычисления в поле GF(2^8)

Конечное поле $GF(2^8) = \mathbb{F}_{256}$, состоящее из 256 элементов, привлекательно для построения криптографических примитивов. В данном случае байты (8-битовые блоки) могут быть интерпретированы как элементы этого поля, а операции над элементами поля легко реализуемы.

Поле $\mathbb{F}_{256}$ можно рассматривать как факторкольцо $\mathbb{F}_2\,[x]\,/\,(f(x))$, где $f(x) \in \mathbb{F}_2\ [x]$ – неприводимый многочлен 8- ой степени [40]. На более простом языке это означает следующее. Элементы поля $\mathbb{F}_{256}$ представлены всевозможными многочленами

---

[40] Многочлен $f(x)$ необходимо зафиксировать. Выбор другого многочлена приведет в некоторому полю $\mathbb{F}'_{256}$ с другим представлением элементов. С алгебраической (абстрактной) точки зрения поля $\mathbb{F}_{256}$ и $\mathbb{F}'_{256}$изоморфны, т.е. отличают-

Элементы поля $\mathbb{F}_{256}$ представлены всевозможными многочленами

$$a(x) = a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x^1 + a_0$$

с коэффициентами из поля $\mathbb{F}_2 = \{0,1\}$, а многочлены в свою очередь, представлены 8-битовыми наборами (байтами) $a_7a_6a_5a_4a_3a_2a_1a_0$. Например, многочлен $x^6+x^5 + x^3+x^1 + 1$ представлен двоичным набором 01101011 (или байтом $0\text{x}6b$ в 16–ричной записи). Операция сложения ($\oplus$) элементов поля $\mathbb{F}_{256}$ – это обычная операция сложения многочленов из $\mathbb{F}_2[x]$. Поскольку многочлены представлены байтами, то в данном случае сложение – это побитовое сложение байтов по модулю 2 (операция $\oplus$, или xor).

Операция умножения ($\odot$) в поле $\mathbb{F}_{256}$ реализуется сложнее, а именно: $a(x)\odot b(x) = c(x)$, где $c(x) = a(x) \cdot b(x)\ mod\ f(x)$ – остаток от деления многочлена $a(x) \cdot b(x)$ на $f(x)$.

Пример. Пусть $f(x) = x^8+x^4 + x^3+x^2 + 1$ – неприводимый многочлен, на основе которого определяется конкретная реализация поля $\mathbb{F}_{256} \cong \mathbb{F}_2[x]/(f(x))$ и пусть $a(x) = x^7+x^5+x^1 + 1$ и $b(x) = x^6 + x^5 + x^4+x^3+x^1 + 1$ – многочлены, представляющие элементы данного поля. Тогда $a(x) \oplus b(x) = x^7+x^6+x^4+x^3$, $a(x) \odot b(x) = x^7 + x^3 + x^1 + 1$ (поскольку $a(x)b(x) = x^{13} + x^{12} + x^9 + x^6 + x^5 + x^3 + x^2 + 1 = (x^5 + x^4)f(x) + x^4 + x^3 + x^2 + 1$), или, на "языке байтов",

$$a(x) = 0\text{x}a3,\ b(x) = 0\text{x}7b;$$

$$\text{x}a3 \oplus 0\text{x}7\text{b} = 0\text{x}d8,\ \ a(x) \odot b(x) = 0\text{x}1d.$$

Вычисление многочлена $c(x) = a(x)b(x)\ mod\ f(x)$ сводится к вычислению

$$a(x) \cdot x^m\ mod\ f\ (x) = (((a(x) \cdot x)\ mod\ f(x))\ x^{m-1})\ mod\ f(x),$$

причем

ся только обозначениями элементов. Тем не менее, поля $\mathbb{F}_{256}$ и $\mathbb{F}'_{256}$в некоторых случаях следует считать различными, поскольку элементы этих полей могут участвовать в суррогатных вычислениях (т.е. в рамках разных вычислительных систем). Например, элементы поля $\mathbb{F}_{256}$, представленные байтами, могут интерпретироваться как элементы кольца $\mathbb{Z}_{256}$ целых чисел по модулю 256, и как элементы мультипликативной группы целых чисел по модулю 257 и т.п. Итоговый результат таких смешанных вычислений зависит от того, как согласованы представления элементов.

$$(a(x)\cdot x)\ mod\ f(x)=\begin{cases} a(x)\cdot x, & \text{если } a_7=0\,,\\ a(x)\cdot x-f(x), & \text{если } a_7=0 \end{cases}$$

(заметим, что в поле характеристики 2 сложение и вычитание − одно и то же).

Пусть $g(x)$ − многочлен седьмой степени такой, что $f(x)=x^8+g(x)$; будем считать, что многочлен $g(x)$ представлен байтом g. Тогда вычисление $c=a\odot b$ – произведения элементов $a,\ b\in\mathbb{F}_{256}$ – можно выполнить по схеме (где все элементы – байты):

$c:=$ 0x00;
$mask:=$ 0x01;
for $i:=\ 0$ ***to*** 7 ***do*** {
if $(b\&\ mask)\neq$ 0x00 ***then*** $c:=c\oplus a$;
if $(a\&$ 0x80$)=$ 0x00 ***then*** $a:=shl_1(a)$***else*** $a:=shl_1(a)\oplus g$;
NB. Здесь $shl_1(a)$ – сдвиг битов байта a на одну позицию влево.
$mask:=shl_1(mask)$
}.

Значение $c=a^m(a,\ c\in\mathbb{F}_{256},\ m\in\mathbb{N})$ вычисляется по быстрой схеме:

$c:=$ 0x01;
while $m>0$ ***do*** {
if m нечетно ***then*** $c:=c\odot a$;
$a:=a\odot a$;
$m:=m$ ***div*** 2
}.

Отметим, что $0^0=1$ и $0^m=0$ для $m\ \geq 1$; если $a\neq 0$, то $a^{-n}=a^{255-n}$ ввиду $a^{255}=1$.

Мультипликативный порядок $ord(a)$ ненулевого элемента $a\in\mathbb{F}_{256}$ определяется как наименьшее $m\in\mathbb{N}$, для которого $a^m=1$. Значение $ord(a)$ можно вычислить по схеме:

$ord:=255;\ p[1]:=3;\ p[2]:=5;\ p[3]:=7;$
for $i:=1$ ***to*** 3 ***do*** {
$m:=ord\ div\ p[i]$;
if $a^m=1$ ***then*** $ord:=m$
}.

В поле $\mathbb{F}_{256}$ имеется $\varphi(255) = \varphi(3 \cdot 5 \cdot 17) = 2 \cdot 4 \cdot 16 = 128$ элементов порядка 255 ($\varphi(\cdot) -$ функция Эйлера); такие элементы называются *примитивными*. Пусть ω – один из них. Поиск ω можно осуществить по схеме:

$$\omega := 0\text{x}02;\ \textbf{\textit{while}}\ ord(\omega) < 255\ \textbf{\textit{do}}\ \omega := \omega + 1,$$

где символ " $+$ " обозначает обычное арифметическое сложение байтов. Любой другой примитивный элемент ω′ может быть вычислен как $\omega' := \omega^m$, где m – число, взаимно простое с 255. Тот факт, что $ord\ (\omega) = 255$, означает, что мультипликативная группа $\mathbb{F}_{256}^*$, состоящая из ненулевых элементов поля $\mathbb{F}_{256}$, является циклической, т.е. $\mathbb{F}_{256}^* = \mathbb{F}_{256} \backslash \{0\} = \{\omega^0, \omega^1, \ldots, \omega^{254}\}$.

Целое число j $(0 \le j \le 254)$ такое, что $a = \omega^j$, называется *дискретным логарифмом элемента* $a \in \mathbb{F}_{256}^*$ *по основанию* ω и обозначается $ind_\omega a$. Операции умножения и возведения в степень можно ускорить, если построить две вспомогательные таблицы $TD[0..254]$ и $TL[1..255]$, определяемые как $TD_j = \omega^j$, $TL_j = j$, $j = 0, 1, \ldots, 254$. Таблицы заполняются следующим образом:

```
a := 1;
for j := 0 to 254 do {
    TL[a] := j; TD[j] := a; a := a⊙ω
}.
```

Для любых $a, b \in \mathbb{F}_{256}^*$ имеем:

$$a \odot b = TD[(TL[a] + TL[b]) mod\ 255];$$
$$a^m = TD[(m * TL[a])\ mod\ 255], m \in N.$$

Если элементы мультипликативной группы $\mathbb{F}_q^*$ поля $\mathbb{F}_q$ представлены степенями фиксированного примитивного элемента $\beta \in \mathbb{F}_q^*$, то сложение в поле $\mathbb{F}_q$ облегчается, если использовать *логарифмы Якоби*[41] $L(n)$, определяемые равенством $1 + \beta^n = \beta^{L(n)}$, где случай

---

[41] ***Карл Густав Якоб Якоби*** (10 12.1804 – 18.02.1851) – немецкий математик и механик. Внёс огромный вклад в комплексный анализ, линейную алгебру, динамику и другие разделы математики и механики. Член Берлинской (1836) и Венской (1848) академий наук, Лондонского королевского общества (1833), член-корр. Парижской (1830), иностранный член-корр. Петербургской (1830, с

$\beta^n = -1$ исключается. (Для $1 + \beta^n = 0$ полагаем $L(n) = *$. Другими словами, $0 = \beta^*$. Отметим, что $\beta^n = -1$ при $n = (q-1)/2$.) Если $m \geq n$ и L определен, то $\beta^m + \beta^n = \beta^n(1 + \beta^{m-n}) = \beta^{n+L(m-n)}$.

1833 года – её почётный член) и Мадридской (1848) академий наук. Логарифмы Якоби называют также *логарифмами Зеха* (или *Зеча*).

Глава VI. Решение уравнений в $\mathbb{Z}$ по модулю n

§ 57. Сравнения с одним неизвестным

Пусть $f(x) = ax^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{Z}[x]$, $m \in \mathbb{N}, a \neq 0$, $m \nmid a$. Рассмотрим сравнение

$$f(x) \equiv 0 \ (mod\ m). \qquad (1)$$

Число n называется *степенью* этого сравнения. Решением сравнения называется множество всех $x \in \mathbb{Z}$, которые удовлетворяют (1). Если x − одно из решений сравнения (1), то любое число $y \equiv x \ (mod\ m)$ также удовлетворяет (1), т.е. является решением этого сравнения. Класс чисел $\{y \mid y \in \mathbb{Z},\ y \equiv x \ (mod\ m)\}$ рассматривается как одно решение. Другими словами, решениями являются различные элементы кольца $\mathbb{Z}_m$, удовлетворяющие (1). Если $m = p$ − простое число, то $\mathbb{Z}_m$ − поле $\mathbb{F}_p$. В этом случае решениями (1) являются корни многочлена $f(x) \in \mathbb{F}_p[x]$. При этом число корней с учетом их кратностей не превосходит $n = \deg f(x)$. Если m − составное число, то $\mathbb{Z}_m$ − кольцо с делителями нуля; в этом случае число решений сравнения (1) может превосходить степень многочлена $f(x)$. Например, сравнение второй степени $x^2 \equiv 1 \ (\mathrm{mod}\ 8)$ и сравнение третьей степени $x^3 \equiv 0 \ (\mathrm{mod}\ 8)$ имеют по четыре решения. В первом случае решения суть 1, 3, 5, 7, а во втором − 0, 2, 4, 6. Вопрос о вычислении корней многочленов над конечными полями рассмотрен в главе VII.

§ 58. Двучленные сравнения. Символы Лежандра [42] и Якоби

Пусть $n \in \mathbb{N}$; $a, m \in \mathbb{Z}$. Рассмотрим сравнение

---

[42] ***Адриен Мари Лежандр*** (18.09.1752 – 10.01.1833) − французский математик. Обосновал и развил теорию геодезических измерений, продвинул сферическую тригонометрию. В области математического анализа ввел т. н. многочлены Лежандра, преобразование Лежандра и исследовал эйлеровы интегралы I и II рода. Доказал приводимость эллиптических интегралов к каноническим формам, нашёл их разложения в ряды. Член Парижской Академии наук (с 1783).

$$x^n \equiv a\ (mod\ m),\ \text{НОД}\ (a, m) = 1. \qquad (1)$$

Если сравнение (1) имеет решение $x \in \mathbb{Z}$, то число $y = x + km$, $k \in \mathbb{Z}$, также будет решением этого сравнения. Одно из чисел y лежит в множестве $\mathbb{Z}_m = \{0, 1,\ldots, m-1\}$. Как отмечено выше, рассматриваются только те решения сравнения (1), которые лежат в $\mathbb{Z}_m$. Так как НОД$(a, m) = 1$, то $a \not\equiv 0\ (mod\ m)$. Также можно считать, что $a \in \mathbb{Z}_m$.

Определение. Если сравнение (1) имеет решение, то число a называется *вычетом степени n по модулю m*, в противном случае a называется *невычетом степени n по модулю m*. При $n = 2$ вычеты называются *квадратичными* (или *квадратами*), при $n = 3$ – *кубическими* (*кубами*), при $n = 4$ – *биквадратичными* (*биквадратами*).

Далее рассматривается случай $n = 2$, причем вначале рассматриваются двучленные сравнения по простому нечетному модулю p:

$$x^2 \equiv a\ (mod\ p),\ (a, p) = 1. \qquad (2)$$

58.1. ***Теорема.*** *Если a – квадратичный вычет, то уравнение* (1) *имеет в точности два решения в $\mathbb{Z}_p$: если $x_1 \in \mathbb{Z}_p$ – решение, то $x_2 = p - x_1 (mod\ p)$ – второе решение.*

Доказательство. Так как p нечетно, то $x_1 \not\equiv x_2\ (\text{mod}\ p)$. Этими двумя решениями исчерпываются все решения сравнения (3). □

58.2. ***Теорема.*** *Приведённая система вычетов по модулю p состоит из $(p-1)/2$ квадратичных вычетов, сравнимых с числами*

$$1^2, 2^2, 3^2,\ldots, ((p-1)/2)^2, \qquad (3)$$

и такого же числа квадратичных невычетов.

Доказательство. Квадратичными вычетами в $\mathbb{Z}_p$ являются квадраты следующих элементов: $1, 2,\ldots, p-1)/2, p-1, p-2,\ldots, p-(p-1)/2)$. Числа (3) попарно не сравнимы по модулю p, поскольку $b^2 \equiv c^2\ (\text{mod}\ p) \Longrightarrow\ (b-c)(b+c) \equiv 0\ (mod\ p) \Longrightarrow b \equiv c$ или $b \equiv p - c\ (mod\ p)$. Кроме того, $b^2 \equiv (p-b)^2\ (mod\ p)$. □

58.3. ***Теорема.*** *Если a – квадратичный вычет по модулю p, то*

$$a^{(p-1)/2} \equiv 1\ (mod\ p); \qquad (4)$$

если a – квадратичный невычет по модулю p, то

$$a^{(p-1)/2} \equiv -1\ (mod\ p). \qquad (5)$$

Доказательство. Согласно Малой теореме Ферма имеем

$$a^{p-1} \equiv 1\ (mod\ p) \Longrightarrow \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv\ 0\ (mod\ p),$$

откуда следует одно из сравнений (4) или (5), но не оба одновременно (в противном случае, вычитая из первого сравнения второе, получаем $0 \equiv 2 \pmod{p}$, что невозможно для нечетного числа p).

Каждый квадратичный вычет a удовлетворяет сравнению вида (2) для некоторого $x \in \mathbb{Z}$, из него следует сравнение (4). Последнее сравнение имеет не более $(p-1)/2$ решений относительно a. Такими числами a являются $(p-1)/2$ чисел вида (3). □

Символ Лежандра $\left(\frac{a}{p}\right)$ определяется для всех a, не делящихся на p, как

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{если } a - \text{ квадратичный вычет по модулю } p, \\ -1, \text{если } a - \text{ квадратичный невычет по модулю } p. \end{cases}$$

Если $a = 0$, то полагают $\left(\frac{a}{p}\right) = 0$.

Из теоремы 58.3 следует, что

$$\left(\frac{a}{p}\right) = a^{(p-1)/2}. \qquad (7)$$

58.4. ***Теорема.*** *Символ Лежандра удовлетворяет следующим свойствам:*

A. $a \equiv b \ (mod\ p) \Longrightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

B. $\left(\frac{1}{p}\right) = 1$;

C. $\left(\frac{-1}{p}\right) = \left(\frac{p-1}{p}\right) = (-1)^{(p-1)/2}$;

D. $\left(\frac{ab\ldots c}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\ldots\left(\frac{c}{p}\right)$;

E. $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$.

Доказательство. *A*. Свойство вытекает из того факта, что числа a и b одновременно являются либо квадратами, либо не являются квадратами по модулю p. *B.* Свойство очевидно: так как $1^2 = 1$, то $1-$ квадратичный вычет. *C.* Вытекает из свойства a и равенства (5). Если $p -$ число вида $4m + 1$, то -1 является квадратичным вычетом по модулю p; если $p -$ число вида $4m + 3$, то -1 является квадратичным невычетом по модулю p. *D*. Вытекает из следующей цепочки равенств:

$$\left(\frac{ab\dots c}{p}\right) = (ab\dots c)^{(p-1)/2} = a^{(p-1)/2}b^{(p-1)/2}\dots c^{(p-1)/2}$$
$$= \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\dots\left(\frac{c}{p}\right).$$

E. Вытекает из свойства *D*. В частности, $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$. Поэтому из числителя символа Лежандра можно удалить любой квадрат. □

58.5. ***Теорема.*** *Для нечетного простого числа p имеем*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1, & \text{если } p = 8m+1 \text{ или } 8m+7; \\ -1, & \text{если } p = 8m+3 \text{ или } 8m+5. \end{cases}$$

Доказательство. См.[**10**], гл. V, § 2; или [**3**].

57.5. ***Теорема*** Гаусса. *Для нечетных простых чисел p и q имеет место следующий закон взаимности квадратичных вычетов*:

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right). \qquad (8)$$

Доказательство. См. там же.

Пусть $R = p_1p_2\dots p_k$ − разложение нечетного числа $R \geq 3$ на простые сомножители, среди которых могут быть равные. Пусть числа P и a взаимно просты. *Символ Якоби* $\left(\frac{a}{P}\right)$ определяется равенством $\left(\frac{a}{R}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_k}\right)$.

Символ Якоби по своим свойствам аналогичен символу Лежандра, но имеются и новые, которые позволяют ускорить вычисление символа Лежандра ([**10**], гл. V, § 3)):

A. $a \equiv b \pmod R \Longrightarrow \left(\frac{a}{R}\right) = \left(\frac{b}{R}\right)$;

B. $\left(\frac{1}{R}\right) = 1$;

C. $\left(\frac{-1}{R}\right) = \left(\frac{R-1}{R}\right) = (-1)^{(R-1)/2}$;

D. $\left(\frac{ab\dots c}{R}\right) = \left(\frac{a}{p_1}\right)\left(\frac{b}{p_1}\right)\dots\left(\frac{c}{p_1}\right)\dots\left(\frac{a}{p_k}\right)\left(\frac{b}{p_k}\right)\dots\left(\frac{c}{p_k}\right) = \left(\frac{a}{R}\right)\left(\frac{b}{R}\right)\dots\left(\frac{c}{R}\right)$;

E. $\left(\frac{ab^2}{R}\right) = \left(\frac{a}{R}\right)$;

F. $\left(\frac{2}{R}\right) = (-1)^{\frac{R^2-1}{8}}$;

G. $\left(\frac{Q}{R}\right) = (-1)^{\frac{R-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{R}{Q}\right)$.

§ 59. Сравнения второй степени по составному модулю

59.1. ***Теорема***. *Пусть* $m = m_1 m_2 \dots m_k \in \mathbb{N}$, *где* $m_1, m_2, \dots, m_k$ *– попарно взаимно простые натуральные числа. Тогда сравнение*

$$f(x) \equiv 0 \ (mod\ m) \qquad (1)$$

равносильно системе сравнений

$$\begin{cases} f(x) \equiv 0 \ (mod\ m_1), \\ \dots \\ f(x) \equiv 0 \ (mod\ m_k). \end{cases} \qquad (2)$$

Число решений сравнения (1) *равно* $S = S_1 S_2 \dots S_k$ **,** *где* S_i *– число решений* i*-го сравнения в системе* (2), $i = 1, 2, \dots, k$**.**

Доказательство. Первая часть утверждения о равносильности (1) и (2) вытекает из свойств сравнений в § 7.

Вторая часть утверждения об общем числе решений достаточно очевидна. Пусть x_i – любое из S_i решений сравнения $f(x) \equiv 0 \ (mod\ m_i)$, $i = 1, 2, \dots, k$. Тогда общее число решений системы сравнений (2) равно $S_1 S_2 \dots S_k = S$ – числу наборов $(x_1, x_2, \dots, x_k)$. □

59.2. ***Следствие***. *Решение сравнения* (1)*, где* $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, *где* $p_1, p_2, \dots, p_k$ *- различные простые числа, сводится к исследованию и решению сравнений вида*

$f(x) \equiv 0 \ (mod\ p^{\alpha})$, p *– простое число,* $\alpha \in \mathbb{N}$. (3)

Рассмотрим алгоритм Виноградова [43] нахождения решений сравнения (3), изложенный в [**10**]. Сравнение (3) сводится (при некоторых ограничениях на $f(x)$) к сравнению

$$f(x) \equiv 0 \ (mod\ p). \qquad (4)$$

Замечание. Вопрос о вычислении корней многочлена $f(x) \in \mathbb{F}_p[x]$ рассматривается ниже в главе VII. □

Во-первых, отметим, что всякое x, удовлетворяющее (3), должно также удовлетворять и сравнению (4). Пусть $x \equiv x_1 \ (mod\ p)$ – какое-либо решение сравнения (4). Тогда $x = x_1 +$

---

[43] ***Иван Матвеевич Виноградов*** (2(14).09.1891—20.03.1983) — выдающийся советский математик (в области аналитической теории чисел), академик АН СССР (с 1929) по Отделению физико-математических наук (математика).

pz_1, $z_1 \in \mathbb{Z}$, $-$ также решение сравнения (4). Подставим x в сравнение $f(x) \equiv 0\ (mod\ p^2)$ и разложим левую часть по формуле Тейлора. В результате (принимая во внимание, что $\frac{1}{k!}f^{(k)}(x) -$ целое число, и отбрасывая члены, кратные p^2) получим

$$f(x_1) + pz_1 f'(x_1) \equiv 0\ (mod\ p^2), \frac{f(x_1)}{p} + z_1 f'(x_1) \equiv 0\ (mod\ p).$$

Ограничиваясь случаем $p \nmid f'(x_1)$, имеем одно решение:

$$z_1 \equiv u_1\ (mod\ p),\ z_1 \equiv u_1 + pz_2.$$

Выражение для x принимает вид

$$x = x_1 + pu_1 + p^2 z_2 = x_2 + p^2 z_2,$$

Подставляя x в сравнение $f(x) \equiv 0\ (mod\ p^3)$, получим

$$f(x_2) + p^2 z_2 f'(x_2) \equiv 0\ (mod\ p^3),$$

$$\frac{f(x_2)}{p^2} + z_2 f'(x_2) \equiv 0\ (mod\ p^2), \qquad (5)$$

причем $p \nmid f'(x_2)$, так как $x_2 \equiv x_1 (mod\ p)$,

$$f'(x_2) \equiv f'(x_1)\ (mod\ p).$$

Поэтому сравнение (5) имеет одно решение $z_2 \equiv u_2\ (mod\ p)$, $z_2 = u_2 + pz_3$, а x в этом случае принимает вид $x = x_2 + p^2 u_2 + p^3 z_3 = x_3 + p^3 z_3$ и т.д.

Указанные действия позволяют, исходя из решения сравнения (4), постепенно найти сравнимое с ним решение сравнения (3). Таким образом, имеет место следующая

59.3. ***Теорема***. *Всякое решение* $x = x_1\ (mod\ p)$ *сравнения* (4) *при условии, что* $p \nmid f'(x_1)$*, дает одно решение сравнения* (3):

$$x = x_\alpha + p^\alpha z_\alpha;\ x = x_\alpha\ (mod\ p^\alpha).$$

В заключение этого раздела рассмотрим сравнение второй степени по составному модулю. Начнем со сравнения

$$x^2 - a \equiv 0\ (mod\ p^\alpha),\ p\ -\text{нечетное простое число},\ \alpha \in \mathbb{N},\ \text{НОД}\ (a,p) = 1. \qquad (6)$$

Полагая $f(x) = x^2 - a$, имеем $f'(x) = 2x$. Пусть $x \equiv x_1\ (mod\ p) -$ какое-либо решение сравнения (4). x_1 существует, если $a -$ квадратичный вычет по модулю p, и не существует, если $a -$ квадратичный невычет по модулю p. Допустим первое. Тогда НОД $(a,p) =$ НОД $(x_1,p) =$ НОД $(2x_1,p) = 1 \Longrightarrow p \nmid f'(x_1)$. Следовательно, для разыскания решений сравнения (6) можно использовать описанный выше метод, примененный к сравнению (3). Та-

ким образом, имеет место следующее утверждение о числе решений сравнения (6):

59.4. ***Теорема***. *Сравнение* (6) *имеет два решения, если* $a -$ *квадратичный вычет, и не имеет решений, если* $a -$ *квадратичный невычет по модулю* p.

Теперь рассмотрим сравнение

$$x^2 - a \equiv 0 \pmod{2^\alpha},\ \alpha \in \mathbb{N},\ \text{НОД}\ (a, 2) = 1. \qquad (7)$$

Здесь $2 \mid f'(x_1)$. Поэтому описанный выше метод разыскания решений этого сравнения неприменим. Пусть сравнение разрешимо. Тогда НОД $(a, 2) = 1 \Longrightarrow$ НОД $(x, 2) = 1 \Longrightarrow x = 2m + 1 \Longrightarrow x^2 - 1 = 4m(m + 1) \Longrightarrow 8 \mid (x^2 - 1)$. Приводя сравнение (7) к виду $(x^2 - 1) + 1 \equiv a\ (mod\ 2^\alpha)$, заключаем, что для разрешимости этого сравнения необходимо

$$a \equiv 1\ (mod\ 4) \text{ при } \alpha = 2;\ a \equiv 1\ (mod\ 8) \text{ при } \alpha \geq 3. \qquad (8)$$

Далее рассмотрим вопрос о числе решений сравнения (7), считая, что (8) выполняется.

Случай $\alpha = 1$. Сравнения (7) имеет одно решение: $x \equiv 1\ (mod\ 2)$.

Случай $\alpha = 2$. Сравнения (7) имеет два решения: $x \equiv 1, 3\ (mod\ 4)$.

Случай $\alpha = 3$. Сравнения (7) имеет четыре решения: $x \equiv 1, 3, 5, 7\ (mod\ 8)$.

Случай $\alpha > 3$. Числа $a = (2t + 1)^2\ (mod\ 2^\alpha)$, при $t = 0, 1, \ldots, \alpha$, удовлетворяют (8) и различны. Каждое сравнение $x^2 \equiv a\ (mod\ 2^\alpha)$, $a \equiv (2t + 1)^2$, имеет четыре решения:

$$2t + 1,\ 2t + 1 + 2^{\alpha-1},\ -(2t + 1),\ -(2t + 1 + 2^{\alpha-1})\ (mod\ 2^\alpha).$$

Из полученных в данном разделе результатов следует

59.5. ***Теорема***. *Для разрешимости сравнения* (7) *необходимо и достаточно выполнение условий* (8). *Если эти условия выполнены, то число решений равно*: 1 *при* $\alpha = 1$; 2 *при* $\alpha = 2$; 4 *при* $\alpha \geq 3$.

Для разрешимости сравнения общего вида

$$x^2 \equiv a\ (mod\ m),\ \alpha \in \mathbb{N},\ m = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k},\ \text{НОД}\ (a, m) = 1$$

необходимыми условиями являются (6) *и* $\left(\frac{a}{p_1}\right) = \left(\frac{a}{p_2}\right) = \cdots = \left(\frac{a}{p_k}\right) = 1$. *Если все условия выполнены, то число решений равно*: 2^k *при* $\alpha = 0$ и $\alpha = 1$; 2^{k+1} *при* $\alpha = 2$; 2^{k+2} *при* $\alpha \geq 3$.

Глава VII. Решение алгебраических уравнений в конечных полях

§ 60. Решение двучленных уравнений

Пусть $\mathbb{F}_q$ – поле характеристики p (p – простое число), содержащее $q = p^s$ элементов, $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$ – мультипликативная группа этого поля. Рассмотрим уравнение

$$x^m - a = 0,\ a \in \mathbb{F}_q^*. \qquad (1)$$

Представим число m в виде $m = p^t n$, где t – неотрицательное целое, НОД $(n, p) = 1$. Тогда ввиду $u^{p^s} = u$, $(u \pm v)^{p^k} = u^{p^k} \pm v^{p^k}$ для любых $k \in \mathbb{N}$ и $u, v \in \mathbb{F}_q$, уравнение (1) приводится к виду

$(x^n - b)^{p^t} = 0,\ b = a^{p^r},\ r \equiv -t\ (mod\ s),\ 0 \le r < s.$

Каждый корень этого уравнения имеет кратность p^t. Поэтому далее можно ограничиться исследованием уравнения

$$x^n - b = 0,\ b \in \mathbb{F}_q^*,\ \text{НОД}\ (n, p) = 1, \qquad (2)$$

все корни которого имеют кратность 1.

Элемент $b \in \mathbb{F}_q^*$ называется *вычетом степени* n, если уравнение (2) имеет решение $x \in \mathbb{F}_q^*$, в противном случае элемент b называется *невычетом степени* n (при $n = 2$ вычеты и невычеты называются *квадратичными*, при $n = 3$ – *кубическими*, при $n = 4$ – *биквадратными*).

Мультипликативная группа $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$ поля $\mathbb{F}_q$ является *циклической*, т.е. $\mathbb{F}_q^* = <\alpha> = \{\alpha^0, \alpha^1, \dots, \alpha^{q-2}\}$, где $\alpha \in \mathbb{F}_q^*$ – некоторый элемент (называемый *примитивным элементом поля* $\mathbb{F}_q$). Пусть $b = \alpha^z$. Уравнение (2) имеет в $\mathbb{F}_q^*$ решение $x = \alpha^y$ тогда и только тогда, когда имеет решение сравнение

$$ny \equiv z\ mod\ (q - 1). \qquad (3)$$

Предположим, что это сравнение имеет решение и НОД $(n, q-1) = d$. Тогда $n_1 d = n$, $q_1 d = q - 1$, НОД $(n_1, q_1) = 1$ и $d \mid z$ (т.е. z делится на d без остатка), $z = z_1 d$. В этом случае сравнение (3) равносильно сравнению $n_1 y \equiv z_1\ mod\ q_1$, которое имеет единственное решение относительно $y \in [0, q_1 - 1]$, а именно: $y \equiv z_1 n_1^{-1}\ mod\ q_1$, где n_1^{-1} – *мультипликативный обратный элемент к* n_1 *по*

модулю q_1, т.е. $n_1 n_1^{-1} \equiv 1 \, mod \, q_1$. Отсюда следует, что решениями сравнения (3) являются: $y, y + q_1, \dots, y + (d-1) q_1$, а уравнение (2) имеет d решений (корней): $x = \alpha^{y+iq_1}$, $i = 0, 1, \dots, d-1$. Имеет место

60.1. ***Теорема***. *Уравнение* (2) *имеет в точности* $d = \text{НОД}(n, q-1)$ *решений в* $\mathbb{F}_q^*$, *где* $q = p^s$, *тогда и только тогда, когда* $b^{\frac{q-1}{d}} = 1$. *Если* $b^{\frac{q-1}{d}} \neq 1$, *то решений, лежащих в* $\mathbb{F}_q^*$, *нет*.

Доказательство. Пусть $b = \alpha^z$. Если $d \nmid z$, то сравнение (3) не имеет решений, и $b^{\frac{q-1}{d}} \neq 1$. Если решение (корень) уравнения (2) существует, то $x^{n\frac{q-1}{d}} = x^{n_1(q-1)} = 1$. □

Чтобы найти решение уравнения (2), необходимо вычислить z, для которого $a = \alpha^z$. Это задача дискретного логарифмирования.

§ 61. Алгоритм дискретного логарифмирования

Пусть $\alpha -$ примитивный элемент поля $\mathbb{F}_q$. Уравнение

$$\alpha^z = b \qquad (1)$$

всегда разрешимо (причем однозначно) относительно $z \in \{0, 1, \dots, q-2\}$ для любого $b \in \mathbb{F}_q^*$. Число z называется *дискретным логарифмом* (или *индексом*) *элемента* b *по основанию* α. Соответствующее z обозначается как $ind_\alpha \, b$. Задача дискретного логарифмирования заключается в вычислении значения $z = ind_\alpha \, b$. Вычисление можно осуществить путем последовательного перебора чисел $z \in \{0, 1, \dots, q-2\}$. В общем случае, когда q велико, это трудная задача ввиду, возможно, большого объёма вычислений. Рассмотрим алгоритм, который позволяет быстро решать задачу дискретного логарифмирования, если $q-1$ есть произведение относительно небольших простых чисел.

Пусть $q - 1 = p^k h$, НОД $(p, h) = 1, p -$ простое число. Алгоритм последовательно строит целые числа u_j, $j = 0, 1, \dots, k$, которые удовлетворяют равенству

$$(b^h \alpha^{-hu_j})^{p^{k-j}} = 1. \qquad (2)$$

Замечание. Все вычисления проводятся в поле $\mathbb{F}_q$. □

Так как $b^{p^k h} = 1$, то $b^{hp^{k-1}} -$ корень уравнения $x^p - 1 = 0$. Все корни последнего уравнения исчерпываются элементами c^i,

$i = 0, 1, \ldots, p-1$, где $c = \alpha^{hp^{k-1}}$. Поэтому путем перебора можно найти значение c^{u_0}, удовлетворяющее равенству (2) при $j = 0$, т.е. $b^{hp^{k-1}} = c^{u_0}$. Предположим, что найдено значение u_j, удовлетворяющее уравнению (2). Определим число t с помощью уравнения

$$(b^h \alpha^{-hu_j})^{p^{k-(j+1)}} = c^t, \qquad (3)$$

и положим $u_{j+1} = u_j + tq^j$. Тогда имеют место равенства

$$(b^h \alpha^{-hu_{j+1}})^{p^{k-(j+1)}} = c^t \alpha^{-thp^{k-1}} = 1, \qquad (4)$$

которые означают, что u_{j+1} удовлетворяет (2) при замене j на $j + 1$. Для $j = k$ равенство (2) ввиду (1) означает, что $\alpha^{(z-u_k)h} = 1$. Так как α – образующий элемент группы $\mathbb{F}_q^*$, то

$$(z - u_k)h \equiv 0\ (mod\ q-1) \Longrightarrow z \equiv u_k (mod\ p^k)\ .$$

Если $q - 1 = p_1^{k_1} \ldots p_m^{k_m}$, где все простые числа p_i различны и относительно малы, то указанная процедура позволяет получить систему сравнений следующего вида:

$$\begin{cases} z \equiv v_1\ (mod\ p_1^{k_1}), \\ \ldots \\ z \equiv v_m\ (mod\ p_m^{k_m}), \end{cases}$$

Эту систему можно решить относительно z, используя китайскую теорему об остатках (см. § 12), и, следовательно, найти вычет $z\ (mod\ q-1)$, удовлетворяющий уравнению (1). □

О вычислении дискретных логарифмов см. также [**30**, глава 6].

§ 62. Степенной алгоритм

Для вычисления $y = b^z$, где z – неотрицательное целое число, полезно использовать следующий алгоритм (где операции над y и b осуществляются в поле $\mathbb{F}_q$, $z\ div\ 2 = \left[\frac{z}{2}\right]$ – частное от деления z на 2):

```
y := 1;
while z > 0 do {
    if z нечетно then y := y · b;
    b := b · b;
    z := z div 2
}.
```

Алгоритм основан на использовании следующего соотношения:

$$y = \begin{cases} (b^2)^{\left[\frac{z}{2}\right]}, \text{если } z - \text{четное число;} \\ (b^2)^{\left[\frac{z}{2}\right]} \cdot b, \text{если } z - \text{нечетное число,} \end{cases}$$

и затрачивает $O(log_2 z)$ времени (по числу арифметических операций).

§ 63. Корни многочленов степени $n \leqslant 4$ над конечным полем характеристики 2

Этот раздел посвящен вычислению корней многочленов $f(x) \in \mathbb{F}_{2^m}[x]$ степеней $n = 2,3,4$. Искомые корни лежат в поле $\mathbb{F}_{2^m}$. Другие корни могут лежать в расширениях поля $\mathbb{F}_{2^m}$. При необходимости их следует искать, переходя к соответствующему расширению основного поля $\mathbb{F}_{2^m}$. Если порядок поля $\mathbb{F}_{2^m}$ является относительно небольшим, то при вычислении корней, лежащих в поле $\mathbb{F}_{2^m}$, можно ограничиться вычислением корней многочлена $g(x) = \text{НОД}\,(x^{2^m} - x, f(x))$. Это позволит избавиться от "лишних" кратных корней и, возможно, понизить степень исследуемого многочлена. Вычисление $g(x)$ можно реализовать по следующей схеме (где символ $\oplus$ означает сложение многочленов в кольце $\mathbb{F}_{2^m}[x]$):

$y(x) \coloneqq x;$

$\boldsymbol{for}\ i \coloneqq 1\ \boldsymbol{to}\ m\ \boldsymbol{do}\ y(x) \coloneqq y(x)^2\ mod\ f(x);$

$g(x) \coloneqq y(x) \oplus x.$

Сделаем ещё одно замечание о корнях многочленов.

63.1. ***Теорема Орбит*** [**47**]. *Пусть*

$$\sigma(x) = y^n + \sigma_1 y^{n-1} + \sigma_2 y^{n-2} + \cdots + \sigma_n,$$
$$\delta(x) = y^n + {\sigma_1}^2 y^{n-1} + {\sigma_2}^2 y^{n-2} + \cdots + {\sigma_n}^2$$

− многочлены с коэффициентами из поля $\mathbb{F}_{2^m}$. Элемент β, лежащий в поле $\mathbb{F}_{2^m}$ или в любом его расширении $\mathbb{F}_{2^{km}}$, тогда и только тогда является корнем $\sigma(x)$, когда β^2 есть корень $\delta(x)$.

Доказательство. *Пусть* $\sigma(\beta) = 0$. Тогда

$$\delta(\beta^2) = \beta^{2n} + {\sigma_1}^2 \beta^{2(n-1)} + {\sigma_2}^2 \beta^{2(n-2)} + \cdots + {\sigma_n}^2 = \sigma(\beta)^2 = 0.$$

Обратно, пусть $\delta(\gamma) = 0$. В поле характеристики 2 любой элемент γ является квадратом некоторого элемента β, так что $\gamma = \beta^2$. Если

$\gamma \in \mathbb{F}_{2^{km}}$, то $\beta = \sqrt{\gamma} = \gamma^{2^{km-2}}$. Так как $\delta(\beta^2) = \sigma(\beta)^2$ и $\beta = \sqrt{\gamma}$, то $\delta(\gamma) = 0 \Longrightarrow \sigma(\sqrt{\gamma}) = 0$. □

63.2. ***Следствие.*** *Число корней у многочленов $\sigma(x)$ и $\delta(x)$ в поле $\mathbb{F}_{2^m}$ одинаково.*

Определим многочлены

$$\sigma^{(i)}(x) = x^n + {\sigma_1}^{2^i} x^{n-1} + {\sigma_2}^{2^i} x^{n-2} + \cdots + {\sigma_n}^{2^i},\ i = 0, 1. \ldots$$

Отметим, что $\sigma(x) = \sigma^{(0)}(x)$, $\delta(x) = \sigma^{(1)}(x)$, $\sigma^{(m)}(x) = \sigma^{(0)}(x)$ ввиду $y^{2^m} = y$ для любого $y \in \mathbb{F}_{2^m}$. Если $\beta_1, \beta_2, \ldots, \beta_s -$ корни $\sigma(x)$, то ${\beta_1}^{2^i}$, ${\beta_2}^{2^i}$,…, ${\beta_s}^{2^i} -$ корни $\sigma^{(i)}(x)$. Если β и $\beta^{2^i} -$ корни $\sigma(x)$, то β^{2^i} – общий корень $\sigma(x)$ и $\sigma^{(i)}(x)$ и, следовательно, является корнем $\theta^{(i)}(x) =$ НОД ($\sigma(x)$, $\sigma^{(i)}(x)$). Многочлен $\theta^{(i)}(x)$ полезно использовать для вычисления корней многочлена $\sigma(x)$, когда $0 < deg\, \theta^{(i)}(x) < deg\, \sigma(x)$.

63.1. Квадратные многочлены

Рассмотрим уравнение

$$x^2 + ax + b = 0,\ a, b \in \mathbb{F}_{2^m}. \qquad (1)$$

Для вычисления корней уравнения (1) школьная формула

$$x_{1,2} = \frac{-a \pm \sqrt{a^2 - 4b}}{2}$$

не годится, так как в поле характеристики 2 деление на 2 равносильно делению на 0. Если $a = 0$, то уравнение (1) имеет единственный корень $x = b^{2^{m-1}}$ кратности 2. При $a \neq 0$ уравнение (1) заменой $x = ay$ приводится к виду

$$y^2 + y + \beta = 0,\ \beta = \frac{b}{a^2} \in \mathbb{F}_{2^m}. \qquad (2)$$

63.3. ***Теорема*** [**42**; **26**, с. 273, теорема 15]. *Оба корня уравнения* (2) *лежат в $\mathbb{F}_{2^m}$ тогда и только тогда, когда*

$$Tr_m(\beta) = \beta + \beta^2 + \cdots + \beta^{2^{m-1}} = 0;$$

если же $Tr_m(\beta) = 1$, то оба корня лежат в $\mathbb{F}_{2^{2m}} \backslash \mathbb{F}_{2^m}$.

Доказательство. Запишем представления элементов x, x^2 и $\beta \in \mathbb{F}_{2^m}$ в нормальном базисе $\{\gamma, \gamma^2, \ldots, \gamma^{2^{m-1}}\}$ поля $\mathbb{F}_{2^m}$ над полем $\mathbb{F}_2$:

$$x = x_0\gamma + x_1\gamma^2 + \cdots + x_{m-1}\gamma^{2^{m-1}}; \quad (3)$$
$$x^2 = x_{m-1}\gamma + x_0\gamma^2 + \cdots + x_{m-2}\gamma^{2^{m-1}},$$
$$\beta = \beta_0\gamma + \beta_1\gamma^2 + \cdots + \beta_{m-1}\gamma^{2^{m-1}},$$

где $x_0, x_1, \ldots, x_{m-1}; \beta_0, \beta_1, \ldots, \beta_{m-1} \in \mathbb{F}_2$.

Подставим в (2) $y = x$, где x представлено в виде (3). Если x – решение уравнения (2), то приравнивая коэффициенты в полученном выражении при γ^{2^i}, $i = 0, 1, \ldots, m-1$, нулю, получим

$$\begin{aligned} &x_0 + x_{m-1} + \beta_0 = 0 \\ &x_1 + x_0 + \beta_1 = 0 \\ &\ldots \\ &x_{m-1} + x_{m-2} + \beta_{m-1} = 0. \end{aligned} \quad (4)$$

Заметим, что $\gamma^{2^m} = \gamma$ и

$$Tr_m(\beta) = \sum_{i=0}^{m-1} \left(\beta_0\gamma + \beta_1\gamma^2 + \cdots + \beta_{m-1}\gamma^{2^{m-1}}\right)^{2^i}$$
$$= \sum_{i=0}^{m-1} (\beta_0 + \beta_1 + \cdots + \beta_{m-1})\gamma^{2^i}.$$

Складывая равенства (4), получаем

$$0 = \sum_{i=0}^{m-1} \beta_i = Tr_m(\beta).$$

Следовательно, равенство $Tr_m(\beta) = 0$ является необходимым условием, чтобы корень уравнения (2) лежал в $\mathbb{F}_{2^m}$. Это условие является также и достаточным, поскольку тогда решениями уравнения (2) являются y_0 и y_1, значения которых определены ниже формулой (5). □

В [**46**] приведено несколько формул для корней уравнения (2) соответствующих разным значениям β и m. Однако результат может быть сформулирован проще:

63.4. ***Теорема*** [**18**]. *Если $Tr_m(\beta) = 0$, то корни уравнения* (2) *могут быть вычислены по формуле:*

$$y_k = k + \sum_{i=1}^{m-1} \beta^{2^i} \sum_{j=0}^{i-1} u^{2^j}, k \in \mathbb{F}_2, \quad (5)$$

где $u \in \mathbb{F}_{2^m}$ *– любой элемент, для которого* $Tr_m(u) = 1$ (ввиду известных свойств функции Tr_m такой элемент u существует).

Доказательство. В справедливости формулы (5) можно убедиться непосредственно – подстановкой $y = y_k$:

$$y_k^2 + y_k + \beta =$$
$$= k^2 + k + \beta^2 u + \beta^4(u + u^2) + \cdots + \beta^{2^{m-1}}\left(u + u^2 + \cdots + u^{2^{m-2}}\right)$$
$$+ \beta^4 u^2 + \beta^8(u^2 + u^4) + \cdots \beta^{2^m}\left(u^2 + \cdots + u^{2^{m-2}} + u^{2^{m-1}}\right) + \beta =$$
$$= \beta Tr_m(u) + \beta u + u Tr_m(\beta) + \beta u + \beta = 0. \ \square$$

63.2. Кубические многочлены

Рассмотрим уравнение

$$f(x) = x^3 + ax^2 + bx + c = 0, \ f(x) \in \mathbb{F}_{2^m}[x]. \qquad (6)$$

Пусть $a^2 = b$. Тогда $f(x) = (x + a)^3 + a^3 + c = 0$ и $x = \sqrt[3]{a^3 + c} + a$.

Пусть $a^2 \neq b$. Тогда уравнение (6) подстановкой $x = a + y\sqrt{a^2 + b}$ приводится к виду

$$a^3 + y^3\sqrt{(a^2 + b)^3} + a^2 y\sqrt{a^2 + c} + a^3 + ay^2(a^2 + b) + ab +$$
$$by\sqrt{a^2 + b} + c$$
$$= y^3\sqrt{(a^2 + b)^3} + y\sqrt{(a^2 + b)^3} + \ ab + c$$
$$= \sqrt{(a^2 + b)^3}(y^3 + y + k), \qquad (7)$$

где

$$k = \frac{ab + c}{\sqrt{(a^2 + b)^3}}.$$

Уравнение (7) подстановкой $y = w + \frac{1}{w}$ приводится к виду

$$w^3 + \frac{1}{w^3} + w + \frac{1}{w} + w + \frac{1}{w} + k = w^3 + \frac{1}{w^3} + k = 0,$$

или

$$w^6 + kw^3 + 1 = 0.$$

Полагая $z = w^3$, получим $z^2 + kz + 1 = 0$. Квадратное уравнение решаем, используя результаты предыдущего раздела. Далее находим $w = \sqrt[3]{z}$, затем $y = w + \frac{1}{w}$ и

$$x = a + y\sqrt{a^2 + b} = a + y(a^2 + b)^{2^{m-1}} = a + y\left(a + b^{2^{m-1}}\right).$$

Замечание. Здесь возникает задача вычисления корня уравнения $z = w^3$ относительно w. Если $3 \nmid 2^m - 1$ (т.е. $2^m - 1$ не делится нацело на 3), то $w = z^n$, где $n \in \mathbb{N}$ – мультипликативный обратный элемент к 3 по модулю $2^m - 1$. Если $z \neq 0$ и $3 \mid 2^m - 1$ (т.е. $2^m - 1$ кратно 3), то w – корень, который можно вычислить, решая задачу дискретного логарифмирования (см. § 61), либо как ненулевой корень линеаризованного многочлена $w^4 - zw$ (см. § 65).

Необходимыми условиями, чтобы все корни уравнения $y^3 + y + k = 0$ лежали в $\mathbb{F}_{2^m}$ являются [**58**]:

$$Tr_m\left(\frac{1}{k}\right) = Tr_m(1),$$

где, как и прежде, $Tr_m(\beta) = \beta + \beta^2 + \cdots + \beta^{2^{m-1}}$ – след элемента $\beta \in \mathbb{F}_{2^m}$ в $\mathbb{F}_2$.

Если m четно, то $Tr_m(1) = Tr_m\left(\frac{1}{k}\right) = 0$ и все корни многочлена $z^2 + kz + 1$ лежат в $\mathbb{F}_{2^m}$. С другой стороны, если m нечетно, то

$$Tr_m(1) = Tr_m\left(\frac{1}{k}\right) = 1,$$

и корни этого многочлена лежат в $\mathbb{F}_{2^{2m}}$. В этом случае, переходя к полю $\mathbb{F}_{2^{2m}}$, мы можем найти корни указанного многочлена.

63.4. ***Теорема*** [**42**, теорема 2]. *Кубическое уравнение*

$$x^3 + x + \beta = 0, \beta \in \mathbb{F}_{2^m}^*, \qquad (7)$$

имеет единственное решение $x \in \mathbb{F}_{2^m}$ тогда и только тогда, когда

$$Tr_m(1) \neq Tr_m\left(\frac{1}{\beta}\right).$$

63.5. ***Теорема*** [**42**, теорема 3]. *Все три корня кубического уравнения* (7) *лежат в $\mathbb{F}_{2^m}^*$ тогда и только тогда, когда $P_m(\beta) = 0$, где функция $P_m(x)$ определяется рекуррентно:*

$$P_1(x) = x,\ P_2(x) = x,\ P_k(x) = P_{k-1}(x) + x^{2^{k-3}} P_{k-2}(x).$$

63.6. ***Теорема*** [**63**]. *Пусть t_1, t_2 – корни многочлена $t^2 + bt + a^3 \in \mathbb{F}_{2^m}[t]$, причем $t_1, t_2 \in \mathbb{F}_{2^m}$, если $Tr_m\left(\frac{a^3}{b^2}\right) = 0$, $t_1, t_2 \in \mathbb{F}_{2^{2m}}$, если $Tr_m\left(\frac{a^3}{b^2}\right) = 1$. Тогда корни кубического уравнения $x^3 + ax + b = 0$, $a, b \in \mathbb{F}_{2^m}$, лежат*:

1) *все три корня в $\mathbb{F}_{2^m}$ тогда и только тогда, когда $Tr_m\left(\frac{a^3}{b^2}\right) = Tr_m(1)$ и t_1, t_2 – кубы в $\mathbb{F}_{2^m}$ при четном m, кубы в $\mathbb{F}_{2^{2m}}$ при нечетном m;*

2) *один корень в* $\mathbb{F}_{2^m}$*, два других в* $\mathbb{F}_{2^{2m}}$ *тогда и только тогда, когда* $Tr_m\left(\frac{a^3}{b^2}\right) \neq Tr_m(1)$;

3) *все три корня в* $\mathbb{F}_{2^{3m}} \backslash \mathbb{F}_{2^m}$ *тогда и только тогда, когда* $Tr_m\left(\frac{a^3}{b^2}\right) = Tr_m(1)$ *и* $t_1, t_2 -$ *некубы в* $\mathbb{F}_{2^m}$ *при четном* m*, и некубы в* $\mathbb{F}_{2^{2m}}$ *при нечетном* m.

63.3. Многочлены четвертой степени

Рассмотрим уравнение

$$f(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 = 0,\ f(x) \in \mathbb{F}_{2^m}[x]. \qquad (8)$$

Если $a_4 = 0$, то один из корней уравнения (8) равен нулю, а другие являются корнями кубического уравнения $x^3 + a_1x^2 + a_2x + a_3 = 0$, вычисление которых описано выше в разделе 63.2. Отметим также, что если $a_1 = a_2 = a_3 = 0$, то уравнение (8) имеет единственный корень $x = \sqrt[4]{a_4} = {a_4}^{2^{m-2}}$ кратности 4. Поэтому далее будем предполагать, что $a_4 \neq 0$ и среди элементов a_1,a_2,a_3 хотя бы один не равен нулю.

Пусть $a_1 \neq 0$. Подстановкой $x = \frac{1}{y} + \sqrt{\frac{a_3}{a_1}}$ уравнение (8) приводится к виду

$$\left(\frac{1}{y}\right)^4 + \left(\frac{a_3}{a_1}\right)^2 + a_1\left(\frac{1}{y^3} + \frac{1}{y^2}\sqrt{\frac{a_3}{a_1}} + \frac{1}{y}\left(\frac{a_3}{a_1}\right) + \sqrt{\left(\frac{a_3}{a_1}\right)^3}\right)$$
$$+ a_2\left(\frac{1}{y^2} + \frac{a_3}{a_1}\right) + a_3\left(\frac{1}{y} + \sqrt{\frac{a_3}{a_1}}\right) + a_4$$
$$= \frac{1}{y^4} + \frac{a_1}{y^3} + \frac{1}{y^2}\left(a_1\sqrt{\frac{a_3}{a_1}} + a_2\right) + \left(\frac{a_3}{a_1}\right)^2 + a_1\sqrt{\left(\frac{a_3}{a_1}\right)^3} + a_2\frac{a_3}{a_1}$$
$$+ a_3\sqrt{\frac{a_3}{a_1}} + a_4.$$

Так как $a_1\sqrt{\left(\frac{a_3}{a_1}\right)^3} + a_3\sqrt{\frac{a_3}{a_1}} = 0$, то уравнение (8) приводится к виду

$$\frac{1}{y^4}+\frac{a_1}{y^3}+\frac{A_2}{y^2}+A_0=\frac{1}{y^4}(A_0y^4+A_2y^2+a_1y+1)=0,$$

где

$$A_2=a_2+\sqrt{a_1a_3},\ A_0=\left(\frac{a_3}{a_1}\right)^2+\frac{a_2a_3}{a_1}+a_4.$$

Корни уравнения $A_0y^4+A_2y^2+a_1y+1=0$ могут быть вычислены методами § 65, а если $A_2=0$, то с использованием формул § 66.

Пусть $A_2\neq 0$. Полагая $=z\sqrt{\frac{A_2}{A_0}}$, получаем

$$z^4+z^2+k_1z+k_2=0,\ k_1=a_1\sqrt{\frac{A_0}{A_2^3}},k_2=\frac{A_0}{A_2^2}. \qquad (9)$$

Уравнение (9) можно представить в виде

$$z^4+z^2+k_1z+k_2=(z^2+Az+B)(z^2+Az+C)=0.$$

Тогда

$$A^2+B+C=1,$$
$$A(B+C)=k_1,$$
$$B\cdot C=k_2,$$

откуда следует, что

$$A^3+A+k_1=0, \qquad (10)$$
$$B^2+(1+A^2)B+k_2=0. \qquad (11)$$

Это даёт следующую процедуру вычисления корней уравнения (8):

(1) решаем кубическое уравнение (10) относительно A;

(2) решаем квадратное уравнение (11) относительно B;

(3) полагаем $C=\frac{k_2}{B}$;

(4) решаем уравнения $z^2+Az+B=0$ и $z^2+Az+C=0$ относительно z;

(5) полагаем $y=z\sqrt{\frac{A_2}{A_0}}$;

(6) находим искомый корень (корни)

$$x=\frac{1}{y}+\sqrt{\frac{a_3}{a_1}}=\frac{1}{y}+(a_3{a_1}^{-1})^{2^{m-1}}={y}^{2^m-2}+{a_3}^{2^{m-1}}{a_1}^{2^{m-1}-1}.$$

Чтобы завершить исследование, остается рассмотреть случай $a_1=0$. Аналогично предыдущему случаю имеем

$$x^4+a_2x^2+a_3x+a_4=(z^2+Az+B)(z^2+Az+C)=0.$$

Значения A, B, C удовлетворяют соотношениям:

$$A^2+B+C=a_2,$$

$A(B + C) = a_3$,
$B \cdot C = a_4$,
из которых следует, что $A^3 + a_2 A = a_3$, $C^2 + C(A^2 + a_2) = a_4$, $B = \frac{a_4}{C}$. Дальнейшие действия аналогичны предыдущему случаю, где $a_1 \neq 0$: последовательно вычисляем значения A, B, C и находим искомые корни уравнения (8), решая соответствующие квадратные уравнения.

63.4. $GF(2^{16})$ как квадратичное расширение $GF(2^8)$

Элементами поля $\mathbb{F}_{2^{16}}$ являются пары (a_1,a_0) элементов $a_1,a_0 \in \mathbb{F}_{2^8}$. Компоненты a_1, a_0 такой пары интерпретируются как коэффициенты многочлена $a_1 x + a_0$. При этом пары $(0, a_0)$ являются элементами поля $\mathbb{F}_{2^8}$. Операция сложения в $\mathbb{F}_{2^{16}}$ выполняется по правилу: $(a_1, a_0) + (b_1, b_0) = (a_1 \oplus b_1,\ a_0 \oplus b_0)$, где $\oplus$ – сложение в поле $\mathbb{F}_{2^8}$. Поле $\mathbb{F}_{2^{16}}$ рассматривается как фактор-кольцо $\mathbb{F}_{2^8}[x]/(f(x))$ кольца $\mathbb{F}_{2^8}[x]$ по модулю идеала, порожденному неприводимым многочленом $f(x) = x^2 + f_1 x + f_0 \in \mathbb{F}_{2^8}[x]$ второй степени. Поэтому, построим многочлен $f(x)$: путем перебора $f_1, f_0 \in \mathbb{F}_{2^8}$, где $f_1 \cdot f_0 \neq 0$, находим те значения, для которых уравнение $x^2 + f_1 x + f_0 = 0$ не имеет решений в $\mathbb{F}_{2^8}$ (см. теорему 63.3). Тогда

$$(a_1 x + a_0) \cdot (b_1 x + b_0) = a_1 b_1 x^2 + (a_1 b_0 + a_0 b_1)x + a_0 b_0$$

$$\equiv (a_1 b_0 + a_0 b_1 + a_1 b_1 f_1)x + a_0 b_0 + a_1 b_1 f_0 \ mod\ f(x).$$

Так что $(a_1, a_0) \odot (b_1, b_0) = (a_1 b_0 + a_0 b_1 + a_1 b_1 f_1,\ a_0 b_0 + a_1 b_1 f_0)$.

Многочлен $f(x)$ является неприводимым многочленом в $\mathbb{F}_{2^8}[x]$. Возможно, он является также и примитивным, т.е. $\alpha = (1, 0)$ – его корень. Если это не так, то построим неприводимый многочлен $g(x)$ с таким свойством. Ненулевой элемент $\beta = (a_1, a_0) \in \mathbb{F}_{2^{16}}$ является примитивным элементом поля $\mathbb{F}_{2^{16}}$, т.е. порождающим элементом циклической группы $\mathbb{F}^*_{2^{16}} = <\beta> = \mathbb{F}_{2^{16}} \setminus \{0\} = \{\beta^0,\ \beta^1, \dots,\ \beta^{2^{16}-2}\}$, тогда и только тогда, когда

$$\beta^{2^{16}-1/p} \neq (0, 1) \text{ для } p = 3, 5, 17, 257, \qquad (12)$$

где числа $p = 3, 5, 17, 257$ являются простыми делителями числа $2^{16} - 1 = 65535$. Таким образом, для нахождения искомого элемента β необходимо реализовать перебор пар $\beta = (a_1,a_0) \in \mathbb{F}_{2^{16}}$,

$a_1 \neq 0$, с проверкой на выполнимость (12). Корнями многочлена $g(x)$ будут β и β^{2^8}, так что $g(x) = (x + \beta)\left(x + \beta^{2^8}\right) = x^2 + \left(\beta + \beta^{2^8}\right)x + \beta^{2^8+1} = x^2 + g_1 x + g_0$, где $\beta + \beta^{2^8} = (0, g_1)$, $\beta^{2^8+1} = (0, g_0)$, $g_1, g_0 \in \mathbb{F}_{2^8}$.

Рассмотренный подход может быть распространен на построение квадратичного расширения любого конечного поля $\mathbb{F}_q$ при условии, что временна́я сложность используемого перебора приемлема.

§ 64. Кубические уравнения в конечных полях $GF(3^m)$ характеристики 3

Рассмотрим общее кубическое уравнение с коэффициентами из конечного поля $\mathbb{F}_{3^m}$:

$$x^3 - \sigma_1 x^2 + \sigma_2 x - \sigma_3 = 0, \sigma_1, \sigma_2, \sigma_3 \in \mathbb{F}_{3^m}. \quad (1)$$

Это уравнение может быть приведено к виду

$$x^3 - x^2 = 0 \quad (2)$$

или к виду

$$x^3 - ax + b = 0;\ a, b \in \mathbb{F}_{3^m}. \quad (3)$$

Действительно, если $\sigma_1 \neq 0$, то заменой $x = \sigma_1 y - \sigma_2/\sigma_1$ уравнение (1) приводится к виду

$$y^3 - y^2 + \sigma = 0;\ \sigma = \frac{\sigma_1^2\sigma_2^2 - \sigma_2^3 - \sigma_1^3\sigma_3}{\sigma_1^6},$$

которое в свою очередь, при $\sigma \neq 0$ заменой $y = 1/z$ приводится к виду (3).

Корнями уравнения (2) являются 0 (кратности 2) и 1. При $a = 0$ уравнение (3) имеет единственный корень (кратности 3), равный $(-b^{3^{m-1}})$. Однако явные формулы можно указать и для корней уравнения (3) с $a \neq 0$.

Замечание. Уместно отметить, что в случае поля характеристики 3 для решения кубических уравнений известные формулы Кардано [**22**, § 64] непригодны (в них есть деление на 3, что для поля характеристики 3 равносильно делению на 0). Для нахождения корней уравнения (3) обычно рекомендуют методы, в которых эта задача сводится к решению системы линейных уравнений [**20**; **4**, гл. 11; **24**, гл. 3, § 4].

Пусть ζ – примитивный элемент поля $\mathbb{F}_{3^m}$. Если $a = \zeta^{2n}$ (т.е. a – квадрат в $\mathbb{F}_{3^m}$), то уравнение (3) заменой $x = \zeta^n y$ приводится к виду

$$y^3 - y + \beta = 0;\ \beta = \frac{b}{\zeta^{3n}} = \frac{b}{\sqrt{a^3}} \in \mathbb{F}_{3^m}. \qquad (4)$$

Аналогично, если $a = \zeta^{2n+1}$ (т.е. a – неквадрат в $\mathbb{F}_{3^m}$), то уравнение (3) приводится к виду

$$y^3 - \zeta y + \beta = 0, \beta = \frac{b}{\zeta^{3n}} \qquad (5)$$

(та же замена). Отметим следующие известные факты об уравнениях (4) и (5) [**2**, §§ 13, 14; **63**, теорема 2]. Пусть

$$T_s(\beta) = \beta^{3^0} + \beta^{3^1} + \cdots + \beta^{3^{s-1}}$$

– след элемента $\beta \in \mathbb{F}_{3^s}$ в поле $\mathbb{F}_3$. Тогда, если $T_m(\beta) = 0$, то корни уравнения (4) лежат в $\mathbb{F}_{3^m}$; если $T_m(\beta) \neq 0$, то корни этого уравнения лежат в $\mathbb{F}_{3^{3m}} \setminus \mathbb{F}_{3^m}$. Один корень уравнения (5) лежит в $\mathbb{F}_{3^m}$, а два других – в $\mathbb{F}_{3^{2m}} \setminus \mathbb{F}_{3^m}$.

Если корни уравнения (4) лежат в $\mathbb{F}_{3^{dm}}$ (здесь $d = 1$ или 3), то они могут быть вычислены по формуле

$$\xi_k = k + \sum_{i=1}^{dm-1} \beta^{3^i} \sum_{j=0}^{i-1} u^{3^j}, \qquad k \in \mathbb{F}_3, \qquad (6)$$

где u – любой элемент поля $\mathbb{F}_{3^{dm}}$, для которого $T_{dm}(u) = 2$ (ввиду известных свойств функции T такой элемент заведомо найдётся). Если m не кратно 3 и $d = 1$, то формула (6) может быть упрощена:

$$\xi_k = k - m \sum_{i=1}^{m-1} i\beta^{3^i}, k \in \mathbb{F}_3.$$

Корни уравнения (5) могут быть вычислены по формуле

$$\lambda_k = k\sqrt{\zeta} - \sum_{i=0}^{m-1} \zeta^{-\left(\frac{3^{i+1}-1}{2}\right)} \beta^{3^i}, k \in \mathbb{F}_3. \qquad (7)$$

Корень c, лежащий в $\mathbb{F}_{3^m}$, получается при $k = 0$. Два других корня лежат в $\mathbb{F}_{3^{2m}} \setminus \mathbb{F}_{3^m}$. Элементы a, b, ζ и β можно рассматривать как элементы поля $\mathbb{F}_{3^{2m}}$. Пусть α – примитивный элемент поля $\mathbb{F}_{3^{2m}}$. Тогда $\zeta = \alpha^{3^m+1}$ – примитивный элемент поля $\mathbb{F}_{3^m}$, $\sqrt{\zeta} = \alpha^{\frac{3^m+1}{2}}$, a – квадрат в поле $\mathbb{F}_{3^{2m}}$, $\beta = b\sqrt{\frac{\zeta^3}{a^3}}$. Так что для вычисления корней

уравнения (5) по формуле (7) требуется уметь извлекать квадратные корни из элементов поля $\mathbb{F}_{3^m}$ [**43**].

В справедливости формул (6) и (7) нетрудно убедиться непосредственно – подстановкой $y = \xi_k$ и $y = \lambda_k$ соответственно в (4) и (5).

Замечание. Для вычисления корней уравнения (5) достаточно вычислить корень $c \in \mathbb{F}_{3^m}$. Два других корня равны $c + \delta_1$, $c + \delta_2$, где δ_1, δ_2 – ненулевые корни уравнения $y^3 - \zeta y = 0$, а именно: $\delta_1 = \sqrt{\zeta} = \alpha^{\frac{3^m+1}{2}}$, $\delta_2 = 2\sqrt{\zeta}$. Аналогично, корнями уравнения (4) являются: c, $c + 1$, $c + 2$, где c – любой из корней уравнения (4), получаемый по формуле (6). □

§ 65. Вычисление корней линеаризованных и аффинных многочленов

Определение. Многочлен $L(x) \in \mathbb{F}_{q^m}[x]$ называется *линеаризованным*, если

$$L(x) = \delta_{m-1}x^{q^{m-1}} + \delta_{m-2}x^{q^{m-2}} + \cdots + \delta_1 x^{q^1} + \delta_0 x.$$

Пусть $\alpha^0, \alpha^1, \ldots, \alpha^{m-1}$ – степенной базис поля $\mathbb{F}_{q^m}$ над полем $\mathbb{F}_q$. Тогда

$$L(\alpha^i) = \sum_{i=0}^{m-1} \delta_i \alpha^{q^i} = \sum_{i=0}^{m-1} L_{ij}\alpha^j,\ L_{ij} \in \mathbb{F}_q.$$

Пусть $\beta = \beta_0\alpha^0 + \beta_1\alpha^1 + \cdots + \beta_{m-1}\alpha^{m-1}$; $\beta \in \mathbb{F}_{q^m}$; $\beta_0, \ldots, \beta_{m-1} \in \mathbb{F}_q$;

$L(\beta) = \gamma = \gamma_0\alpha^0 + \gamma_1\alpha^1 + \cdots + \gamma_{m-1}\alpha^{m-1}$; $\gamma_0, \ldots, \gamma_{m-1} \in \mathbb{F}_q$.

Тогда

$$L(\beta) = \beta_0 L(\alpha^0) + \beta_1 L(\alpha^1) + \cdots + \beta_{m-1}L(\alpha^{m-1})$$
$$= \sum_{i=0}^{m-1} \beta_i \sum_{i=0}^{m-1} L_{ij}\alpha^j = \gamma_0\alpha^0 + \gamma_1\alpha^1 + \cdots + \gamma_{m-1}\alpha^{m-1}.$$

Отсюда следует, что

$$\gamma_j = L_{0j}\beta_0 + L_{1j}\beta_1 + \cdots + L_{m-1j}\beta_{m-1},\ j = 0, 1, \ldots, m-1,$$

или, в матричной записи,

$$\mathcal{L}\begin{pmatrix}\beta_0\\ \beta_1\\ \cdots\\ \beta_{m-1}\end{pmatrix}=\begin{pmatrix}\gamma_0\\ \gamma_1\\ \cdots\\ \gamma_{m-1}\end{pmatrix},$$

где $\mathcal{L}-$ матрица размера $(m\times m)$ следующего вида:

$$\mathcal{L}=\begin{pmatrix}L_{00} & L_{10} & \ldots & L_{m-1,0}\\ L_{01} & L_{11} & & L_{m-1,1}\\ \cdots & & & \cdots\\ L_{0,m-1} & L_{1,m-1} & \cdots & L_{m-1,0}\end{pmatrix}.$$

Если $\beta-$ корень многочлена $L(x)$, то $\left(\gamma_0,\ldots,\gamma_{m-1}\right)=(0,\ldots,0)$.

Пример [**4**]. Рассмотрим многочлен

$$L(x)=x^4+\alpha^7x^2+\alpha^{18}x \qquad (1)$$

над $\mathbb{F}_{2^5}=\mathbb{F}_2(\alpha)$, где $\alpha-$ корень неприводимого примитивного многочлена x^5+x^2+1. Используя таблицу дискретных логарифмов и антилогарифмов поля $\mathbb{F}_{2^5}$, получаем

$L(1)=1+\alpha^7+\alpha^{18}=\alpha+\alpha^2+\alpha^4,$
$L(\alpha)=\alpha^4+\alpha^9+\alpha^{12}=\alpha^2+\alpha^3,$
$L(\alpha^2)=\alpha^8+\alpha^{11}+\alpha^{20}=\alpha+\alpha^2,$
$L(\alpha^3)=\alpha^{12}+\alpha^{13}+\alpha^{21}=\alpha+\alpha^3,$
$L(\alpha^4)=\alpha^{16}+\alpha^{15}+\alpha^{22}=1+\alpha^4,$

а матрица $\mathcal{L}$ имеет вид:

$$\mathcal{L}=\begin{pmatrix}0&0&0&0&1\\ 1&0&1&1&0\\ 1&1&1&0&0\\ 0&1&0&1&0\\ 1&0&0&0&1\end{pmatrix}.$$

Корни линеаризованного многочлена $L(x)$ можно найти, решая систему линейных уравнений

$$\begin{cases} L_{00}\beta_0+L_{10}\beta_1+\cdots+L_{m-1,0}\beta_{m-1}=0\\ L_{01}\beta_0+\beta_1\,L_{11}+\cdots+L_{m-1,1}\beta_{m-1}=0\\ \qquad\qquad\qquad\ldots\\ L_{0,m-1}\beta_0+L_{1m-1}\,\beta_1+\cdots+L_{m-1,m-1}\beta_{m-1}=0\end{cases}$$

относительно $\beta_0,\beta_1,\ldots,\beta_{m-1}\in\mathbb{F}_q$. В матричной записи эта система выглядит как $\mathcal{L}\,\boldsymbol{\beta}=\mathbf{0}$, где $\boldsymbol{\beta}-$ вектор-столбец с компонентами $\beta_0,\beta_1,\ldots,\beta_{m-1}$, $\mathbf{0}-$ нулевой столбец. В частности, корнями многочлена (1) в поле $\mathbb{F}_{2^5}$ являются 0 и α^{12}. Другие два корня лежат в $\mathbb{F}_{2^{10}}$.

Определение. Многочлен $A(x) \in \mathbb{F}_{q^m}[x]$ называется *аффинным*, если

$$A(x) = L(x) - \gamma,$$

где $L(x) -$ линеаризованный многочлен, $\gamma \in \mathbb{F}_{q^m}$.

Корни аффинного многочлена $A(x)$ можно найти, решая систему неоднородных линейных уравнений

$$\mathcal{L}\,\boldsymbol{\beta} = \boldsymbol{\gamma}, \qquad (2)$$

где $\boldsymbol{\gamma} -$ столбец с компонентами $\gamma_0, \gamma_1, \ldots, \gamma_{m-1} \in \mathbb{F}_q$, $\boldsymbol{\gamma} = \gamma_0\alpha^0 + \cdots + \gamma_{m-1}\alpha^{m-1}$.

Решения уравнения (2) можно найти, представляя $\boldsymbol{\beta}$ в нормальном базисе $\varepsilon, \varepsilon^q, \ldots, \varepsilon^{q^{m-1}}$ поля $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$, а именно:

$$\boldsymbol{\beta} = \beta_0\varepsilon + \beta_1\varepsilon^q + \cdots + \beta_{m-1}\varepsilon^{q^{m-1}}, \beta_0, \ldots, \beta_{m-1} \in \mathbb{F}_q.$$

Если $x = \boldsymbol{\beta} \in \mathbb{F}_{q^m}$ является корнем многочлена

$$A(x) = \delta_{m-1}x^{q^{m-1}} + \delta_{m-2}x^{q^{m-2}} + \cdots + \delta_1 x^{q^1} + \delta_0 x - \gamma,$$

то x является также корнем многочлена

$$A(x)^q = \delta_{m-2}^q x^{q^{m-1}} + \cdots + \delta_1^q x^{q^2} + \delta_0^q x^q + \delta_{m-1}^q x - \gamma^q \bmod x^{q^m} - x\,.$$

Другими словами, решение x удовлетворяет следующей системе уравнений:

$$\begin{cases} \delta_{m-1}x^{q^{m-1}} + \delta_{m-2}x^{q^{m-2}} + \cdots + \delta_1 x^{q^1} + \delta_0 x^{q^0} = \gamma \\ \delta_{m-2}^q x^{q^{m-1}} + \delta_{m-3}^q x^{q^{m-2}} + \cdots + \delta_0^q x^{q^1} + \delta_{m-1}^q x^{q^0} = \gamma^q \\ \cdots \\ \delta_0^{q^{m-1}} x^{q^{m-1}} + \delta_1^{q^{m-1}} x^{q^{m-2}} + \cdots + \delta_{m-2}^{q^{m-1}} x^{q^1} + \delta_{m-1}^{q^{m-1}} x^{q^0} = \gamma^{q^{m-1}} \end{cases}$$

Обозначая $x^{q^0}, x^{q^1}, \ldots, x^{q^{m-1}}$ соответственно через $y_0, y_1, \ldots, y_{m-1}$, получаем следующую систему неоднородных линейных уравнений:

$$\begin{pmatrix} \delta_0 & \delta_1 & \cdots & \delta_{m-1} \\ \delta_{m-1}^q & \delta_0^q & & \delta_{m-2}^q \\ \vdots & & \ddots & \vdots \\ \delta_1^{q^{m-1}} & \delta_2^{q^{m-1}} & \cdots & \delta_0^{q^{m-1}} \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{m-1} \end{pmatrix} = \begin{pmatrix} \gamma \\ \gamma^q \\ \vdots \\ \gamma^{q^{m-1}} \end{pmatrix}.$$

Среди найденных решений $\left(y_0, y_1, \ldots, y_{m-1}\right) \in \mathbb{F}_{q^m}^n = \mathbb{F}_{q^m} \times \ldots \times \mathbb{F}_{q^m}$ (декартово произведение m эземпляров поля $\mathbb{F}_{q^m}$) оставляем

только те, для которых $y_1 = y_0^q$, $y_2 = y_1^q$, …, $y_{m-1} = y_{m-2}^q$, и полагаем $x = y_0$ (это будут решения уравнения (2), лежащие в $\mathbb{F}_{q^m}$).

Наименьшее аффинное кратное. Над полем $\mathbb{F}_{q^m}$ аффинных многочленов мало. Однако, если умножить произвольный многочлен $f(x)$ на некоторый другой многочлен, можно получить аффинный многочлен. Например, если умножить кубический многочлен над полем характеристики 2 на соответствующий линейный множитель, то можно получить аффинный многочлен четвертой степени. Так что корни кубического многочлена можно легко выделить среди корней аффинного многочлена.

Опишем алгоритм вычисления аффинного многочлена, кратного $f(x)$ [**4**, алгоритм 11.21; **24**, гл.3, § 4, с. 145]**.**

$A1$. Пусть $deg\, f = n \geq 1 -$ степень многочлена $f(x)$. Вычислим многочлены $r_i(x)$, удовлетворяющие условию

$$x^{q^i} \equiv r_i(x) (\mathrm{mod}\, f(x), i = 0, 1, \ldots, n-1\,.$$

$A2$. Находим элементы $\alpha_i \in \mathbb{F}_{q^m}$, не все равные нулю, чтобы линейная комбинация

$$\sum_{i=0}^{n-1} \alpha_i r_i(x) = \sum_{j=0}^{n-1} \left(\sum_{i=0}^{n-1} \alpha_i r_{ji} \right) x^j$$

была постоянным многочленом. С этой целью приравниваем нулю $n-1$ коэффициентов при положительных степенях $x^j, 1 \leq j \leq n-1$, переменной x.

В результате получим систему из $n-1$ однородных линейных уравнений относительно n неизвестных $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$:

$\alpha_0 r_{10} + \alpha_1 r_{11} + \cdots + \alpha_{n-1} r_{1,n-1} = 0,$

$\alpha_0 r_{20} + \alpha_1 r_{21} + \cdots + \alpha_{n-1} r_{2,n-1} = 0,$

…

$\alpha_0 r_{n-1,0} + \alpha_1 r_{n-1,1} + \cdots + \alpha_{n-1} r_{n-1,n-1} = 0,$

или, в матричной записи,

$$\begin{pmatrix} r_{10} & r_{11} & \cdots & r_{1,n-1} \\ r_{20} & r_{21} & & r_{2,n-1} \\ \vdots & & \ddots & \vdots \\ r_{n-1,0} & r_{n-1,1} & \cdots & r_{n-1,n-1} \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Такая система всегда имеет нетривиальное решение. Фиксируя некоторое нетривиальное решение $\left(\alpha_0, \alpha_1, \dots, \alpha_{n-1}\right)$ этой системы уравнений, получаем, что

$$\sum_{i=0}^{n-1} \alpha_i r_i(x) = \alpha$$

для некоторого $\alpha \in \mathbb{F}_{q^m}$. Это означает, что

$$\sum_{i=0}^{n-1} \alpha_i x^{q^i} \equiv \sum_{i=0}^{n-1} \alpha_i r_i(x) \equiv \alpha \left(mod\ f(x)\right),$$

и

$$A(x) = \sum_{i=0}^{n-1} \alpha_i x^{q^i} - \alpha$$

есть ненулевой аффинный многочлен над $\mathbb{F}_{q^m}$, делящийся на $f(x)$. Многочлен $A(x)$ можно выбрать нормированным.

§ 66. Вычисление корней уравнения $x^{p^s}+ax+b=0,\ a,b \in \mathbb{F}_{p^t}$

Пусть $\mathbb{F}_q$ – конечное поле, содержащее q элементов (q – степень простого числа p); s и t – натуральные числа. Рассматривается уравнение

$$x^{p^s} + ax + b = 0,\ a, b \in \mathbb{F}_{p^t} \qquad (1)$$

и указаны явные формулы для его корней, лежащих в $\mathbb{F}_{p^t}$.

Отметим вкратце известные факты об уравнении (1) и сделаем некоторые замечания.

Многочлен в левой части уравнения (1) относится к так называемым *аффинным* (а при $b = 0$ и к *линеаризованным*) многочленам. Для нахождения корней таких многочленов обычно рекомендуют метод Берлекэмпа [**4**, гл. 11], в котором эта задача сводится к решению системы линейных уравнений.

При $a = 0$ уравнение (1) имеет единственный корень (кратности p^s), равный $-b^{p^r}$, где $r \geq 0$ – любое целое число такое, что $r + s \equiv 0\ (mod\ t)$. Поэтому всюду далее будем считать, что $a \neq 0$. Полагая $n = \frac{s}{d}$, $m = \frac{t}{d}$ и $q = p^d$, где $d = (s, t)$ – наибольший общий делитель s и t, уравнение (1) можно переписать следующим образом:

$$x^{q^n} + ax + b = 0;\ a, b \in \mathbb{F}_{q^m},\ a \neq 0,\ (n, m) = 1. \qquad (2)$$

Последнее уравнение исследовалось в [9], где показано. что оно может иметь 0, 1 или q корней, лежащих в $\mathbb{F}_{q^m}$; однако, какая из этих возможностей реализуется при тех или иных a и b, не установлено. Вопрос о разрешимости уравнения (2) рассмотрен в [**23**, с. 244, аддитивная форма теоремы Гильберта [44] 90; см. также **6**, гл.V, § 11.5], откуда можно извлечь также и формулы для корней этого уравнения.

К уравнениям типа (2) относятся рассмотренные в §§ 63−64 квадратное уравнение над $\mathbb{F}_{2^m}$ и приведённое кубическое уравнение над $\mathbb{F}_{3^m}$, а именно:

$$x^2 + ax + b = 0;\ a, b \in \mathbb{F}_{2^m} \qquad (3)$$

и

$$x^3 + ax + b = 0;\ a, b \in \mathbb{F}_{3^m}. \qquad (4)$$

Замечание. Напомним, что хорошо известная ″школьная″ формула для корней квадратного уравнения в случае поля характеристики 2 оказывается непригодной: в таком поле деление на 2 равносильно делению на 0. То же самое можно сказать и о кубическом уравнении над полем характеристики 3 (как, впрочем, и над полем характеристики 2) − формулы Кардано [45] здесь также непригодны. Для указанных полей это влечёт определённые трудности и при решении уравнений четвёртой степени. Заметим, что в поле характеристики $p \geq 5$ такие проблемы не возникают и для решения уравнений степени $n \leq 4$ можно использовать известные формулы для полей нулевой характеристики [**22**, § 64]. Некоторые результаты об уравнениях (3) и (4) получены в [**18**, **20**, **46**]. Исследуя более

---

[44] ***Давид Гильберт*** (23.01.1862 − 14.92.1943) − немецкий математик-универсал, внёс значительный вклад в развитие многих областей математики. Член многих академий наук, в том числе Берлинской, Лондонского королевского общества, иностранный почётный член Академии наук СССР (1934). Лауреат премии имени Н. И. Лобачевского (1903). В 1910−1920-е годы (после смерти Анри Пуанкаре) был признанным мировым лидером математиков.

[45] ***Джероламо Кардано*** (24.09.1501 − 21.09.1576) − итальянский математик, инженер, философ, врач и астролог. В его честь названы открытые Сципионом дель Ферро формулы решения кубического уравнения.

общее уравнение (2), мы приводим формулы, которые пригодны, конечно, и для решения указанных квадратного и кубического уравнений. В отличие от [46] (где, заметим, дано несколько формул для корней уравнения $x^2 + x + b = 0$; $b \in \mathbb{F}_{2^m}$, соответствующих различным значениям n и m) мы уже показали, что корни уравнений (3) и (4) могут быть вычислены по одной − единственной формуле, которая "работает" во всех случаях, когда эти уравнения имеют решения соответственно в $\mathbb{F}_{2^m}$ и $\mathbb{F}_{3^m}$.

Формулы для корней уравнения (2). Положим

$$A = a^{\frac{q^m-1}{q-1}} - (-1)^m,\ T(u) = \sum_{i=0}^{m-1} u^{q^i},\ S = \sum_{i=0}^{m-1} c_i b^{q^{in}},$$

где a, b, n, m, q те же, что и в уравнении (2); $c_0 = 1$, $c_i = -c_{i-1}a^{-q^{in}}$, $i = 1, 2, \ldots$ Величина S известна как резольвента Гильберта-Лагранжа.

Отметим следующее свойство функции $T(u)$, называемой обычно *следом* элемента $u \in \mathbb{F}_{q^m}$ относительно расширения $\mathbb{F}_{q^m} / \mathbb{F}_q$: для любого $z \in \mathbb{F}_q$ найдётся $u \in \mathbb{F}_{q^m}$ такой, что $Tr(u) = z$.

66.1. ***Лемма***. *Если $A = 0$, то в $\mathbb{F}_{q^m}$ найдётся элемент w такой, что $w^{q^n-1} = -a$.*

Доказательство. Все $a \in \mathbb{F}_{q^m}$, для которых $A = 0$, суть следующие элементы: $a_r = \zeta^{r(q-1)+f}$, $r = 0, 1, \ldots, \frac{q^m-1}{q-1} - 1$, где ζ – первообразный элемент мультипликативной группы поля $\mathbb{F}_{q^m}$, а $f = 0$ или $\frac{q-1}{2}$ соответственно случаям: 1) m или q чётно; 2) m и q оба нечётны. Если $a = a_r$, то искомый элемент w равен $\zeta^{(r+s)l}$, где l – любое число, для которого

$$l\frac{q^n-1}{q-1} \equiv 1 \left(mod\ \frac{q^m-1}{q-1}\right)$$

(ввиду НОД $(q^n - 1,\ q^m - 1) = q^{\text{НОД}\,(m,n)} - 1 = q - 1$ такое l существует);

$$s = 0,\ \frac{q^m-1}{2(q-1)},\ \left(1 + \frac{q^m-1}{q-1}\right)/2$$

соответственно случаям, когда 1) q чётно; 2) m чётно, а q нечётно; 3) m и q нечётны. □

66.2. ***Теорема***. *Учитывая только те из корней уравнения* (2), *которые лежат в* $\mathbb{F}_{q^m}$, *имеем:*

1) *если* $A = 0$, *но* $S \neq 0$, *то уравнение* (2) *не имеет корней*;

2) *если* $A \neq 0$, *то имеется единственный корень*

$$\xi^{(0)} = (-1)^m S \cdot (aA)^{-1}; \tag{5}$$

3) *наконец, если* $A = S = 0$, *то имеется* q *корней, а именно:*

$$\xi_k = wk - \frac{1}{a}\sum_{i=1}^{m-1} c_i b^{q^{in}} \sum_{j=0}^{i-1} u^{q^{jn}},\ k \in \mathbb{F}_q, \tag{6}$$

где w, u *– любые элементы поля* $\mathbb{F}_{q^m}$, *для которых*

$$w^{q^n-1} = -a, \qquad T(u) = -1. \tag{7}$$

Замечание. Существование элементов w и u, удовлетворяющих (7), обосновано выше. Для случая $A = 0$ имеем $c_i = (aw)^{1-q^{in}}$, $i = 0,1,2,\ldots$, и $S = wT\left(\frac{b}{aw}\right)$. Поэтому здесь $S = 0$ равносильно $T\left(\frac{b}{aw}\right) = 0$. Формула (6) переписывается тогда так:

$$\xi_k = w\left(k - \sum_{i=1}^{m-1}\left(\frac{b}{aw}\right)^{q^{in}} \sum_{j=0}^{i-1} u^{q^{jn}}\right), k \in \mathbb{F}_q. \quad \square$$

Доказательство. Пусть ξ – некоторый корень уравнения (2), лежащий в $\mathbb{F}_{q^m}$ (в предположении, что он существует). Тогда

$$0 \equiv \sum_{i=0}^{m-1} c_i\left(\xi^{q^n} + a\xi + b\right)^{q^{in}} =$$

$$= \sum_{i=1}^{m} c_i \xi^{q^n} + \sum_{i=0}^{m-1}\left(c_i a^{q^{in}} \xi^{q^{in}} + c_i b^{q^{in}}\right) =$$

$$= c_{m-1}\xi^{q^{mn}} + c_0 a\xi + S.$$

Учитывая, что $v^{q^{rm}} = v$ для любых $v \in \mathbb{F}_{q^m}$ и $r = 0, 1,\ldots$ и

$$c_{m-1} = (-1)^{m-1} a^{-q^n - q^{2n} - \ldots - q^{(m-1)n}}$$

$$= (-1)^{m-1} a^{-q^1 - q^2 - \ldots - q^{(m-1)}}$$

(последнее имеет место ввиду $(n, m) = 1$ и

$q^n + q^{2n} + \cdots + q^{(m-1)n} \equiv q^1 + q^2 + \cdots + q^{(m-1)}\ (mod\ q^m - 1)$), получаем

$$(-1)^{m-1} aA\xi + S \equiv 0. \tag{8}$$

Из тождества (8) вытекают утверждения 1) и 2) в формулировке теоремы. Убедиться в том, что $\xi^{(0)}$ – корень уравнения (2), когда $A \neq 0$, можно непосредственно – подстановкой $x = \xi^{(0)}$ в (2). Остаётся проверить, что в случае $A = S = 0$ любое из q значений ξ_k, определяемое согласно (6), является корнем уравнения (2):

$$\xi_k^{q^n} + a\xi_k + b =$$

$$= (wk)^{q^n} + awk - \sum_{i=1}^{m-1} \left(\frac{c_i}{a}\right)^{q^n} b^{q^{(i+1)n}} \sum_{j=0}^{i-1} u^{q^{(j+1)n}}$$

$$- \sum_{i=1}^{m-1} c_i b^{q^{in}} \sum_{j=0}^{i-1} u^{q^{jn}} + b =$$

$$= \sum_{i=2}^{m-1} c_i b^{q^{in}} \sum_{j=0}^{i-1} u^{q^{jn}} - \sum_{i=1}^{m-1} c_i b^{q^{in}} \sum_{j=0}^{i-1} u^{q^{jn}} + b =$$

$$= -u\left(\sum_{i=2}^{m-1} c_i b^{q^{in}} + c_1 b^{q^n}\right) + b\left(-u + \sum_{j=0}^{i-1} u^{q^{jn}}\right) + b =$$

$$= -uS + bT(u) + b = 0. \ \square$$

Некоторые приложения. 1) С уравнением (1) связаны и некоторые другие уравнения. Так, если ξ – один из корней уравнения

$$x^{p^s+1} + ax + b = 0, a, b \in \mathbb{F}_{p^t}, b \neq 0, \qquad (9)$$

то нетрудно показать, что остальные его корни суть $\xi + y_i^{-1}$, где $y_i,\ i = 1,\ldots,p^s$, – корни уравнения

$$y^{p^s} + \frac{\xi}{\xi^{p^s}+a} y + \frac{1}{\xi^{p^s}+a} = 0. \qquad (10)$$

Уравнение (10) есть уравнение типа (1), и мы можем вычислить его корни, применяя полученные формулы. Вопрос, однако, в том, как найти хотя бы один корень уравнения (9).) Покажем, как вычислить корни уравнения (9), лежащие в $\mathbb{F}_{2^m}$, на примере уравнения

$$x^{2^s+1} + ax + b = 0;\ a, b \in \mathbb{F}_{2^m}. \qquad (11)$$

Пусть $\xi \in \mathbb{F}_{2^m}$ – корень данного уравнения. Если $\xi^{2^s} + a \neq 0$, то $y \neq 0$, и для вычисления y используем уравнение (2). Если $\xi^{2^s} + a = 0$, то $\xi^{2^m} + a^{2^{m-s}} = 0$, и тогда $\xi = a^{2^{m-s}}$, или $a = \xi^{2^s}$. По-

скольку $\xi^{2^m} = \xi$ для любого $\xi \in \mathbb{F}_{2^m}$, и $\xi^{2^s+1} - \xi^{2^s}\xi + b = 0$. В этом случае уравнение (11) имеет вид

$$x^{2^s+1} + ax = 0$$

и, следовательно, $x = 0$ и $x = a^{2^{m-s}}$.

Корни уравнения (11) удобно представить в степенном или нормальном базисах над полем $\mathbb{F}_2$. Это позволит свести вычисление корней к решению системы нелинейных квадратичных уравнений над полем $\mathbb{F}_2$.

В качестве простого примера рассмотрим уравнение

$$x^9 + ax + b = 0;\ a, b \in \mathbb{F}_{2^4}. \qquad (12)$$

Поле $\mathbb{F}_{2^4}$ (см. таблицу ниже), рассматривается как факторкольцо кольцо $\mathbb{F}_2[x]$ по идеалу, порожденному примитивным многочленом $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$. Элементы поля могут быть представлены как в степенном базисе $\boldsymbol{\alpha} = (1, \alpha, \alpha^2, \alpha^3)$, так и в нормальном базисе $\boldsymbol{\beta} = (\beta, \beta^2, \beta^4, \beta^8)$, где $\beta = \alpha^3, \alpha$ – примитивный элемент поля $\mathbb{F}_{2^4}$**.** Любой элемент $c \in \mathbb{F}_{2^4}$ однозначно представим в виде

$$c = a_0 \cdot 1 + a_1 \cdot \alpha + a_2 \cdot \alpha^2 + a_3 \cdot \alpha^3 = b_0 \cdot \beta + b_1 \cdot \beta^2 + b_2 \cdot \beta^4 + b_3 \cdot \beta^8$$

для некоторых $a_i, b_i \in \mathbb{F}_2, i = 0, 1, 2, 3$. Переход от нормального базиса к степенному базису, и обратно, реализуется с помощью линейных преобразований $(b_0, b_1, b_2, b_3)\, A = (a_0, a_1, a_2, a_3)$ и $(a_0, a_1, a_2, a_3)A^{-1} = (b_0, b_1, b_2, b_3)$,

Таблица

Представление элементов поля $\mathbb{F}_{2^4}$ в степенном и нормальном базисах

в виде степени α	в виде многочлена	в виде вектора $a_3a_2a_1a_0$	в виде вектора $b_3b_2b_1b$	в виде степени α	в виде многочлена	в виде вектора a_3a_2a	в виде вектора $b_3b_2b_1b$
$\alpha^\infty = 0$	0	0000	0000	α^7	$\alpha^3 + \alpha + 1$	1011	0111
α^0	1	0001	1111	α^8	$\alpha^2 + 1$	0101	1100
α^1	α	0010	1001	α^9	$\alpha^3 + \alpha$	1010	1000
α^2	α^2	0100	0011	α^{10}	$\alpha^2 + \alpha + 1$	0111	0101
α^3	α^3	1000	0001	α^{11}	$\alpha^3 + \alpha^2 + \alpha$	1110	1110
α^4	$\alpha + 1$	0011	0110	α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$	1111	0100
α^5	$\alpha^2 + \alpha$	0110	1010	α^{13}	$\alpha^3 + \alpha^2 + 1$	1101	1101
α^6	$\alpha^3 + \alpha^2$	1100	0010	α^{14}	$\alpha^3 + 1$	1001	1011

где

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}, \; A^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}.$$

Пусть в уравнении (12) $a = \alpha, b = \alpha^{13}$. Тогда, записывая a, b, x в нормальном базисе, а именно: $a = \beta + \beta^8$, $b = \beta + \beta^4 + \beta^8$, $x = x_0\beta + x_1\beta^2 + x_2\beta^4 + x_3\beta^8$, получим следующую систему нелинейных квадратичных уравнений относительно $x_0, x_1, x_2, x_3 \in \mathbb{F}_2$:

$$x_0x_1 + x_1x_2 + x_1x_3 + x_1 + x_2x_3 + x_3 = 1,$$
$$x_0x_2 + x_0x_3 + x_0 + x_1x_2 + x_1 + x_2x_3 + x_3 = 0,$$
$$x_0x_1 + x_0x_3 + x_1x_3 + x_1 + x_2x_3 + x_2 + x_3 = 1,$$
$$x_0x_1 + x_0x_2 + x_0x_3 + x_1x_2 + x_1 + x_2 = 1.$$

Вычисляя редуцированный базис Грёбнера[46] при линейном упорядочении $x_0 > x_1 > x_2 > x_3$, получаем эквивалентную систему уравнений:

$x_0 + x_3 + 1 = 0,$

$x_1 + 1 = 0,$

$x_2x_3 + x_2 + x_3 + 1 = 0.$

Её решениями являются:

$x_0 = 1,\ x_1 = 1,\ x_2 = 1,\ x_3 = 0,$

$x_0 = 0,\ x_1 = 1,\ x_2 = 0,\ x_3 = 1,$

$x_0 = 0, x_1 = 1,\ x_2 = 1, x_3 = 1.$

Соответственно решениями уравнения (12) будут:

$\alpha^3 + \alpha^6 + \alpha^{12} = \alpha^7,$

$\alpha^6 + \alpha^9 = \alpha^5,$

$\alpha^6 + \alpha^{12} + \alpha^9 = \alpha^{14}.$

Если характеристика рассматриваемого поля равна 2 и НОД $(2^s - 1,\ 2^m - 1) = 1$ (что, заметим, выполняется для уравнения (12)), то можно использовать следующий способ вычисления корней уравнения (9). Осуществим замену $x = y^{2^s-1}$, затем умножим обе части полученного уравнения на y. В результате получим уравнение

$$y^{2^{2s}} + ay^{2^s} + by = 0. \qquad (13)$$

С учетом соотношения $y^{16} = y$ для $y \in \mathbb{F}_{2^4}$ уравнение (12) преобразуется к виду

$$y^4 + ay^8 + by = 0. \qquad (14)$$

Многочлены в (13) и (14) являются линеаризованными, вычисление их корней, как уже отмечалось, сводится к решению системы линейных уравнений. Возникающие ″лишние″ корни отбрасываются.

Полагаем $y = y_0\beta + y_1\beta^2 + y_2\beta^4 + y_3\beta^8$. Тогда уравнение (14) сводится к решению следующей системы уравнений относительно $y_0,\ y_1, y_2, y_3 \in \mathbb{F}_2$:

---

[46] Методы решения систем нелинейных алгебраических уравнений с использованием базисов Грёбнера здесь не рассматриваются. См., например, [**15**, гл. 2, § 8].

$\beta y_2 = 0,$
$\beta^8(y_0 + y_1 + y_3) = 0.$

Решениями этой системы будут

$(y_0, y_1, y_2, y_3) = (0, 0, 0, 0)$
$(y_0, y_1, y_2, y_3) = (0, 1, 0, 1)$
$(y_0, y_1, y_2, y_3) = (1, 0, 0, 1)$
$(y_0, y_1, y_2, y_3) = (1, 1, 0, 0)$

Соответственно решениями уравнения (12) являются:
$y = \alpha^5, y = \alpha^7, y = \alpha^{14},$
приобретенное решение $y = 0$ является лишним. Остальные шесть корней уравнения (12) лежат в некоторых расширениях поля $\mathbb{F}_{2^4}$. Они могут быть вычислены как корни уравнения (10).

2) Приведём ещё два следствия доказанной выше теоремы. Первое из них о разложении многочлена

$$g(x) \equiv x^4 + ax + b = 0;\ a, b \in \mathbb{F}_{2^m},\ a \neq 0, \qquad (15)$$

на неприводимые над $\mathbb{F}_{2^m}$ множители уточняет (применительно к многочлену (15)) результат из [**57**] о разложении многочленов над $\mathbb{F}_{2^m}$ четвёртой степени; второе обобщает одну из теорем Диксона [47] [**50**, § 21; **2**, § 14].

Будем говорить, что многочлен $g(x)$ имеет тип (1^4), если он разлагается в произведение линейных множителей над $\mathbb{F}_{2^m}$; многочлен $g(x)$ имеет тип $(1^2 2^1)$, если он разлагается в произведение двух линейных множителей над $\mathbb{F}_{2^m}$ и неприводимого над $\mathbb{F}_{2^m}$ квадратного многочлена и т.д. Элемент $a \in \mathbb{F}_{2^m}$ будем называть *кубом*, если $a = c^3$ для некоторого $c \in \mathbb{F}_{2^m}$, и *некубом* – в противном случае. Наконец, положим

$$T_0(\beta) = \sum_{i=0}^{m-1} \beta^{2^i} \text{ и } T_1(\beta) = \sum_{i=0}^{m-1} \beta^{2^{2i}},$$

причём T_1 определено лишь для чётного m.

---

[47] ***Леонард Юджин Диксон*** (22.01.1874 – 17.01.1954) – английский математик. Известен трудами в области общей алгебры, теории групп, теории чисел и истории математики.

66.3. ***Следствие.*** *Для многочлена* (15) *возможны следующие типы:*

а) (1^4); *б*) $(1^2 2^1)$; *в*) $(1^1 3^1)$; *г*) (2^2); *д*) (4^1).

Условия, при которых имеет место соответствующий тип, суть следующие:

а) m *чётно,* $a -$ *куб и* $T_1(\beta) = 0$*;*

б) m *нечётно и* $T_0(\beta) = 0$*;*

в) m *чётно,* $a -$ *некуб;*

г) m *чётно,* $a -$ *куб и* $T_1(\beta) \neq 0$*;*

д) m *нечётно и* $T_0(\beta) \neq 0$,

где $\beta = \frac{b}{aw}$, *а* w *– корень уравнения* $w^3 = a$.

Доказательство этого утверждения опускается: оно осуществляется разбором случаев и непосредственным применением доказанной выше теоремы. Отметим лишь, что в тех случаях, когда требуется вычислить w, этот элемент лежит в $\mathbb{F}_{2^m}$. □

66.4. ***Задача***. *Пусть* $b -$ *произвольный элемент поля* $\mathbb{F}_{q^m}$, *и* $a = \zeta^i$, *где* $\zeta -$ *первообразный элемент поля* $\mathbb{F}_{q^m}$. *Требуется установить, при каких значениях* a *и* b *многочлен*

$$g(x) \equiv x^q + ax + b \in \mathbb{F}_{q^m}[x]$$

есть произведение линейного многочлена и неприводимого над $\mathbb{F}_{q^m}$ *многочлена степени* $q - 1$.

Замечание. В [**2**] соответствующее утверждение получено для $a = -\zeta$ (т.е. $i = 1$, если q чётно и $q \neq 2^1$, и $i = \frac{q^m+1}{2}$, если q нечётно). В исходной работе [**50**] к тому же $m = 1$.

Указание. Здесь достаточно найти условия, при которых многочлен $g(x)$ имеет единственный корень в каждом из расширений $\mathbb{F}_{q^{km}}$, $k = 1, 2, \ldots, q-2$, поля $\mathbb{F}_{q^m}$, или, что равносильно ввиду доказанной теоремы,

$$\mathrm{A}_{k,q,m} = \zeta^{i\frac{q^{km}-1}{q-1}} - (-1)^{km} \neq 0 \text{ при любом } k = 1, 2, \ldots, q-2 \,. \qquad (16)$$

§ 67. Решение квадратных уравнений над конечным полем нечётной характеристики

Данный раздел посвящен решению квадратных уравнений вида

$$y^2 - by + c = 0, b, c \in \mathbb{F}_q, \qquad (1)$$

над конечным полем $\mathbb{F}_q$, $q = p^n$, $n \in \mathbb{N}$, $p -$ нечётное простое число. Рассматриваются пять основных способов решения квадратных уравнений:

1. Метод, восходящий к Лежандру;
2. Метод Поклингтона;
3. Метод Чиполлы;
4. Метод Чиполлы-Лемера;
5. Метод Тонелли-Шенкса.

Уравнение (1) заменой $y = x + \frac{b}{2}$ приводится к виду $x^2 = a$, где $a = \frac{b^2 - 4c}{4}$. Последнее уравнение имеет решение $x \in \mathbb{F}_q$ тогда и только тогда, когда $a^{(q-1)/2} = 1$. Если уравнение $x^2 = a$ имеет решение $x \in \mathbb{F}_q$, то элемент a называется *квадратом*, или *квадратичным вычетом* в $\mathbb{F}_q$, а само решение называется *квадратным корнем* из a. Если уравнение $x^2 = a$ не имеет решений $x \in \mathbb{F}_q$, то элемент a называется *неквадратом*, или *квадратичным невычетом* в $\mathbb{F}_q$. Для неквадратов имеем $a^{(q-1)/2} = -1$. Множество ненулевых квадратов образуют в $\mathbb{F}_q^*$ подгруппу порядка $\frac{q-1}{2}$. Уравнение (1) либо не имеет решений в $\mathbb{F}_q$, либо имеет в точности два решения, с учётом кратности корней.

Замечание . В кольце $\mathbb{Z}_n$, когда $n -$ составное число, квадратное уравнение может иметь больше решений. Например, уравнение $x^2 = 1\ (mod\ 8)$ имеет 4 решения: 1, 3, 5, 7.

Для нечетного простого числа p и целого числа a, не делящегося на p, определим *символ Лежандра* $\left(\frac{a}{p}\right)$, полагая $\left(\frac{a}{p}\right) = 1$ или -1 соответственно случаям, когда $a -$ квадрат и неквадрат в $\mathbb{F}_p$. Другими словами, $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$.

Свойства символа Лежандра отмечены в теореме 58.4.

Квадратные корни в $\mathbb{F}_q$**.** Пусть $\mathbb{F}_q -$ поле из $q = p^n$ элементов, p – нечетное простое число, $n \in \mathbb{N}$. Рассмотрим некоторые способы вычисления корней уравнений

$$x^2 = a,\ a \in \mathbb{F}_q, \qquad (2)$$

лежащих в $\mathbb{F}_q$.

Чтобы уравнение (1) имело корень, лежащий в $\mathbb{F}_q$, необходимо и достаточно, чтобы $a^{\frac{q-1}{2}} = 1$. Если $a^{\frac{q-1}{2}} \neq 1$, то корни уравнения (1) лежат в $\mathbb{F}_{q^2}$. Далее предполагаем, что $a^{\frac{q-1}{2}} = 1$.

67.1. ***Теорема***. *Если* $q \equiv 3\ (mod\ 4)$, a *– квадрат в* $\mathbb{F}_q$, *то уравнение* $x^2 = a$ *имеет следующие решения*: $x = \pm\, a^{k+1}$, *где* $k = \frac{q-3}{4}$.

Доказательство: $(a^{k+1})^2 = a^{2k+2} = a^{\frac{q-1}{2}} a = a$. □

67.2. ***Теорема***. *Пусть* $p = 8m + 5$ *– простое число,* a *– квадрат в* $\mathbb{F}_p$, $d = a^{\frac{p-1}{4}}$. *Тогда уравнение* (1) *имеет следующие решения:*

$$x = \begin{cases} \pm\, a^{\frac{p+3}{8}}, \text{если } d = 1, \\ \pm\, 2a(4a)^{\frac{p-5}{8}}, \text{ если } d = -1. \end{cases}$$

Доказательство. Если $d = 1$, то $(a^{\frac{p+3}{8}})^2 = a^{\frac{p+3}{4}} = a^{\frac{p-1}{4}} a = a$. Если $d = -1$, то

$$\left(2a(4a)^{\frac{p-5}{8}}\right)^2 = 4^{\frac{p-1}{4}} a^{\frac{p+3}{4}} = 2^{\frac{p-1}{2}} a^{\frac{p-1}{4}} a = \left(\frac{2}{p}\right)(-1)\, a = a. \square$$

Замечание. Утверждение теоремы 67.2 справедливо для произвольного поля $\mathbb{F}_q$ с $q = 8m + 5$ элементами, а не только для простого поля $\mathbb{F}_p$. Если q не является простым числом, то вместо числа 2 следует взять любой элемент, являющийся квадратичным невычетом в $\mathbb{F}_q$.

67.3. ***Теорема***. *Пусть* $q = 16m + 9$, т.е. $q = 9, 25, 41, 57,\ 73, \ldots$ *Тогда уравнение* (2) *имеет следующие решения:*

$$x = \begin{cases} \pm\, a^{m+1}, & \text{если } a^{4m+4} = a^2 \text{ и } a^{2m+2} = a; \\ \pm\, a^{m+1} b^{4m+2}, & \text{если } a^{4m+4} = a^2 \text{ и } a^{2m+2} = -a; \\ \pm\, a^{m+1} b^{2m+1}, & \text{если } a^{4m+4} = -a^2 \text{ и } a^{2m+2} b^{4m+2} = a; \\ \pm\, a^{m+1} b^{6m+3}, & \text{если } a^{4m+4} = -a^2 \text{ и } a^{2m+2} b^{4m+2} = -a, \end{cases}$$

где $b \in \mathbb{F}_q$ *– квадратичный невычет, т.е.* $b^{8m+4} = -1$.

Доказательство. Имеем $a^{8m+4} = 1 \Rightarrow a^{4m+2} = \pm 1 \Rightarrow a^{4m+4} = \pm a^2$. Если $a^{4m+4} = a^2$, то $a^{2m+2} = \pm a$. Если $a^{2m+2} = a$, то $x = \pm\, a^{m+1}$ – корни уравнения (1). Если $a^{2m+2} = -a$, то $a^{2m+2} b^{8m+4} = a$. В этом случае корнями уравнения (1) будут $x = \pm\, a^{m+1} b^{4m+2}$. Пусть теперь $a^{4m+4} = -a^2$. Тогда $a^{4m+4} b^{8m+4} = a^2 \Longrightarrow a^{2m+2} b^{4m+2} = \pm a$. Если $a^{2m+2} b^{4m+2} = a$, то

$x = \pm a^{m+1}b^{2m+1}$. Если $a^{2m+2}b^{4m+2} = -a$, то $a^{2m+2}b^{4m+2}b^{8m+4} = a \Rightarrow x = \pm a^{m+1}b^{6m+3}$. □

Перейдем к непосредственному рассмотрению методов решения квадратных уравнений над конечным полем нечетной характеристики:

67.1. Метод, восходящий к Лежандру

67.4. ***Теорема***. *Пусть* $a, b \in \mathbb{F}_q$, *причём* a *– квадрат в* $\mathbb{F}_q$, *т.е.* $a = v^2$ *для некоторого* $\mathbb{F}_q$, $b^2 - a$ *– неквадрат в* $\mathbb{F}_q$. *Обозначим через* $c + dx$ *многочлен, определяемый в кольце* $\mathbb{F}_q[x]$ *сравнением* $c + dx \equiv (b - x)^{\frac{q-1}{2}} \, mod \, x^2 - a$. *Тогда* $c = 0$, $(d^{-1})^2 = a$, *что позволяет вычислить значения квадратных корней из* a *как* $v = d^{-1}$ *и* $v = -d^{-1}$.

Доказательство. Пусть $f + gx$ – многочлен, определяемый как $f + gx \equiv (b - x)^{q-1} \, mod \, x^2 - a$. Так как $f + gv = (b - v)^{q-1} = 1$ и $f - gv = (b + v)^{q-1} = 1$, если $v \neq \pm b$, то $f = 1$, $g = 0$ и $(b - x)^{q-1} \equiv 1 \, mod \, x^2 - a$. Применяя последнее сравнение к многочлену $c + dx$, получаем

$(c + dx)^2 = (c^2 + d^2a) + 2cdx \equiv (b - x)^{q-1} \equiv 1 \bmod x^2 - a$

и, следовательно, $c^2 + d^2a = 1$, $cd = 0$. Допустим, что $d = 0$. Тогда $c^2 = 1$ и $(b - x)^{\frac{q-1}{2}} \equiv e \bmod x^2 - a$, где $e \in \{1, -1\}$. Замена x на $-x$ даёт сравнение $(b + x)^{\frac{q-1}{2}} \equiv e \bmod x^2 - a$. Но тогда $(b - v)^{\frac{q-1}{2}}(b + v)^{\frac{q-1}{2}} = (b^2 - a)^{\frac{q-1}{2}} = 1$, что противоречит условию о том, что $b^2 - a$ – неквадрат в $\mathbb{F}_q$. Значит, $c = 0$, а $d^2a = 1$. □

67.2. Метод Поклингтона [48]

67.5. ***Теорема***. *Пусть* a, b, c, d *– те же, что и в теореме* 3, $q \equiv 1 \, (mod \, 4)$, $f + gx$ *– многочлен, определяемый в кольце* $\mathbb{F}_q[x]$

---

[48] ***Генри Кабурн Поклингтон*** (28.01.1870 – 15.05.1952) – английский математик.

сравнением $f + gx \equiv (b - x)^{\frac{q-1}{4}} \bmod x^2 - a$. *Тогда* $\left(\frac{f}{g}\right)^2 = -a$, *и, следовательно,* $\frac{f}{g}$ *и* $-\frac{f}{g}$ *– квадратные корни из* $-a$ *(заметим, что при* $q \equiv 1 \pmod 4$ *как* a, *так и* $-a$ *являются квадратами в* $\mathbb{F}_q$).

Доказательство. С учётом предыдущей теоремы имеем $(f + gx)^2 = (f^2 + g^2 a) + 2fg \equiv (b - x)^{\frac{q-1}{2}} \equiv c + dx = dx \bmod x^2 - a$. Следовательно, $f^2 + g^2 a = 0$ и $\left(\frac{f}{g}\right)^2 = -a$. □

67.3. Метод Чиполлы

67.6. ***Теорема***. *Пусть* a,b *– те же, что и в теореме* 3, $c + dx$ *– многочлен, определяемый в кольце* $\mathbb{F}_q[x]$ *сравнением* $c + dx \equiv (b - x)^{\frac{q+1}{2}} \bmod x^2 - (b^2 - a)$. *Тогда* $d = 0$, $c^2 = a$ *и, следовательно,* c *и* $-c$ *являются корнями из* a.

Доказательство. Имеем следующие сравнения по модулю $x^2 - (b^2 - a)$:

$x^q = x(x^2)^{\frac{q-1}{2}} \equiv x(b^2 - a)^{\frac{q-1}{2}} = -x \Longrightarrow (b - x)^q = b^q - x^q \equiv b + x;$
$(c^2 + d^2(b^2 - a)) + 2cdx = (c + dx)^2 \equiv (b - x)^{q+1}$
$\equiv (b + x)(b - x) = b^2 - x^2 \equiv b^2 - (b^2 - a) = a.$

Значит, $c^2 + d^2(b^2 - a) = a$, $cd = 0$. Очевидно, что $c \neq 0$, поскольку в противном случае элемент $b^2 - a$ должен быть квадратом в $\mathbb{F}_q$, а это противоречит условию теоремы. Поэтому $d = 0$, но тогда $c^2 = a$. □

67.4. Метод Чиполлы-Лемера [49]

67.7. ***Теорема.*** *Пусть* a, $b \in \mathbb{F}_q$, *причём* a *– квадрат, а* $b^2 - 4a$ *– неквадрат в* $\mathbb{F}_q$; $c + dx$ *– многочлен, определяемый в кольце* $\mathbb{F}_q[x]$ *сравнением* $c + dx \equiv x^{\frac{q+1}{2}} \bmod x^2 - bx + a$. *Тогда* $c^2 = a$, $d = 0$.

---

[49] ***Деррик Генри «Дик» Лемер*** (23.02.1905 — 22.05.1991) – американский математик в области теории чисел.

Доказательство. Так как дискриминант $D(f) = b^2 - 4a$ многочлена $f(x) = x^2 - bx + a$ не является квадратом в $\mathbb{F}_q$, то $f(x)$ – неприводимый многочлен в кольце $\mathbb{F}_q[x]$. Его корни лежат в $\mathbb{F}_{q^2} \cong \mathbb{F}_q[x]/(f(x))$. Если α – один из корней, то α^q – его второй корень, причём $\alpha + \alpha^q = b$, $\alpha^{q+1} = a$, $\alpha^2 = b\alpha - a$. Поле $\mathbb{F}_{q^2} \cong \mathbb{F}_q(\alpha)$ образовано элементами $u + v\alpha$, $u,v \in \mathbb{F}_q$. Из равенства $c + d\alpha = \alpha^{\frac{q+1}{2}}$ следует, что $(c + d\alpha)^2 = a$. Поскольку $(c + d\alpha)^2 = c^2 + 2cd\alpha + d^2\alpha^2 = (c^2 - d^2a) + d(db + 2c)\alpha$, то $c^2 - d^2a = a$, $d(db + 2c) = 0$. Если допустить, что $d \neq 0$, то $d = -\frac{2c}{b}$ и $c^2 - d^2a = c^2\frac{b^2-4a}{b^2} = a$, откуда следует, что $b^2 - 4a$ – квадрат в $\mathbb{F}_q$, но это противоречит условию теоремы. Значит, $d = 0$, но тогда $c^2 = a$. □

67.5. Метод Тонелли–Шенкса

Изложим идею метода, предложенного Тонелли[50] и развитого Шенксом[51] [**60, 61**]. Представим число q в виде $2^s t + 1$, где $s, t \in \mathbb{N}$, t нечётно. Пусть a – квадрат в $\mathbb{F}_q^*$, т.е. $a = x^2$ для некоторого $x \in \mathbb{F}_q^*$. Отметим, что мультипликативная группа $\mathbb{F}_q^*$, поля $\mathbb{F}_q$ является циклической, и любая её подгруппа также циклическая. Полагая

$$G_s = \{\beta^t \mid \beta \in \mathbb{F}_q^*\};\ G_e = \{\gamma^2 \mid \gamma \in G_{e+1}\},\ e = s-1, s-2, \ldots, 1,$$

имеем следующую цепочку циклических подгрупп группы $\mathbb{F}_q^*$: $G_1 < G_2 < \cdots < G_{s-1} < G_s$. Порядок группы G_e равен 2^e, $e = 1, 2, \ldots, s$. Каждый элемент группы G_e является квадратом некоторого элемента из G_{e+1}. Если g_{e+1} – порождающий элемент группы G_{e+1}, то $g_e = g_{e+1}^2$ – порождающий элемент группы G_e. В любой цикли-

---

[50] ***Альберто Тонелли*** (25.12.1849 – 29.12.1920) – итальянский математик.

[51] ***Дэниел Шенкс*** (17.01.1917 – 6.09.1996) –— американский математик в области теории чисел. Известен монографией «*Решённые и нерешённые проблемы теории чисел*». Предложил алгоритм извлечения квадратного корня по простому модулю для факторизации целых чисел.

ческой группе порядка n имеется $\varphi(n)$ порождающих элементов. Поскольку $\varphi(2^s) = 2^{e-1}$, то в G_s каждый второй элемент, т.е. неквадрат, является порождающим элементом. Поэтому в качестве g_s можно взять любой элемент $g = b^t$, где $b -$ неквадрат в $\mathbb{F}_q^*$, поскольку в этом случае $g^{2^{s-1}} = b^{(q-1)/2} = -1$. Так как $a^t -$ квадрат и $a^{t2^{e-1}} = x^{(q-1)/2} = 1$, то $a^t \in G_{s-1}$. Поэтому существует чётное число k такое, что $a^t g^k = 1$, но тогда $x = a^{(t+1)/2} g^{k/2}$. Действительно, $x^2 = (a^{t+1})g^k = (a^t g^k)a = a$. Таким образом, вычисление значения x сводится к решению задачи дискретного логарифмирования в группе G_s: найти k такое, что $g^k = a^{-t}$.

Пусть $k = (k_1 k_2 \dots k_{s-1})_2 = k_1 2^1 + k_2 2^2 + \cdots + k_{s-1} 2^{s-1}$, где $k_i \in \{0, 1\}, -$ двоичное (битовое) представление числа k. Значения k_i, и, следовательно, k можно вычислить последовательно (″бит за битом″) следующим способом.

Имеем

$$g^{k_1 2^1 + k_2 2^2 + \cdots + k_{s-1} 2^{s-1}} = a^{-t}.$$

Возводя обе части этого равенства в степень 2^{s-2}, получим $g^{k_1 2^{s-1}} = a^{-t2^{s-2}}$. Тогда $A_1 = a^{-t2^{s-2}} = 1$ или -1, когда $k_1 = 0$ и 1 соответственно. Поэтому

$$k_1 = \begin{cases} 0, \text{если } A_1 = 1, \\ 1, \text{если } A_1 = -1. \end{cases}$$

Аналогично, возводя в степень 2^{s-3} обе части равенства

$$g^{k_2 2^2 + \cdots + k_{s-1} 2^{s-1}} = a^{-t} g^{-k_1 2^1}$$

вычислим значение k_2. Продолжая этот процесс, вычислим значение k.

Алгоритм TS1 $(\boldsymbol{a}, \boldsymbol{x}: \mathbb{F}_q)$

Вход: $a \in \mathbb{F}_q -$ квадрат в поле $\mathbb{F}_q$ нечётной характеристики.

1. (Вычисление s, $t \in \mathbb{N}$ таких, что $q - 1 = 2^s t$, где t нечётно.)

$s := 0$;

$t := q - 1$;

while $t -$ *чётное число* ***do*** $\{s := s + 1; t := t \; div \; 2\}$;

2. Вычисляем (путём перебора) квадратичный невычет $b \in \mathbb{F}_q$;

$g := b^t$;

3. (Вычисление $h -$ квадратного корня из a^{-t}.)

$c := a^t$;
$h := 1$;
$g := g^{-1}$;
for $i := 1$ ***to*** $s - 1$ ***do*** {
$n := 2^{s-1-i}$; $d := c^n$;
if $d \neq 1$ ***then*** $\{h := hg; c := cg^2\}$;
$c := c^2$
};
4. $x := a^{(t+1)/2}h$; $return\ (x)$.
Выход: $x \in \mathbb{F}_q$ – квадратный корень из a (т.е. $x^2 = a$).

Алгоритм TS2 $(\boldsymbol{a}, \boldsymbol{x}: \mathbb{F}_q)$
Вход: $a \in \mathbb{F}_q^*$ – квадрат в поле $\mathbb{F}_q$ нечётной характеристики.
1. (Вычисление s, $t \in \mathbb{N}$ таких, что $q - 1 = 2^s t$, где t нечётно.)
$s := 0$;
$t := q - 1$;
while $not\ odd\ (t)$ ***do*** {
$s := s + 1$;
$t := t\ div\ 2$
};
2. Находим какой-либо квадратичный невычет $b \in \mathbb{F}_q^*$; $g := b^t$;
3. $c := g$; $k := s$; $x := a^{\frac{t-1}{2}}$; $y := ax^2$; $x := ax$;
4. ***while*** $y \neq 1$ ***do*** {
вычисляем наименьшее $m \in \mathbb{N}$ такое, что $y^{2^m} = 1$:
$u := c^{2^{k-m-1}}$; $c := u^2$; $k := m$; $x := xu$; $y := yc$; $goto\ 4$.
}.
5. $return\ (x)$.
Выход: $x \in \mathbb{F}_q^*$ – квадратный корень из a (т.е. $x^2 = a$).

Обоснование алгоритма. В начале шага 4 всякий раз выполняются равенства: $ay = x^2$; $c^{2^{k-1}} = -1$; $y^{2^{k-1}} = 1$. Так как группа G_k состоит из элементов, порядок которых является делителем числа 2^k, то c – порождающий элемент этой группы, а $y \in G_{k-1}$ – квадрат в G_k. Число k уменьшается на каждом шаге. Поэтому об-

щее число шагов не превышает s, и алгоритм успешно завершается, если a – квадратичный вычет в $\mathbb{F}_q^*$.

Замечание. Если значение m, вычисляемое на шаге 4, равно s, то a – квадратичный невычет в $\mathbb{F}_q^*$ и уравнение $x^2 = a$ заведомо не имеет решения в $\mathbb{F}_q^*$. В этом случае искомые корни лежат в поле $\mathbb{F}_{q^2}$.

§ 68. Уравнения степени n ⩽ 4 над конечным полем характеристики ⩾ 5

Пусть $\mathbb{F}_q$ – конечное поле из $q = p^m$ элементов, $p \neq 2, 3$ – простое число. Рассмотрим уравнения

$x^2 + a_1 x + a_2 = 0, a_1, a_2 \in \mathbb{F}_q;$ (1)

$x^3 + a_1 x^2 + a_2 x + a_3 = 0, a_1, a_2, a_3 \in \mathbb{F}_q;$ (2)

$x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4 = 0, a_1, a_2, a_3, a_4 \in \mathbb{F}_q.$ (3)

Корни этих уравнений могут лежать как в поле $\mathbb{F}_q$, так в некоторых его расширениях. Вычисление значений корней может быть осуществлено по хорошо известным формулам [**7**, **22**].

Уравнение (**1**). Корни вычисляются по формулам

$$x_1 = \frac{-a_1 + \sqrt{D}}{2},\ x_2 = \frac{-a_1 - \sqrt{D}}{2},$$

где $D = a_1^2 - 4a_2$. Вопрос о вычислении $\sqrt{D}$ рассмотрен выше в § 67.

Уравнение **(2)** путем замены $x = y - \frac{a_1}{3}$ приводится к "неполному" виду

$$y^3 + ay + b = 0, \quad (4)$$

где

$$a = \frac{a_1}{3} + a_2, \qquad b = 2\left(\frac{a_1}{3}\right)^3 - \frac{a_1 a_2}{3} + a_3.$$

Корни последнего уравнения вычисляются по формулам Тартальи-Кардано:

$$y_1 = \sqrt[3]{-\frac{27}{2}b + \frac{3}{2}\sqrt{-3D}} + \sqrt[3]{-\frac{27}{2}b - \frac{3}{2}\sqrt{-3D}},$$

$$y_2 = \rho^2\left(\sqrt[3]{-\frac{27}{2}b + \frac{3}{2}\sqrt{-3D}}\right) + \rho\left(\sqrt[3]{-\frac{27}{2}b - \frac{3}{2}\sqrt{-3D}}\right),$$

$$y_3 = \rho\left(\sqrt[3]{-\frac{27}{2}b + \frac{3}{2}\sqrt{-3D}}\right) + \rho^2\left(\sqrt[3]{-\frac{27}{2}b - \frac{3}{2}\sqrt{-3D}}\right),$$

где

$D = -4a^3 - 27b^2$, $\rho = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$, $\rho^2 = -\frac{1}{2} - \frac{1}{2}\sqrt{-3}$

(заметим, что $\rho^0 = 1,\ \rho,\ \rho^2$ – кубические корни из единицы).

68.1. ***Теорема*** Диксона [**50**, **58**]. *Корни многочлена* (4)*, где* a, $b \in \mathbb{F}_{p^m}$, $p > 3$, $D = -4a^3 - 27b^2 \neq 0$, *характеризуются следующим образом*:

1) *все три корня лежат в* $\mathbb{F}_{p^m}$ *тогда и только тогда, когда* $D = 81\mathrm{c}^2$ *– квадрат в* $\mathbb{F}_{p^m}$, $\frac{1}{2}\left(-b + \mathrm{c}\sqrt{-3}\right)$ *есть куб*

в $\begin{cases} \mathbb{F}_{p^m}, & \text{если } p^m \equiv 1 \ (mod\ 3), \\ \mathbb{F}_{p^{2m}}, & \text{если } p^m \equiv 2 \ (mod\ 3); \end{cases}$

2) *один корень лежит в* $\mathbb{F}_{p^m}$, *а два других лежат в* $\mathbb{F}_{p^{2m}}$, *тогда и только тогда, когда* D *– неквадрат в* $\mathbb{F}_{p^m}$;

3) *все три корня лежат в* $\mathbb{F}_{p^{3m}}$ *тогда и только тогда, когда* $D = 81\mathrm{c}^2$ *– квадрат в* $\mathbb{F}_{p^m}$, $\frac{1}{2}\left(-b + d\sqrt{-3}\right)$ *есть некуб*

в $\begin{cases} \mathbb{F}_{p^m}, & \text{если } p^m \equiv 1 \ (mod\ 3), \\ \mathbb{F}_{p^{2m}}, & \text{если } p^m \equiv 2 \ (mod\ 3). \end{cases}$

Отметим: если $p^m \equiv 1 \ (mod\ 3)$, то $w = \sqrt{-3} \in \mathbb{F}_{p^m}$; если $p^m \equiv 2 \ (mod\ 3)$, то $w \in \mathbb{F}_{p^{2m}}$.

Извлечение кубических корней в конечном поле $\mathbb{F}_q$ ***характеристики*** $p \neq 3$.

Пусть α – примитивный элемент поля $\mathbb{F}_q$, $a = \alpha^k$, $x = \alpha^m$ – корень уравнения $x^3 = a$. Тогда $\alpha^{3m} = \alpha^k$, или $3m \equiv k \ (mod\ q - 1)$.

Если НОД $(3, q - 1) = 1$, то существует $d \in \mathbb{N}$ такое, что $3d \equiv 1 \ (mod\ q - 1)$ (d – мультипликативный обратный к 3 по модулю $q - 1$, вычисляется с использованием расширенного алгоритма Евклида). Тогда $3m \equiv k \ (mod\ q - 1) \Longrightarrow m \equiv dk \ (mod\ q - 1)$. Другими словами, $x = a^d$.

Если НОД $(3, q - 1) = 3$, то необходимо найти $k = ind\ _{\alpha} a$ – дискретный логарифм элемента a по основанию α. Если $3 \mid k$, то $3m \equiv k \ (mod\ q - 1) \Longrightarrow m \equiv \frac{k}{3} \ (mod\ \frac{q-1}{3})$. В этом случае уравнение $x^3 = a$ имеет три решения: $x = a^{k/3}$, $a^{k/3}\omega$, $a^{k/3}\omega^2$, где $\omega = \alpha^{q-1/3}$ – корень уравнения $x^3 = 1$.

Если НОД $(3, q - 1) = 3$ и $k \not\equiv 0 \ (mod\ 3)$, то уравнение $x^3 = a$ не имеет корней в $\mathbb{F}_q$.

Уравнение (**3**) путем замены $x = y - \frac{a_1}{4}$ приводится к ″неполному″ виду

$$y^4 + by^2 + cy + d = 0, \qquad (5)$$

где

$$b = \frac{8a_1a_3 - 3a_2^2}{8a_1^2}, c = \frac{8a_1^2a_4 + a_2^3 - 4a_1a_2a_3}{8a_1^3},$$
$$d = \frac{16a_1a_2^2a_3 - 64a_1^2a_2a_4 - 3a_2^4 + 256a_1^3a_3}{256a_1^4}$$

Решение Феррари [52]: пусть α_0 − один из корней ″неполного″ кубичного уравнения

$$\alpha^3 + b\alpha^2 + \left(\frac{b^2}{4} - d\right)\alpha - \frac{c^2}{8} = 0.$$

Тогда четыре корня ″неполного″ уравнения (5) находятся как корни двух квадратных уравнений:

$$z^2 - \beta\sqrt{2\alpha_0}\, z + \left(\frac{b}{2} + \alpha_0 + \beta\frac{c}{2\sqrt{2\alpha_0}}\right) = 0,$$

получающихся при $\beta = -1$ и 1.

---

[52] ***Лодовико Феррари*** (2.02.1522 − 5.10.1565) – итальянский математик, нашедший общее решение уравнения четвёртой степени.

Приложения

A. Конечные поля $GF(8), GF(16), GF(32)$

Для построения поля $\mathbb{F}_{2^n}$ используются неприводимые многочлены над полем $\mathbb{F}_2$ степени n, где $n = 1, 2, 3$ ...

Степень	Неприводимые многочлены
1	$(x+1), (x)$
2	(x^2+x+1)
3	$(x^3+x^2+1), (x^3+x+1)$
4	$(x^4+x^3+x^2+x+1), (x^4+x^3+1), (x^4+x+1)$
5	$(x^5+x^2+1), (x^5+x^3+x^2+x+1), (x^5+x^4+x^3+x+1),$ $(x^5+x^4+x^3+x^2+1), (x^5+x^4+x^2+x+1)$

Пример. Возьмём кубический многочлен $f(x)$, неприводимый в $\mathbb{F}_2[x]$. Его можно использовать для построения расширения $\mathbb{F}_{2^3} = \mathbb{F}_8$ поля $\mathbb{F}_2$. Элементы поля $\mathbb{F}_8$ представлены многочленами из $\mathbb{F}_2[x]$ степени ≤ 2 с операциями сложения и умножения многочленов по модулю $f(x)$. Например, если $a(x) = x^2 + x + 1$ и $b(x) = x + 1$, то $a(x) + b(x) = x^2 + 2x + 2 = x^2$, $a(x) \cdot b(x) = x^3 + 2x^2 + 2x + 1 = x^3 + 1 = (x^3 + x + 1) + x \equiv x\ (mod\ f\ (x))$.

Умножение в поле $\mathbb{F}_8 \cong \mathbb{F}_2[x]/(x^3 + x^2 + 1)$

Многочлен $a_2x^2 + a_1x + a_0$ обозначаем для краткости двоичным набором $a_2a_2a_0$.

×	000	001	010	011	100	101	110	111
000	000	000	000	000	000	000	000	000
001	000	001	010	011	100	101	110	111
010	000	010	100	110	011	001	111	101
011	000	011	110	101	111	100	001	010
100	000	100	011	111	110	010	101	001
101	000	101	001	100	010	111	011	110
110	000	110	111	001	101	011	010	100
111	000	111	101	010	001	110	100	011

Поле $\mathbb{F}_{16}$

Конечное поле $\mathbb{F}_{16}$ изоморфно факторкольцу $\mathbb{F}_2[x]/(f(x))$, где $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$ – неприводимый примитивный многочлен. Ненулевые элементы поля представлены значениями многочленов $\alpha_3 x^3 + \alpha_2 x^2 + \alpha_1 x + \alpha_0 \in \mathbb{F}_2[x]$ при $x = \alpha$, где α – корень многочлена $f(x)$,. Так что у $= \alpha_3\alpha^3 + \alpha_2\alpha^2 + \alpha_1\alpha + \alpha_0$, $\alpha_3, \alpha_2, \alpha_1, \alpha_0 \in \mathbb{F}_2$. Нулевой элемент поля получается при $x = 0$. Так как мультипликативная группа поля $\mathbb{F}_{16}$ является циклической, а $f(x)$ – примитивный многочлен, то любой ненулевой элемент у $\in \mathbb{F}_{16}$ равен α^m при некотором $m \in [0..14]$. Соответствующее число m (дискретный логарифм) обозначаем как ind_αу. Полагаем $ind_\alpha 0 = \infty$. Через N(у)обозначим числовое значение двоичного набора $\alpha_3\alpha_2\alpha_1\alpha_0$, т.е. $N(\text{у}) = \alpha_3 2^3 + \alpha_2 2^2 + \alpha_1 2 + \alpha_0$.

Элементы поля $\mathbb{F}_{16}$ представлены в следующей таблице

$\boldsymbol{ind_\alpha}$у	у = $\boldsymbol{\alpha_4\alpha_3\alpha_2\alpha_1\alpha_0}$	$\boldsymbol{N}$(у)	у = $\boldsymbol{\alpha_4\alpha_3\alpha_2\alpha_1\alpha_0}$	$\boldsymbol{N}$(у)	$\boldsymbol{ind_\alpha}$у
∞	0000	0	0000	0	∞
0	0001	1	0001	1	0
1	0010	2	0010	2	1
2	0100	4	0011	3	4
3	1000	8	0100	4	2
4	0011	3	0101	5	8
5	0110	6	0110	6	5
6	1100	12	0111	7	10
7	1011	11	1000	8	3
8	0101	5	1001	9	14
9	1010	10	1010	10	9
10	0111	7	1011	11	7
11	1110	14	1100	12	6
12	1111	15	1101	13	13
13	1101	13	1110	14	11
14	1001	9	1111	15	12

Поле $\mathbb{F}_{32}$

Конечное поле $\mathbb{F}_{2^5} = \mathbb{F}_{\mathbf{32}}$ изоморфно факторкольцу $\mathbb{F}_2[x]/(f(x))$, где $f(x) = x^5 + x^2 + 1 \in \mathbb{F}_2[x]$ – неприводимый примитивный многочлен. Мультипликативная группа этого поля $\mathbb{F}_{2^5}^* = \mathbb{F}_{2^5} \backslash \{0\}$ является циклической, т.е. $\mathbb{F}_{2^5} =< \alpha >= \{1, \alpha, \alpha^2, \dots, \alpha^{q-2}\}$ для любого элемента $\alpha \in \mathbb{F}_{2^5}$, $\alpha \neq 1$ (в качестве α берём один из корней многочлена $f(x)$. Элементы поля $\mathbb{F}_{32}$ представлены в приводимой ниже таблице.

Степенной базис	Нормальный базис	$ind_\alpha \beta$	$\beta_4\beta_3\beta_2\beta_1\beta_0$	$N(\beta)$	β	$\gamma_4\gamma_3\gamma_2\gamma_1\gamma_0$	N(γ)	$Z(x)$
		∞	00000	0	00000	00000	0	1
1		0	00001	1	00001	11111	31	∞
α^1		1	00010	2	00010	00011	3	18
α^2		2	00100	4	00011	00110	6	5
α^3	$\varepsilon = \alpha^3$	3	01000	8	00100	00001	1	29
α^4		4	10000	16	00101	01100	12	10
		5	00101	5	00110	11001	25	2
	$\varepsilon^2 = \alpha^6$	6	01010	10	00111	00010	2	27
		7	10100	20	01000	01010	10	22
		8	01101	13	01001	11000	24	20
		9	11010	26	01010	01110	14	16
		10	10001	17	01011	10011	19	4
		11	00111	7	01100	11010	26	19
	$\varepsilon^4 = \alpha^{12}$	12	01110	14	01101	00100	4	23
		13	11100	28	01110	01011	11	14
		14	11101	29	01111	10100	20	13
		15	11111	31	10000	10111	23	24
		16	11011	27	10001	10001	17	9
	$\varepsilon^{16} = \alpha^{17}$	17	10011	19	10010	10000	16	30
		18	00011	3	10011	11100	28	1
		19	00110	6	10100	00101	5	11
		20	01100	12	10101	00111	7	8
		21	11000	24	10110	01101	13	25
		22	10101	21	10111	10101	21	7
		23	01111	15	11000	11011	27	12
	$\varepsilon^8 = \alpha^{24}$	24	11110	30	11001	01000	8	15
		25	11001	25	11010	10010	18	21
		26	10111	23	11011	10110	22	28
		27	01011	11	11100	11101	29	6
		28	10110	22	11101	01001	9	26
		29	01001	9	11110	11110	30	3
		30	10010	18	11111	01111	15	17

Используются следующие обозначения:

$ind_\alpha\beta$ – дискретный логарифм элемента β по основанию $\alpha, \alpha, \beta \in \mathbb{F}_{2^5}^*$. Определяется как наименьшее $x \in \mathbb{N} \cup \{0\}$ такое, что $\alpha^x = \beta$;

$1, \alpha, \alpha^2, \alpha^3, \alpha^4$ – *степенной базис*. Всякий элемент $\beta \in \mathbb{F}_{2^5}$ можно однозначно представить в виде $\beta = \beta_4\alpha^4 + \beta_3\alpha^3 + \beta_2\alpha^2 + \beta_1\alpha + \beta_0$ для некоторых $\beta_4, \beta_3, \beta_2, \beta_1, \beta_0 \in \mathbb{F}_2$;

$(\varepsilon, \varepsilon^2, \varepsilon^4, \varepsilon^8, \varepsilon^{16}) = (\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{17})$ – *нормальный базис*. Всякий элемент $\gamma \in \mathbb{F}_{2^5}$ однозначно представим в виде $\gamma = \gamma_4\varepsilon^{16} + \gamma_3\varepsilon^8 + \gamma_2\varepsilon^4 + \gamma_1\varepsilon^2 + \gamma_0\varepsilon$ для некоторых $\gamma_4, \gamma_3, \gamma_2, \gamma_1, \gamma_0 \in \mathbb{F}_2$.

$Z(x)$ – *логарифм Зеха* – определяется равенством $\alpha^{Z(x)} = \alpha^x + 1$.

Б. Неприводимые примитивные многочлены над полем GF(2) степени $n \leqslant 168$

n	f	n	f	n	f	n	f
1	x + 1	43	6 4 3	85	8 2 1	127	1
2	1	44	6 5 2	86	6 5 2	128	29 27 2
3	1	45	4 3 1	87	13	129	5
4	1	46	8 5 3 2 1	88	8 5 4 3 1	130	3
5	2	47	5	89	38	131	48 47 1
6	1	48	7 5 4 2 1	90	5 3 2	132	29
3	1	49	9	91	7 6 5 3 2	133	52 51 1
8	4 3 2	50	4 3 2	92	6 5 2	134	57
9	4	51	6 3 1	93	2	135	11
10	3	52	3	94	21	136	26 25 1
11	2	53	6 2 1	95	11	137	21
12	8 4 1	54	6 5 4 3 2	96	7 6 4 3 2	138	8 7 1
13	4 3 1	55	24	97	6	139	8 5 3
14	5 3 1	56	7 4 2	98	11	140	29
15	1	57	7	99	7 5 4	141	32 31 1
16	5 3 2	58	19	100	37	142	21
17	3	59	6 5 4 3 1	101	7 6 1	143	21 20 1
18	7	60	1	102	67 66 1	144	70 69 1
19	5 2 1	61	5 2 1	103	9	145	52
20	3	62	6 5 3	104	11 10 1	146	60 59 1
21	2	63	1	105	16	147	38 37 1
22	1	64	4 3 1	106	15	148	27
23	5	65	18	107	65 63 1	149	110 109 1
24	7 2 1	66	8 6 5 3 2	108	31	150	53
25	3	67	5 2 1	109	7 6 1	151	3
26	6 2 1	68	9	110	13 12 1	152	66 65 1
27	5 2 1	69	6 5 2	111	10	153	1
28	3	70	5 3 1	112	45 43 2	154	129 127 2
29	2	71	6	113	9	155	32 31 1
30	6 4 1	72	6 4 3 2 1	114	82 81 1	156	116 115 1
31	3	73	25	115	15 14 1	157	27 26 1
32	22 2 1	74	7 4 3	116	71 70 1	158	27 26 1
33	13	75	6 3 1	117	20 18 2	159	31
34	27 2 1	76	5 4 2	118	33	160	19 18 1
35	2	77	6 5 2	119	8	161	18
36	11	78	7 2 1	120	113 9 2	162	88 87 1
37	5 4 3 2 1	79	9	121	18	163	60 59 1
38	6 5 1	80	7 5 3 2 1	122	60 59 1	164	14 13 1
39	4	81	4	123	2	165	31 30 1
40	5 4 3	82	8 7 6 4 1	124	37	166	39 38 1
41	3	83	7 4 2	125	124 18 17	167	6
42	5 4 3 2 1	84	13	126	37 36 1	168	17 15 2

Показатели степеней $l, k, \ldots, m$ обозначают многочлен $f = x^n + x^l + x^k + \cdots + x^m + 1$.

Источник: W. Stahnke, Primitive binary polynomials, Math. Comp. 27 (1973), 977– 980.

Например, $f(x) = x^{168} + x^{17} + x^{15} + x^2 + 1$ – неприводимый примитивный многочлен 168-ой степени в кольце $\mathbb{F}_2[x]$. Корень этого многочлена является примитивным элементом, т.е. порождает мультипликативную циклическую группу $\mathbb{F}_{2^{168}}^* = < \alpha > = \{1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{2^{168}-2}\}$ поля $\mathbb{F}_{2^{168}}$.

B. Разложение чисел вида $2^n \pm 1$ на простые множители

См. также: ***Д. Кнут***. Искусство программирования для ЭВМ. Т. 2. – М.: Мир, 1977. – С. 26. Таблица 1; ***Х. Уильямс***. Проверка чисел на простоту с помощью вычислительных машин. – В кн.: Кибернетический сборник. Вып. 23. – М.: Мир, 1986. – С. 51-99;
В.И. Нечаев Элементы криптографии (Основы теории защиты информации). – М.: Высшая школа,1999 – Приложения 5.1-5.2.

n	$2^n - 1$	$2^n + 1$
1	1	3
2	3 – простое число Мерсенна [53]	5 – простое число Ферма
3	7 – простое число Мерсенна	3^2
4	$3 \cdot 5$	17 – простое число Ферма
5	31– простое число Мерсенна	$3 \cdot 11$
6	$3^2 \cdot 7$	$5 \cdot 13$
7	127– простое число Мерсенна	$3 \cdot 43$
8	$3 \cdot 5 \cdot 7$	257 – простое число Ферма
9	$7 \cdot 73$	$3^3 \cdot 19$
10	$3 \cdot 11 \cdot 31$	$5^2 \cdot 41$
11	$23 \cdot 89$	$3 \cdot 683$
12	$3^2 \cdot 5 \cdot 7 \cdot 13$	$17 \cdot 241$
13	8191 – простое число Мерсенна	$3 \cdot 2731$
14	$3 \cdot 43 \cdot 127$	$5 \cdot 29 \cdot 113$
15	$7 \cdot 31 \cdot 151$	$3^2 \cdot 11 \cdot 331$
16	$3 \cdot 5 \cdot 17 \cdot 257$	65537 – простое число Ферма
17	131071 – простое число Мерсенна	$3 \cdot 43691$
18	$3^2 \cdot 7 \cdot 19 \cdot 73$	$5 \cdot 13 \cdot 37 \cdot 109$
19	524287 – простое число Мерсенна	$3 \cdot 174763$
20	$3 \cdot 5^2 \cdot 11 \cdot 31 \cdot 41$	$17 \cdot 61681$
21	$7^2 \cdot 127 \cdot 337$	$3^2 \cdot 43 \cdot 5419$
22	$3 \cdot 23 \cdot 89 \cdot 683$	$5 \cdot 397 \cdot 2113$
23	$47 \cdot 178481$	$3 \cdot 2796203$
24	$3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241$	$97 \cdot 257 \cdot 673$

[53] ***Марен Мерсенн*** (8.09.1588 – 1.09.1648) – французский математик, физик, философ и богослов, теоретик музыки.

25	$31 \cdot 601 \cdot 1801$	$3 \cdot 11 \cdot 251 \cdot 4051$
26	$3 \cdot 2731 \cdot 8191$	$5 \cdot 53 \cdot 157 \cdot 1613$
27	$7 \cdot 73 \cdot 262657$	$3^4 \cdot 19 \cdot 87211$
28	$3 \cdot 5 \cdot 29 \cdot 43 \cdot 113 \cdot 127$	$17 \cdot 15790351$
29	$233 \cdot 1193 \cdot 2089$	$3 \cdot 59 \cdot 3033169$
30	$3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331$	$5^2 \cdot 13 \cdot 41 \cdot 61 \cdot 1321$
31	2147483647 – простое число Мерсенна	$3 \cdot 715827773$
32	$3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537$	$641 \cdot 6700417$
…		
63	$7^2 \cdot 73 \cdot 127 \cdot 337 \cdot 92737 \cdot 649657$	$3 \cdot 19 \cdot 43 \cdot 5419 \cdot 77158673929$
64	$3 \cdot 5 \cdot 17 \cdot 257 \cdot 641 \cdot 65537 \cdot 6700417$	$274177 \cdot 67280421310721$

Указатель имен

Предметный указатель

Литература

1. *Акритас М. А.* Основы компьютерной алгебры с приложениями: Пер. с англ. — М., Мир, 1994.
2. *Альберт А.А.* Конечные поля. – В кн.: Кибернетический сборник (новая серия). Вып. 3. – М. : Мир, 1966, с. 7–49.
3. *Айерлэнд К., Розен М.* Классическое введение в современную теорию чисел. – М.: Мир, 1897.
4. *Берлекэмп Э.* Алгебраическая теория кодирования. – М.: Мир, 1971.
5. *Биркгоф Г., Барти Т.* Современная прикладная алгебра. – М.: Мир, 1976.
6. *Бурбаки Н.* Алгебра. Многочлены и поля. Упорядоченные группы. – М.: Наука, 1965.
7. *Ван дер Варден Б. Л.* Алгебра. – М.: Наука, 1947, 1979.
8. *Василенко О. Н.* Теоретико-числовые алгоритмы в криптографии. — М.: МЦНМО, 2003.
9. *Виланова Кловис.* О некоторых трёхчленных уравнениях над конечными полями. // Тр. Унив. дружбы народов им. П. Лумумбы, 1977, вып. 21, с. 17–31.
10. *Виноградов И. М.* Основы теории чисел. – М.: Наука, 1965.
11. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра. В 2-х т. – М.: Гелиос АРВ, 2003.
12. *Иванов Б. Н.* Дискретная математика. Алгоритмы и программы. – М.: Лаборатория базовых знаний, 2003.
13. *Ишмухаметов Ш.Т.* Методы факторизации натуральных чисел. Казань: Казан. ун-т, 2011.
14. *Кнут Д.Е. И*скусство программирования для ЭВМ. – М.: Мир, 1977. Т.2. § 4.6.2. С. 461–482.
15. *Кокс Д., Дж. Литтл Дж., О' Ши Д.* Идеалы, многообразия и алгоритмы. – М.: Мир, 2000.
16. *Кострикин А. И.* Введение в алгебру. – М.: Наука, 1977.
17. *Кострикин А. И.* Введение в алгебру. Ч. 1-3. – М.: Физмат, 2000, 2002.
18. *Кугураков В. С.* Замечание о решении квадратных уравнений в конечном поле характеристики 2. // Вероятностные методы и

кибернетика, вып. 21, с. 107–108. – Казань: Изд-во Казанского университета, 1985.

19. *Кугураков В.С., Кирпичников А. П.* Об одной задаче теории кодирования данных при передаче информации по каналам связи. // Вестник Технологического университета, т. 18, № 15, с. 221–225. – Казань: Изд-во КНИТУ, 2015.

20. *Кугураков В.С., Кирпичников А. П.* Решение кубических уравнений в конечном поле характеристики 3. // Вестник Технологического университета, т. 18, № 6, с. 221–222. – Казань: Изд-во КНИТУ, 2015.

21. *Куликов Л. Я.* Алгебра и теория чисел. – М: Высшая школа, 1979.

22. *Курош А. Г.* Курс высшей алгебры. – М.: Наука, 1975.

23. *Ленг С.* Алгебра. – М.: Мир, 1968.

24. *Лидл Р., Нидеррайтер Г.* Конечные поля. – В 2-х томах. – М.: Мир,1988.

25. *Лидл Р., Пильц Г.* Прикладная абстрактная алгебра. – Екатеринбург: Изд-во УГУ, 1996.

26. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж.* Теория кодов, исправляющих ошибки. – М.: Связь, 1979.

27. *Мальцев А. И.* Алгебраические системы. − М.: Наука, 1970.

28. *Матвеева М.В.* Об исправлении тройных ошибок в кодах Боуза-Чоудхури над полем GF(3). // Проблемы передачи информации, 1968, 4, 1, с. 20–27.

29. *Матвеева М.В.* О решении уравнений третьей степени в поле характеристики 3. // Проблемы передачи информации, 1968, 4, 4, с. 76–78.

30. *Нечаев В.И.* Элементы криптографии (Основы теории защиты информации). – М.: Высшая школа, 1999.

31. *Общая алгебра*. Справочная математическая библиотека. Т. 1, 2. – М: Наука, 1990.

32. *Перечислительные задачи комбинаторного анализа*. – М: Мир, 1979.

33. *Питерсон У.* Коды, исправляющие ошибки. − М.: Мир, 1964.

34. *Постников М.М.* Теория Галуа. – М.: Физматгиз, 1963.

35. *Прасолов В.* Многочлены. − М.: МЦМНО, 1999.

36. *Прикладная комбинаторная математика*. – М: Мир, 1988.

37. *Радемахер Г., Теплиц О.* Числа и
ры. – М.: Физмат, 1962.
38. *Холл М.* Комбинаторика. – М: Мир, 1979.
39. *Холл М.* Теория групп. – М: ИЛ, 1962.
40. *Berlekamp E.R.* Factoring polynomials over finite fields.// Bell System Tech. J., 46, pp. 1853–1859 (1967).
41. *Berlekamp E.R.* Factoring polynomials over large finite fields.// Math. Comp., 24, pp. 713–735 (1970).
42. *Berlekamp E.R., Ramsey H., Solomon G.* On the solutions of algebraic equations over finite fields. – Inform. and Control, 1967, v. 10, pp. 553–564.
43. *Bernstein D.J.* Faster square roots in annoying finite fields, draft. Available from (2001).
44. *Butler M.C.R.* On the reducibility of polynomials over a finite field // Quart. J. Math., Oxford Ser. (2) 5, pp. 102–107 (1954).
45. *Cantor D.G., Zassenhaus H.* A new algorithm for factoring polynomials over finite fields. — Math. Comp., 1981. — Vol. 36. — P. 587–592.
46. *Chen Chin-long.* Formulas for the solutions of quadratic equations over GF(2^n) // IEEE Trans. Inform. Theory, 1982, v. 28, №5, pp. 792–794.
47. *Chien R.T., Cunningham B.D., Oldham L.B.* Hibrid methods for finding roots of polynomial – with application to BCH decoding. // IEEE Trans. Inform. Theory, 1969, v. 15, № 2, pp. 329–335.
48. *Cipolla M.* Un metodo per la risoluzione della congruenza di secondo grado. // Rend. Accad. Sci. Fis. Mat. Napoli, 9 (1903), pp. 154–163.
49. *Dickson L.E.* Criteria for the irreducibility of functions in finite field. // Bull. Amer. Math. Soc. 13 (1906), pp. 1–8.
50. *Dickson. L.E.* A fundamental system of invariants of the modular linear group with a solution of the form problem. – Trans. Amer. Math. Soc., 1911, v. 12, pp. 75–91.
51. *Galois Evariste.* Sur la théorie des nombres. // Bulletin des sciences mathématiques de M. Férussac 13, pp. 428–435 (1830).
52. *Kaltofen E., Lobo A.* Factoring high-degree polynomials by the black box Berlekamp algorithm // Proceedings of the international symposium on Symbolic and algebraic computation (ISSAC '94). — N. Y.: ACM Press, 1994.

53. *Kempfert H.* On the factorization of polynomials. J. Number Theory,1, pp. 116–120 (1969).

54. *Kugurakov V., Gainutdinova A.* On the full monomial automorphism groups of Reed-Solomon codes and their MDS-extensions // Lobachevskii Journal of Mathematics. — 2016. — Vol.37, Is.6. — P.650–669.

55. *Kugurakov V.S, Gainutdinova A, Anisimova T.* On Calculation of Monomial Automorphisms of Linear Cyclic Codes // Lobachevskii Journal of Mathematics. м 2018. — Vol.39, Is.7. — P.1024–1038.

56. *Lehmer D.H.* Computer technology applied to the theory of numbers, In: Studies in Number Theory. Englewood Cliffs, NJ: Prentice-Hall, 1969, pp. 117–151.

57. *Leonard P.A., Williams K.S.* Quartics over F_{2^n} // Proc. Amer. Math. Soc., 36 (1972), pp. 347–350.

58. *Pocklington H. C.* The direct solution of the quadratic and cubic binomial congruences with prime moduli. In: Proc. Cambridge Phil. Soc., Cambridge, U.K., 1917, vol. 19, pp. 57–59.

59. *Schlage-Puchta J.-C.* On Shank's algorithm for modular square roots //Applied Mathematics E-Notes, 5(2005), pp. 84–88. http://www.math.nthu.edu.tw/~amen/

60. *Shanks D.* Five number-theoretic algorithms. In: Proc. 2nd Manitoba Conf. Numer. Math., Manitoba, Canada, 1972. // Utilitas Math., Winnipeg, Man. Congressus Numerantium, No. VII, 1973, pp. 51–70.

61. *Tonelli A.* Bemerkung über die Auflösung quadratischer Congruenzen // Göttinger Nachrichten, 1891, pp. 344-346.

62. *Zassenhaus H.* On Hensel factorization,I, J. Number Theory, 1, pp. 291–311 (1969).

63. *Williams K.S.* Note on Cubics over GF (2^n) and GF (3^n) // J. of Number Theory, 7 (1972), pp. 361–365.