Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Кафедра высшей математики

В.А. Липницкий

СОВРЕМЕННАЯ ПРИКЛАДНАЯ АЛГЕБРА. МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ПОМЕХ И НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Учебное пособие

по курсу «Высшая математика»
для студентов специальностей «Системы, сети и устройства
телекоммуникаций» и «Информатика»
всех форм обучения

Минск 2005

УДК 512 (075.8)
ББК 22.144 я 73
Л 61

Р е ц е н з е н т:
профессор кафедры информатики БГУИР,
доктор физико-математических наук Л.И. Минченко

Липницкий В.А.

Л 61 Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа: Учеб. пособие по курсу «Высшая математика» для студ. спец. «Системы, сети и устройства телекоммуникаций» и «Информатика» всех форм обуч./ В.А. Липницкий. – Мн.: БГУИР, 2005. – 88 с.
ISBN 985-444-789-8

Учебное пособие является первым в Республике Беларусь изданием по алгебраическим основам теории и практики помехоустойчивого кодирования, формирования и обработки дискретных сигналов, защиты информации от несанкционированного доступа. Изложены основы теории чисел, теории групп, теории колец и полей. Структура и подача материала подчинены главной цели – полному, строгому и по возможности краткому изложению теории полей Галуа – одного из основных инструментов построения и обработки кодов и сигналов, многих современных криптосистем.

УДК 512 (075.8)
ББК 22.144 я 73

ISBN 985-444-789-8

СОДЕРЖАНИЕ

Введение

1. Основы теории чисел

1.1. Алгебраические операции на множестве целых чисел
1.2. Наибольший общий делитель целых чисел. Алгоритм Евклида
1.3. Простые числа
1.4. Критерий взаимной простоты целых чисел
1.5. Основная теорема арифметики
1.6. Сравнения
1.7. Кольцо классов вычетов
1.8. Малая теорема Ферма
1.9. Функция Эйлера и теорема Эйлера

2. Элементы теории групп

2.1. Понятие алгебраической системы
2.2. Группы, их основные свойства и типы
2.3. Подгруппы
2.4. Циклические подгруппы
2.5. Смежные классы по подгруппе
2.6. Теорема Лагранжа
2.7. Нормальные подгруппы
2.8. Симметрическая группа
2.9. Знакопеременная группа
2.10. Нормальные подгруппы и фактор-группы
2.11. Гомоморфизмы групп
2.12. Автоморфизмы групп
2.13. Криптосистема RSA

3. Кольца, многочлены и поля

3.1. Основные понятия о кольцах
3.2. Мультипликативная группа кольца
3.3. Делители нуля в кольцах
3.4. Идеалы колец
3.5. Арифметические свойства полиномов
3.6. Многочлены и их корни
3.7. Характерные свойства кольца полиномов
3.8. Фактор-кольца
3.9. Гомоморфизмы колец и полей

4. Теория полей и конечных полей

4.1. Характеристика поля
4.2. Подполя и минимальные подполя
4.3. Векторные пространства и расширения полей
4.4. Алгебраические элементы и алгебраические расширения полей
4.5. Свойства конечных полей: существование и единственность
4.6. Свойства конечных полей: цикличность мультипликативной группы
4.7. Свойства примитивных элементов конечных полей
4.8. Формирование конечных полей
4.9. Автоморфизмы полей. Группа Галуа конечного поля
4.10. Норма и след в конечном поле
4.11. Квадратные уравнения в полях Галуа

Литература

Введение

Современное общество постепенно приходит к осознанию, что на рубеже тысячелетий наступила информационная эпоха, когда информация, достоверная, своевременная и точная, играет важнейшую, определяющую роль. Сейчас самыми состоятельными на Земле являются не владельцы алмазных копий, агрофирм или сталелитейных заводов, а люди, стоящие у руля мощных компьютерных и телекоммуникационных монополий. Факт существования Белорусского государственного университета информатики и радиоэлектроники, одного из крупнейших и популярнейших вузов в Республике Беларусь, свидетельствует о том, что и белорусское общество понимает огромное значение информации в современную эпоху.

На факультетах БГУИР студенты изучают весь спектр вопросов, связанных с обработкой, хранением, передачей и защитой информации от помех и несанкционированного доступа. Соответствующие курсы являются относительно новыми, многие из них находятся в динамике становления или развития в соответствии с технологической революцией или потребностями времени, требуют изучения новых разделов математики, не вошедших в классический курс «Высшая математика» - необходимую базу высшего технического образования. Такие курсы, как «Цифровая обработка сигналов», «Прикладная теория кодирования», «Криптографическая защита информации» (да и не только они) предполагают основательное знание структур современной алгебры. Изложение их внутри соответствующих технических курсов сравнимо с ситуацией изучения романа «Война и мир» параллельно с изложением правил русской грамматики. Только твердое и независимое знание математических основ позволяет осмысленно и уверенно получать новые знания, критически относиться к предмету своих исследований и разработок, находить пути улучшения их слабых мест и недостатков. Базовые предметы в образовании студентов и их математические основания должны быть разделены во времени и пространстве.

В данном учебном пособии изложены основы теории чисел, теории групп, теории колец и полей. Структура и изложение материала подчинены основной задаче – полному, строгому и по возможности краткому изложению теории полей Галуа. Конечные поля – основной инструмент при построении помехоустойчивых кодов и дискретных сигналов, алгоритмов их обработки, многих современных криптосистем. Однако поля Галуа остаются предметом внимания исследователей-математиков и практически полностью отсутствуют в учебной литературе.

Учебное пособие состоит из четырех разделов. В первом разделе изложены основы теории чисел. Основное внимание уделяется свойствам колец классов вычетов по простому и составному модулю – источнику минимальных конечных полей.

Во втором разделе изучаются основы теории групп: группы и их подгруппы – циклические и нормальные, конечные группы и, в частности, группы подстановок, фактор-группы, гомоморфизмы и автоморфизмы групп. Материал, представленный в первых двух разделах, позволяет изложить математическую суть одной из самых популярных в настоящее время систем защиты информации с открытым ключом – криптосистемы RSA.

Третий раздел посвящен изложению теории колец: основные свойства колец, идеалы и фактор-кольца, обстоятельно изучены свойства колец полиномов, факторизация которых по максимальным идеалам дает практически все многообразие полей и конечных полей.

В четвертом разделе систематически изложена теория полей и конечных полей – приведена классификация минимальных полей, теория конечных расширений полей, описание порядков полей Галуа, доказываются их существование и единственность, цикличность мультипликативной группы, приводится описание свойств примитивных элементов и методов формирования конечных полей, их группы Галуа, описание свойств нормы и следа в конечных расширениях полей, исследуется специфика решения квадратных уравнений в полях Галуа, приводятся примеры вычислений в конечных полях, примеры их непосредственного применения.

Изложение материала – замкнутое, с полными доказательствами, сопровождается мотивировкой и примерами прикладного характера.

Пособие относится к предмету «Высшая математика», разделу «Специальные главы высшей математики: современная прикладная алгебра», предназначается для студентов БГУИР специальностей «Информатика» и «Системы и сети телекоммуникаций». Однако издание будет полезно всем, кто изучает проблематику помехоустойчивого кодирования информации, формирования и обработки дискретных сигналов, защиты информации от помех и несанкционированного доступа.

1. Основы теории чисел

1.1. Алгебраические операции на множестве целых чисел

Множество целых чисел Z состоит из элементов 0;±1;±2;…;±n,… . Это счетное множество. На нем определены две алгебраические операции − сложение и умножение. Операции обладают следующими общими свойствами (для любых $a,b,c \in Z$):

1) ассоциативность: $a+(b+c)=(a+b)+c$; $a\cdot(b\cdot c)=a\cdot(b\cdot c)$;
2) коммутативность: $b+a=a+b$; $a\cdot b=b\cdot a$;
3) существует нейтральный элемент - 0 и 1 соответственно: $a+0=0+a=a$; $a\cdot 1=1\cdot a=a$.

Кроме того, операция сложения обладает свойством:

4) для каждого целого $a \in Z$ существует единственное противоположное, то есть такое целое b, что $a+b=b+a=0$.

Ясно, что здесь $b=-a$. Это свойство позволяет ввести вспомогательную операцию – вычитание ($a-b=a+(-b)=c$ – целое число – разность чисел a и b, получаемое вычитанием b из a).

Умножение и сложение связаны свойством

5) $(a+b)\cdot c=a\cdot c+b\cdot c$ − закон дистрибутивности.

Наличие операций сложения и умножения с отмеченными свойствами на множестве целых чисел позволяют отнести Z к разряду коммутативных колец с единицей.

Аналог свойства 4 для умножения выполняется лишь для двух целых чисел 1 и −1. Вообще говоря, для каждого целого $a \in Z$ существует обратное (то есть такое число b, что $a\cdot b=1$), но оно является рациональным, а не целым числом. Следовательно, результат операции деления целого числа a на целое число $b\neq 0$ есть число рациональное и в редких случаях является целым. В общем же случае имеет место

Теорема 1.1.1 (о делении с остатком). *Для любых целых чисел a и b, $b\neq 0$, существует единственные целые числа q и r, $0\le r<|b|$, такие, что $a=b\cdot q+r$.*

В этом равенстве r называют остатком, а q − частным (неполным частным при $r\neq 0$) от деления a на b. Читатель со школьной скамьи умеет находить частное и остаток методом деления уголком.

Пример 1.1.1. а) $a=-20$, $b=3$; тогда $q=-7$, $r=1$;

б) $a=-17$, $b=-5$; тогда $q=4$, $r=3$.

Если в теореме 1.1.1 число $r=0$, то есть $a=b\cdot q$, то говорят, что a делится на b и на q (и пишут: $a\vdots b$, $a\vdots q$), что a является кратным чисел

b и q, что b и q делят a (и пишут: $b \mid a$; $q \mid a$), а также называют b и q делителями или множителями числа a.

Важной для изложения дальнейшего материала является следующая

Лемма 1.1.1. *Если в равенстве* $a_1 + a_2 + \ldots + a_n = b_1 + b_2 + \ldots + b_m$ *все слагаемые - целые числа и все, кроме, может быть, одного, делятся на целое d, то и это исключенное слагаемое делится на d.*

Замечание. Кажется естественной десятичная форма записи целых чисел. В различных ситуациях более удобными являются другие основания. К примеру, во всех компьютерах на микроуровне вычисления проводятся в двоичной системе счисления. Для перехода к ней с десятичной системы счисления используют промежуточную – 16-ричную систему счисления. Последняя широко применяется, в частности, в новом американском стандарте шифрования AES.

1.2. Наибольший общий делитель целых чисел. Алгоритм Евклида

Определение 1.2.1. *Если целые числа* $a_1, a_2, \ldots, a_n$ *делятся на целое число d, то d называют их общим делителем.*

В дальнейшем речь идет только о положительных целых делителях.

Определение 1.2.2. *Максимальный из общих делителей целых чисел* $a_1, a_2, \ldots, a_n$ *называется их наибольшим общим делителем и обозначается через* $НОД(a_1, a_2, \ldots, a_n)$ *или (если это не вызывает разночтений) через* $(a_1, a_2, \ldots, a_n)$.

Теорема 1.2.1. *Если* $a = b \cdot q + c$, *то* $НОД(a,b) = НОД(b,c)$.

Доказательство получается с помощью леммы 1.1.1. Пусть $d = НОД(a,b)$ и $k = НОД(d,c)$. В силу леммы 1.1.1 из делимости a и b на d следует, что и c делится на d. Таким образом, d – общий делитель чисел b и c. Следовательно, k делится на d. Но из равенства $a = bq + c$ следует, что a делится на k. Тогда и d делится k. Так как d и k являются натуральными, то отсюда следует, что $d = k$. Теорема доказана.

Это наблюдение (теорема 1.2.1) позволило Евклиду (примерно 2 300 лет тому назад) обосновать следующий факт (который является, по сути дела, кратным применением теоремы 1.2.1).

Теорема 1.2.2. *Наибольший общий делитель целых чисел a и b* $(a > b)$ *равен последнему отличному от нуля остатку цепочки равенств:*

$$a = b \cdot q_1 + r_1;$$
$$b = b \cdot q_2 + r_2;$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$r_{n-2} = r_{n-1} \cdot q_n + r_n;$$

$$r_{n-1} = r_n \cdot q_{n+1}; \quad m.\,e. \quad r_n = НОД(a,b).$$

Доказательство осуществляется $n-$кратным применением теоремы 1.2.1.

Теорема 1.2.2 непосредственно предоставляет алгоритм нахождения наибольшего общего делителя целых чисел, называемый алгоритмом Евклида.

Пример 1.2.1. С помощью алгоритма Евклида найти $НОД(72, 26)$.

Решение. В соответствии с теоремой 1.2.2 $72 = 26 \cdot 2 + 20$; $26 = 20 \cdot 1 + 6$; $20 = 6 \cdot 3 + 2$; $6 = 2 \cdot 3$. Следовательно, $НОД(72, 26) = 2$.

Алгоритм Евклида легко преобразуется в алгоритм нахождения наибольшего общего делителя не только двух, но и большего количества целых чисел. Алгоритм Евклида остается в классе самых быстрых алгоритмов нахождения наибольшего общего делителя целых чисел. Обратное применение цепочки равенств алгоритма Евклида доказывает следующий факт.

Теорема 1.2.3. *Если* $d = НОД(a,b)$, *то существуют такие целые* u *и* v, *что выполняется следующее соотношение* $d = au + bv$.

Полученное равенство называют соотношением Безу для наибольшего общего делителя целых чисел a и b.

Пример 1.2.2. Из примера 1.2.1 следует, что

$$2 = 20 + 6 \cdot (-3) = 20 + (26 + 20 \cdot (-1)) \cdot (-3) = 20 \cdot 4 + 26 \cdot (-3) =$$
$$= (72 + 26 \cdot (-2)) \cdot (4 + 26 \cdot (-3)) = 72 \cdot 4 + 26 \cdot (-11).$$

1.3. Простые числа

Определение 1.3.1. *Натуральное число* $p > 1$ *называется простым, если оно делится только на* 1 *и на себя.*

Очевидно, справедлива

Теорема 1.3.1. *Всякое натуральное число* $n > 1$ *либо является простым числом, либо имеет простой делитель.*

Заметим, что из соотношения $n = p \cdot q$ натуральных чисел, больших единицы, следует, что либо p, либо q принадлежит отрезку $\left[2; \sqrt{n}\right]$. Легко видеть, наименьший натуральный делитель $p > 1$ натурального числа $n > 1$ является простым числом. Исторически первый метод проверки натурального числа $n > 1$ на простоту заключается в делении его на

простые числа, не превосходящие $\sqrt{n}$. Данный метод носит название «решето Эратосфена» (III в. до н.э.). Вообще говоря, «решето Эратосфена» решает более общую задачу составления списка всех простых чисел на отрезке натурального ряда

$$1, 2, \ldots, n. \qquad (1.1)$$

Суть метода. Начиная с 4, вычеркиваем в (1.1) все четные числа; затем, начиная с 9, вычеркиваем все числа, кратные трем; затем, начиная с 25, все числа, кратные 5, и так далее до наименьшего простого числа p, такого, что $p > \sqrt{n}$. Кратные числу p из множества (1.1) уже вычеркнуты. Оставшиеся не зачеркнутыми в последовательности (1.1) числа будут представлять список всех простых чисел отрезка $[1, n]$.

К настоящему времени разработан достаточно большой цикл алгоритмов проверки числа на простоту. Лишь в августе 2002 г. группа индийских математиков конструктивно установила существование полиномиального алгоритма распознавания простоты натурального числа [6, 22].

Теорема 1.3.2 (Евклид, III в. до н.э.). *Простых чисел бесконечно много.*

Доказательство методом от противного. Предположим, что натуральный ряд содержит лишь конечное множество простых чисел: $p_1, p_2, \ldots, p_n$, $p_1 = 2, p_2 = 3, \ldots$. Составим с их помощью натуральное число $P = p_1 p_2 \cdot \ldots \cdot p_n + 1$. Согласно теореме 1.3.1, либо P – простое, либо содержит простой делитель. Но P не может быть простым, так как не совпадает ни с одним из чисел $p_1, p_2, \ldots, p_n$. Пусть q – простой делитель числа P. Тогда $P = qs = p_1 p_2 \cdot \ldots \cdot p_n + 1$. Число q не совпадает ни с одним из чисел $p_1, p_2, \ldots, p_n$. Иначе 1 делится на соответствующее p_i в соответствии с леммой 1.1.1, что невозможно. Получено противоречие с предположением, что доказывает теорему.

Замечание. При доказательстве данной теоремы вместо числа P можно было взять $P' = p_1 p_2 \cdot \ldots \cdot p_n - 1$ или $P'' = p_1 p_2 \cdot \ldots \cdot p_k + p_{k+1} p_{k+2} \cdot \ldots \cdot p_t$, возможны и иные варианты.

Значение простых чисел заключается в том, что они по теореме 1.3.1 являются составными кирпичиками всех натуральных чисел. Распределение простых чисел среди чисел натурального ряда достаточно непредсказуемо, о чем свидетельствуют следующие две теоремы.

Теорема 1.3.3 (Чебышев, 1852). *Между натуральными числами k и $2k$, $k > 1$, обязательно найдутся простые.*

Теорема 1.3.4. *Для всякого натурального n существует отрезок* $[k,\ k+n]$ *натурального ряда, все числа которого составные.*

Доказательство. В самом деле, все следующие числа составные: (n+2)!+2; (n+2)!+3;…;(n+2)!+(n+2). (Здесь $k!=1\cdot 2\cdot 3\cdot \ldots \cdot k$).

Несмотря на теорему 1.3.4, количество $\pi(x)$ всех простых чисел, меньших x, подчинено достаточно равномерному закону, высказанному в качестве гипотезы 15-летним Гауссом.

Теорема 1.3.5 (Адамар, Валле-Пуссен, 1896). $\pi(x)\approx \dfrac{x}{\ln x}$.

Любопытным фактом является

Теорема 1.3.6 (Эйлер, 1737). *Ряд* $\dfrac{1}{2}+\dfrac{1}{3}+\dfrac{1}{5}+\ldots$ *из обратных простых чисел – расходящийся.*

Замечание. Теорема 1.3.6 утверждает что сумма ряда равна ∞. Доказательство этой теоремы проводится с помощью аналитических средств – теории рядов и бесконечных произведений, его можно найти в [1, 21] – учебных пособиях А.К. Сушкевича, а также К. Айерленда и М. Роузена. Из этого доказательства следует другое доказательство бесконечности множества простых чисел. Частичные суммы ряда обратных простых чисел оцениваются следующей формулой: $\sum_{p\le n}\dfrac{1}{p}=\ln(\ln n)+c+O(1/(\ln n))$ для некоторой константы c. Частичная сумма по всем известным простым числам (примерно 50 млн [5]), меньше 4.

Отметим, что на конец XX века наибольшим известным простым числом было число $2^{6972593}-1$, открытое в 1999 г. Оно принадлежит классу так называемых чисел Мерсенна (имеющих вид 2^p-1, где $p-$простое). Проверка чисел Мерсенна на простоту производится гораздо проще (алгоритм Люка, см., например, [16]), чем произвольных натуральных чисел. Поэтому они и попадают в категорию рекордных.

Обобщением теоремы 1.3.2 является

Теорема 1.3.7 (Дирихле, 1837). *Всякая арифметическая прогрессия* $\{a+b\cdot n\}$, *где* $НОД(a,b)=1$, *содержит бесконечно много простых чисел.*

Доказательство требует мощных аналитических средств ([1,19]) а с точки зрения временных затрат – отдельного спецкурса.

К сожалению, больше в теории чисел аналогичных результатов нет. Попытки найти их составляют целые направления в теории чисел. Сформулируем несколько гипотез и открытых проблем (ОП) теории чисел в данном направлении.

ОП1. Бесконечно ли множество простых чисел Мерсенна? На сегодняшний день (начало 2005 г.) известно 29 простых чисел Мерсенна.

ОП2. Бесконечно ли много простых чисел Ферма, то есть чисел $F_n = 2^{2^m} + 1, \quad m = 0,1,2,...$? Еще Ферма показал, что $F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537$ – простые числа, и высказал предположение, что все числа F_n – простые. Лишь в 1732 г. Эйлер заметил, что F_5 – составное число.

ОП3. Бесконечно ли много простых чисел-близнецов, то есть пар простых чисел вида $p, p+2$? Примерами чисел-близнецов являются пары чисел 5 и 7, 17 и 19, 29 и 31, 41 и 43, 59 и 61, 71 и 73, 101 и 103, 107 и 109, 1997 и 1999 и так далее. Отметим, что в 1919 году Брун доказал, что даже в случае бесконечности пар чисел-близнецов ряд из обратных к ним – сходящийся [21].

ОП4 (Проблема Эйлера). Бесконечно ли много простых чисел – значений полинома $x^2 + x + 41$? Эйлер заметил, что при $x = 0,1,...,39$ полином дает простые числа. Однако уже $f(40) = 41^2$. Следующее утверждение снимает проблему поиска полиномов, принимающих только простые значения.

Теорема 1.3.8. *Никакая целая рациональная функция от x с целыми коэффициентами для всякого натурального x не будет равняться простому числу.*

1.4. Критерий взаимной простоты целых чисел

Определение 1.4.1. *Целые числа a и b называются взаимно простыми, если $НОД(a,b) = 1$.*

Это целые числа, не имеющие общих простых делителей. Развитием теоремы 1.2.3 является следующая

Теорема 1.4.1 (критерий взаимной простоты целых чисел). *Целые числа a и b взаимно просты тогда и только тогда, когда существуют такие целые u и v, что выполняется равенство $a \cdot u + b \cdot v = 1$.*

Доказательство. Необходимость утверждения, то есть существование требуемых целых чисел u и v доказана теоремой 1.2.3. Докажем достаточность утверждения методом от противного. Пусть выполняется равенство целых чисел $a \cdot u + b \cdot v = 1$. Если числа a и b имеют общий делитель $d > 1$, то в силу леммы 1.1.1 число 1 должно делиться на d, что невозможно. Таким образом, предположение о существовании у чисел a и b общего делителя $d > 1$ следует отбросить. Следовательно, $НОД(a,b) = 1$, что и требовалось доказать.

Следствие. *НОД*$(ac,b)=1$ *тогда и только тогда, когда* *НОД*$(a,b)=1$, *НОД*$(c,b)=1$.

Доказательство предоставляется читателю в качестве упражнения.

Важным в теории чисел и ее приложениях является следующее свойство взаимно простых чисел.

Лемма 1.4.1. *Пусть произведение целых чисел* ab *делится на целое число* c *и* *НОД*$(a,c)=1$. *Тогда* b *делится на* c.

Доказательство. Согласно критерию взаимной простоты целых чисел (теорема 1.4.1) имеет место равенство $au+cv=1$ для подходящих целых чисел u и v. Умножим это равенство на число b. Получим равенство $abu+bcv=b$. Левая часть этого равенства делится на c. Следовательно, в силу леммы 1.1.1, и правая часть равенства – число b делится на c. Лемма доказана.

1.5. Основная теорема арифметики

Такое название в теории чисел носит следующее утверждение.

Теорема 1.5.1. *Всякое целое число* $n>1$ *однозначно раскладывается в произведение простых множителей:* $n=p_1\cdot p_2\cdot\ldots\cdot p_s$.

Доказательство. Для малых значений n утверждение теоремы проверяется непосредственно. Пусть $n>1$ и предположим, что утверждение теоремы верно для всех натуральных чисел, меньших n. Согласно теореме 1.3.1 число n либо является простым (и тогда теорема доказана), либо делится на некоторое простое число p. Тогда $n=pm$ для натурального $m<n$. По предположению индукции число m раскладывается в произведение простых. Таким образом, доказано существование разложения всякого натурального числа в произведение простых множителей.

Единственность разложения доказывается методом от противного. Предположим, что натуральное число n имеет два различных разложения в произведение простых множителей:

$$n=p_1p_2\cdot\ldots\cdot p_s=q_1q_2\cdot\ldots\cdot q_t. \qquad (1.2)$$

Предположим, что $t\le s$. В силу леммы 1.1.1 левая часть этого равенства делится на q_1. Если *НОД*$(p_1,q_1)=1$, то согласно лемме 1.4.1 произведение $p_2p_3\cdot\ldots\cdot p_s$ делится на q_1. Рассуждая и далее аналогичным образом, найдем некоторый множитель p_k, делящийся на q_1, то есть найдем $p_k=q_1$. Сократим равенство (1.2) на этот общий множитель. Аналогично рассуждаем с $q_2,q_3,\ldots,q_t$. В конце концов придем к соотношению

$$p_1^* p_2^* \cdot \ldots \cdot p_{s-t}^* = 1, \qquad (1.3)$$

где p_i^*, $1 \le i \le s-t$, – несократившиеся простые множители левой части равенства (1.2). Но единица не может делиться ни на одно из простых чисел. Следовательно, $s = t$, и на самом деле равенство (1.3) имеет вид 1=1. Это и означает единственность разложения в произведение простых множителей с точностью до порядка следования этих множителей. Теорема доказана.

Если в равенстве $n = p_1 \cdot p_2 \cdot \ldots \cdot p_s$ собрать одинаковые множители, то получим следующее каноническое разложение целого числа:

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots p_t^{r_t}.$$

Пример 1.5.1. Приведем примеры канонических разложений целых чисел:

a) $196 = 2 \cdot 98 = 2 \cdot 2 \cdot 49 = 2^2 \cdot 7^2$; b) $2^{12}-1 = 4095 = 3^2 \cdot 5 \cdot 7 \cdot 13$.

По каноническому разложению целых чисел легко находится их наибольший общий делитель, наименьшее общее кратное, решаются иные задачи. Например, можно указать общую формулу всех натуральных делителей числа n, найти их количество, найти сумму $\sigma(n)$ всех натуральных делителей числа:
$\sigma(n) = ((p_1^{r_1+1}-1)/(p_1-1)) \cdot \ldots \cdot ((p_t^{r_t+1}-1)/(p_t-1))$ – детали см. в книге [1].

Следует отметить, что теорема 1.5.1 – это теорема существования. Она не дает метода факторизации натурального числа в произведение простых сомножителей. Поиск эффективного метода факторизации целых чисел оказался сложной алгоритмической проблемой, причем более сложной, чем распознавание простоты натурального числа. [1, 6, 10, 16, 22]. Ни один из имеющихся алгоритмов не является полиномиальным относительно n. Безуспешные и настойчивые поиски такого алгоритма приводят к убеждению, что задача факторизации целых чисел имеет экспоненциальную сложность. Данное обстоятельство, в частности, обеспечивает стойкость криптосистемы RSA (см. [10, 16]).

1.6. Сравнения

Теорема 1.6.1. *Пусть m – натуральное число, $m > 1$. Для любых целых чисел a и b следующие условия равносильны:*

1) a и b имеют одинаковые остатки от деления на m;

2) $a - b$ делится на m, то есть $a - b = mq$ для подходящего целого q;

3) $a = b + mq$ для некоторого целого q.

Доказательство проводится по схеме: $1) \Rightarrow 2) \Rightarrow 3) \Rightarrow 1)$. Из условия 1 следует условие 2: если $a = mq_1 + r$, $b = mq_2 + r$, то $a - b = m(q_1 - q_2)$, что означает делимость $a - b$ на m. Из условия 2 очевидным образом следует условие 3. Докажем, что из условия 3 следует 1). Если $b = ms + r$, то из равенства $a = b + mq$ получаем: $a = b + ms = mq + r + ms = m(q + s) + r$. Теорема доказана.

Определение 1.6.1. *Целые числа a и b называются сравнимыми по модулю m, если они удовлетворяют одному из условий теоремы 1. 6.1. Этот факт обозначают формулой $a \equiv b(\mathrm{mod}\, m)$ или $a \equiv b(m)$. Данное соотношение между целыми числами называют сравнением по модулю m.*

Пример 1.6.1. $-5 \equiv 7(\mathrm{mod}\ 4) \equiv 11(\mathrm{mod}\ 4) \equiv 23(\mathrm{mod}\ 4) \equiv 3(\mathrm{mod}\ 4)$.

Перечислим основные свойства сравнений.

Свойство 1. *Пусть $a \equiv b(\mathrm{mod}\, m)$. Тогда $(a \pm c) \equiv (b \pm c)(\mathrm{mod}\ m)$ для всякого целого c, то есть к обеим частям сравнения можно добавить (или вычесть из обеих частей) одно и то же число.*

Доказательство. $a \equiv b(\mathrm{mod}\, m)$ тогда и только тогда, когда $a - b = mq$ для подходящего целого q. Следовательно, $(a + c) - (b + c) = mq$, то есть $(a + c)$ и $(b + c)$ сравнимы друг с другом по модулю m.

Свойство 2. *Сравнения можно почленно складывать и вычитать: если $a \equiv b(\mathrm{mod}\, m)$, $c \equiv d(\mathrm{mod}\, m)$, то $(a + c) \equiv (b + d)(\mathrm{mod}\, m)$; $(a - c) \equiv (b - d)(\mathrm{mod}\, m)$.*

Доказательство аналогично предыдущему: если $a - b = mq$; $c - d = mt$, то $(a + c) - (b + d) = m(q + t)$. Следовательно, $(a + c) \equiv (b + d)(\mathrm{mod}\, m)$.

Свойство 3. *Сравнения можно почленно перемножать: если $a \equiv b(\mathrm{mod}\, m)$, $c \equiv d(\mathrm{mod}\, m)$, то $ac \equiv bd(\mathrm{mod}\, m)$.*

Доказательство. Согласно третьему условию теоремы 1.6.1 $a = b + mq$, $c = d + mw$ для подходящих целых q и w. Тогда $ac = bd + m(qd + bw + mqw)$. Согласно тому же третьему условию это означает, $ac \equiv bd(\mathrm{mod}\, m)$.

Свойство 4. *Сравнения можно почленно возводить в любую натуральную степень: если $a \equiv b(\mathrm{mod}\, m)$, то $a^n \equiv b^n(\mathrm{mod}\, m)$.*

Доказательство непосредственно вытекает из доказанного свойства 3.

Свойство 5. *Если в сравнении $a \equiv b(\mathrm{mod}\, m)$ числа a, b, m имеют общий множитель d, то на него сравнение можно сократить: $(a/d) \equiv (b/d)(\mathrm{mod}(m/d))$.*

Доказательство. Пусть $a = da_1$, $b = db_1$, $m = dm_1$. Согласно третьему условию теоремы 6.1 $a = b + mq$, то есть $da_1 = db_1 + dm_1 q$. Сократив данное равенство на d, получим равенство $a_1 = b_1 + m_1 q$, означающее сравнимость целых a_1 и b_1 по модулю m_1.

Свойство 6. *Сравнение можно сократить на общий множитель, взаимно простой с модулем: если* $a = da_1$, $b = db_1$, $НОД(d, m) = 1$, *то из сравнения* $da_1 \equiv db_1 (\mathrm{mod}\, m)$ *следует сравнимость* a_1 *и* b_1 *по модулю* m: $a_1 \equiv b_1 (\mathrm{mod}\, m)$.

Доказательство. По второму условию теоремы 6.1 $da_1 - db_1 = mv$ для подходящего целого v. Следовательно, произведение mv делится d. Поскольку $НОД(d, m) = 1$, то согласно лемме 1.5.1 целое v делится d: $v = dv_1$. Следовательно, $a_1 = b_1 + mv_1$, то есть $a_1 \equiv b_1 (\mathrm{mod}\, m)$, что и требовалось доказать.

Перечисленные свойства относятся к арифметическим свойствам сравнений. Сравнимость целых чисел по данному модулю m определяет бинарное отношение $R_{\mathrm{mod}\, m}$ на множестве целых чисел: два целых числа находятся в отношении $R_{\mathrm{mod}\, m}$, тогда и только тогда, когда они сравнимы друг с другом по модулю m. Легко проверяются следующие свойства названного бинарного отношения.

Свойство 7. *Рефлексивность:* $a \equiv a (\mathrm{mod}\, m)$ *для любого целого* a *и всякого натурального* $m > 1$.

Свойство 8. *Симметричность: если* $a \equiv b (\mathrm{mod}\, m)$, *то* $b \equiv a (\mathrm{mod}\, m)$.

Свойство 9. *Транзитивность: если* $a \equiv b (\mathrm{mod}\, m)$, $b \equiv c (\mathrm{mod}\, m)$, *то* $a \equiv c (\mathrm{mod}\, m)$.

Свойства 7–9 означают, что отношение сравнимости на множестве целых чисел Z есть отношение эквивалентности. Это означает, что Z разбивается на непересекающиеся классы попарно сравнимых друг с другом целых чисел по данному модулю. Каждый класс сравнимых друг с другом целых чисел характеризуется общими свойствами представителей этого класса. Например, все они имеют один и тот же остаток от деления на модуль; все они в силу теоремы 1.2.1 имеют одинаковый наибольший общий делитель с этим модулем.

1.7. Кольцо классов вычетов

При делении целых чисел на натуральное целое $m > 1$ существует m различных остатков: $0, 1, 2, ..., m-1$. Соответственно этим остаткам множество Z разбивается на m непересекающихся классов сравнимых

друг с другом чисел, имеющих, как отмечено в п. 1.6, один и тот же остаток. В соответствии с остатками от деления на m эти классы будем обозначать через $\bar{0},\bar{1},\dots \overline{m-1}$. Таким образом, класс $\bar{i} = \{mq + i \mid q \in Z\}$ для каждого целого $i = 0, 1, 2, ..., m-1$. Любой представитель класса однозначно определяет свой класс, то есть для каждого $mq + i$ класс $\overline{mq+i} = \bar{i}$. Поскольку остаток – по-латински residu – переводится на русский как вычет, то множество всех классов по данному модулю сравнимых друг с другом чисел называют множеством классов вычетов по модулю и обозначают через Z/mZ. В силу сказанного $Z/mZ = \{\bar{0}, \bar{1}, ..., \overline{m-1}\}$ – множество из m элементов. Заметим, что для любых классов $\bar{k}, \bar{l} \in Z/mZ$ и для произвольных $k_1, k_2 \in \bar{k}$, $l_1, l_2 \in \bar{l}$, суммы $k_1 + l_1$ и $k_2 + l_2$ принадлежат одному классу из Z/mZ, так как эти суммы сравнимы друг с другом по модулю m согласно свойству 2 сравнений. Аналогично произведения $k_1 \cdot l_1$ и $k_2 \cdot l_2$ лежат в одном классе из Z/mZ.

Определим операции сложения на Z/mZ. Полагаем суммой $\bar{k} \oplus \bar{l}$ такой единственный класс $\bar{z}$ из Z/mZ, в который попадают все суммы $k_1 + l_1$ и $k_2 + l_2$ для $k_1, k_2 \in \bar{k}$, $l_1, l_2 \in \bar{l}$, а произведением $\bar{k}\,\bar{l}$ – тот класс из Z/mZ, в который попадают произведения $\tilde{k} \cdot \tilde{l}$ для $\tilde{k} \in \bar{k}, \tilde{l} \in \bar{l}$.

Поскольку сложение и умножение в Z/mZ однозначно определяются умножением представителей классов, то свойства 1–5 операций сложения и умножения целых чисел справедливы и в Z/mZ:

1) $\bar{k} \oplus \bar{l} = \bar{l} \oplus \bar{k}$; $\bar{l}\,\bar{k} = \bar{k}\,\bar{l}$ – коммутативность;

2) $\bar{k} \oplus (\bar{l} \oplus \bar{r}) = (\bar{k} \oplus \bar{l}) \oplus \bar{r}$; $\bar{k}(\bar{l}\,\bar{r}) = (\bar{k}\,\bar{l})\bar{r}$ – ассоциативность;

3) существует нейтральный элемент: $\bar{k} \oplus \bar{0} = \bar{k}$; $\bar{k}\,\bar{1} = \bar{k}$;

4) для всякого $\bar{k} \in Z/mZ$ существует единственный класс $\bar{l}$, такой, что $\bar{k} \oplus \bar{l} = \bar{0}$, им является $\bar{l} = \overline{m-k}$;

5) $(\bar{k} \oplus \bar{l})\bar{r} = (\bar{k}\,\bar{r}) \oplus (\bar{l}\,\bar{r})$ – дистрибутивность.

Таким образом, Z/mZ является коммутативным кольцом с единицей.

Далее операции сложения и умножения в этом кольце будем обозначать стандартными символами «+» и «·».

Определение 1.7.1. *Элемент $\bar{k} \in Z/mZ$ называется обратимым, если найдется такой класс $\bar{l} \in Z/mZ$, что $\bar{k}\,\bar{l} = \bar{1}$. Тогда класс $\bar{l}$ называют обратным к классу $\bar{k}$.*

Из ассоциативности умножения в кольце Z/mZ вытекает, что если $\bar{k}$ обратимый класс, то обратный класс определен однозначно.

Лемма 1.7.1. *Пусть* $\overline{k} \in Z/mZ$ *такой класс, что* $НОД(k,m)=1$. *Тогда*

1) для каждого $\overline{l} \neq \overline{0}$ *произведение* $\overline{k}\,\overline{l} \neq \overline{0}$;

2) $\overline{k} \cdot \overline{l}_1 \neq \overline{k} \cdot \overline{l}_2$, *если* $\overline{l}_1 \neq \overline{l}_2$;

3) отображение $f : \overline{x} \to \overline{k} \cdot \overline{x}$ *инъективно и, следовательно, биективно на множестве* Z/mZ *(на множестве ненулевых элементов из* Z/mZ);

4) – обратимый класс в кольце Z/mZ.

Доказательство. Предположим, что в условиях леммы найдется класс $\overline{l} \neq \overline{0}$, такой, что $\overline{k} \cdot \overline{l} = \overline{0}$. Это означает, что произведение целых чисел kl делится на m. Поскольку k и m взаимно просты, то согласно лемме 4.1 l делится на m, то есть $\overline{l} = \overline{0}$. Полученное противоречие доказывает справедливость первой части леммы. Предположим, что найдутся такие различные классы $\overline{s}$ и $\overline{t}$, что $\overline{k} \cdot \overline{s} = \overline{k} \cdot \overline{t}$. Тогда по свойству дистрибутивности $\overline{k} \cdot (\overline{s} \oplus (\overline{-t})) = \overline{0}$ для ненулевого класса $(\overline{s} \oplus (\overline{-t})) = \overline{s-t} \neq \overline{0}$, что невозможно в силу доказанной первой части леммы. Из второй части утверждения непосредственно вытекают ее третья и четвертая части.

Замечание. Поскольку, согласно условию леммы 1.7.1, $НОД(d,m)=1$, то по критерию взаимной простоты существуют такие целые $u, v \in Z$, что $ku + mv = 1$. Тогда $\overline{1} = \overline{ku} + \overline{mv} = \overline{ku}$. Следовательно, $\overline{u}$ – обратный к $\overline{k}$ класс.

Лемма 1.7.2. *Пусть* $\overline{k} \in Z/mZ -$ *такой класс, что* $НОД(k,m) = d > 1$. *Тогда*

1) существует класс $\overline{l} \neq \overline{0}$, *что* $\overline{k}\,\overline{l} = \overline{0}$;

2) существуют классы $\overline{l}_1 \neq \overline{l}_2$, *такие, что* $\overline{k} \cdot \overline{l}_1 = \overline{k} \cdot \overline{l}_2$;

3) для всех $\overline{l} \neq \overline{0}$ *произведение* $\overline{k}\,\overline{l} \neq \overline{1}$, *то есть класс* $\overline{l}$ *необратим в кольце Z/mZ.*

Доказательство. В соответствии с выбором класса $\overline{k}$ существуют такие целые s и t, что $k = ds$, $m = dt$. Класс $\overline{t} \neq \overline{0}$, поскольку t не делится на m. Однако $\overline{k} \cdot \overline{t} = \overline{dst} = \overline{ms} = \overline{0}$. Для каждого целого $i, 1 \le i < t$, произведение $\overline{k} \cdot (\overline{i+t}) = \overline{k} \cdot \overline{i} \oplus \overline{k} \cdot \overline{t} = \overline{k} \cdot \overline{i}$. Если бы существовал такой класс $\overline{l} \neq \overline{0}$, что $\overline{k}\,\overline{l} = \overline{1}$, то тогда $\overline{t} \cdot \overline{k} \cdot \overline{l} = \overline{0} = \overline{t} \cdot \overline{1} = \overline{t}$, что противоречит доказанному: $\overline{t} \neq \overline{0}$. Следовательно, для всех $\overline{l} \neq \overline{0}$ произведение $\overline{k}\,\overline{l} \neq \overline{1}$. Лемма полностью доказана.

Теорема 1.7.1. *Класс* $\overline{k}$ *из кольца* Z/mZ *обратим тогда и только тогда, когда* $НОД(k,m)=1$. *Обратный класс также обратим. Произведение обратимых классов есть обратимый класс.*

Доказательство первой части теоремы непосредственно следует из лемм 1.7.1 и 1.7.2. Вторая часть вытекает из критерия взаимной простоты целых чисел. Если целые числа не имеют общих делителей с m, то общих делителей с m не будет и у их произведения в силу основной теоремы арифметики. Отсюда следует третья часть утверждения.

Следствие. *Если* $m=p-$ *простое число, то в кольце* Z/mZ *каждый ненулевой класс обратим.*

Поскольку Z/mZ состоит из конечного множества элементов, то сложение и умножение можно задавать поэлементно в виде таблиц.

Пример 1.7.1. Напишем таблицы сложения и умножения в кольце $Z/3Z$:

$\oplus$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\odot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Из таблицы умножения непосредственно видно, что классы $\overline{1}$ и $\overline{2}$ обратны сами себе, то есть обратимы все ненулевые классы $Z/3Z$ в полном соответствии с теоремой 7.1.

1.8. Малая теорема Ферма

Такое название в теории чисел и ее приложениях носит следующая

Теорема 1.8.1. *Пусть* $p-$*простое число и целое число* a *не делится на* p. *Тогда* $a^{p-1}\equiv 1(\mathrm{mod}\,p)$.

Доказательство. Согласно лемме 1.7.1 равны произведения $(\overline{a}\cdot\overline{1})\cdot(\overline{a}\cdot\overline{2})\cdot\ldots\cdot(\overline{a}\cdot\overline{n-1})=\overline{1}\cdot\overline{2}\cdot\ldots\cdot(\overline{n-1})$. Сократим это равенство на $\overline{2}\cdot\overline{3}\cdot\ldots\cdot\overline{n-1}$. Получим $\overline{a}^{p-1}=\overline{1}$. Это означает, что $a^{p-1}\equiv 1(\mathrm{mod}\,p)$.

Следствие 1. В *кольце* Z/pZ *с простым* p *обратным к классу* $\overline{k} \neq \overline{0}$ *является класс* $\overline{k}^{p-2}$.

Замечание. В соответствии с замечанием к лемме 1.7.1 класс $\overline{k}^{-1}$ можно найти обратной прогонкой алгоритма Евклида. Следствие дает конкурентный способ нахождения обратного класса. Он кажется громоздким, но свойства сравнений позволяют достаточно быстро вычислить остаток от деления k^{p-2} на p. Во-первых, от k можно перейти к остатку от деления k на p. Поэтому можно считать, что $1 < k < p$. Требуемую степень можно вычислить за $o(\log_2(p-2))$ умножений. Для этого можно представить $p-2$ в двоичной системе счисления.

Пример 1.8.1. Найдем остаток от деления 39^{29} на 31.

Решение. $39 \equiv 8 (\mathrm{mod}\, 31)$. Поэтому $39^2 \equiv 8^2 \equiv 2 (\mathrm{mod}\, 31)$. Двоичная запись: 29=11101. Следовательно, для любого натурального a величина $a^{29} = a^{2^4} \cdot a^{2^3} \cdot a^{2^2} \cdot a$. Далее, $39^4 \equiv 8^4 \equiv 2^2 (\mathrm{mod}\, 31)$. Поэтому $39^8 = (39^4)^2 \equiv 4^2 (\mathrm{mod}\, 31)$. Тогда $39^{16} = (39^8)^2 \equiv 16^2 (\mathrm{mod}\, 31) \equiv 8 (\mathrm{mod}\, 31)$. Таким образом, $39^{29} \equiv 8 \cdot 16 \cdot 4 \cdot 8 (\mathrm{mod}\, 31) \equiv 4 \cdot 4 \cdot 8 (\mathrm{mod}\, 31) \equiv 4 (\mathrm{mod}\, 31)$.

Следствие 2. *Если* $a^{m-1} \neq 1 (\mathrm{mod}\, m)$ *для некоторого натурального* a, $1 < a < m-1$, *то число* m *- составное.*

Этот факт часто используется в качестве теста проверки числа на простоту. Он позволяет установить наличие множителей данного числа m, не находя ни одного из таких множителей. Заметим, что из теста выброшено число $m-1$, поскольку $(m-1)^{m-1} \equiv 1 (\mathrm{mod}\, m)$ в силу формулы для бинома $(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k$.

Определение 1.8.1. *Нечетное натуральное число* n *называется псевдопростым по основанию* b *для некоторого целого* b, $1 < b < n-1$, *если* $b^{n-1} \equiv 1 (\mathrm{mod}\, n)$.

Лейбниц полагал, что псевдопростые числа на самом деле просты и использовал для проверки $b = 2$. Однако существует простой контрпример: $2^{340} \equiv 1 (\mathrm{mod}\, 341)$, хотя $341 = 11 \cdot 31$. Заметим, однако, что $3^{340} \equiv 56 (\mathrm{mod}\, 341)$.

Определение 1.8.2. *Нечетное натуральное число называется числом Кармайкла, если оно составное и псевдопростое по всем основаниям* b.

В 1912 г. Р.Д. Кармайкл впервые опубликовал примеры таких чисел (15 чисел), в частности, привел наименьшее из них $561 = 3 \cdot 11 \cdot 17$. Позже выяснилось, что характеризация чисел Кармайкла была получена 15-ю

годами ранее А. Корселтом.

Теорема 1.8.2 (Корселта). *Нечетное натуральное число n является числом Кармайкла тогда и только тогда, когда для каждого его простого делителя p выполнены следующие два условия:*

1) n не делится на p^2; 2) $n-1$ делится на $p-1$.

Доказательство см. в [10].

Числа Кармайкла встречаются довольно редко. Например, между 1 и 10^9 имеется 50 847 534 простых чисел и 646 чисел Кармайкла. Тем не менее имеет место следующий факт.

Теорема 1.8.3 (Альфорд, Гранвиль, Померанц (1994)). *Чисел Кармайкла бесконечно много.*

1.9. Функция Эйлера и теорема Эйлера

Определение 1.9.1. *Функция Эйлера – функция $\varphi(m)$ натурального аргумента m, которая каждому натуральному числу $m>1$ ставит в соответствие количество натуральных чисел, меньших m и взаимно простых с m.*

Эта функция обладает рядом мультипликативных свойств, облегчающих вычисление ее значений. Наиболее очевидным из них является

Свойство 1. *$\varphi(p)=p-1$ для каждого простого числа p.*

Свойство 2. *$\varphi(p^n)=p^n-p^{n-1}$ для каждого простого числа p и для произвольного натурального $n\geq 1$.*

Доказательство. При $n=1$ получаем свойство 1. Предположим, что утверждение справедливо для $n=k-1\geq 1$, то есть предполагаем верным утверждение, что $\varphi(p^{k-1})=p^{k-1}-p^{k-2}$, и докажем его для $n=k$. Итак, по предположению индукции среди натуральных чисел от 1 до p^{k-1} нетривиальные общие делители с p^k имеют p^{k-2} чисел: $p, 2p, ..., p^2, p^2+p, ..., p^{k-1}-p, p^{k-1}$. Тогда на отрезке $[p^{k-1}+1; 2p^{k-1}]$ невзаимно простыми с p^k будут числа $p^{k-1}+p, p^{k-1}+2p, ..., 2p^{k-1}-p, 2p^{k-1}$ и только они. Их количество по построению равно p^{n-1}. Точно так же рассуждаем с числами отрезков $[2p^{k-1}+1;3p^{k-1}];...;[(p-1)p^{k-1}+1; p^k]$. Таких отрезков p, на каждом из них p^{k-2} не взаимно простых с p^k чисел, а всего их будет $p\cdot p^{k-2}=p^{k-1}$. Отсюда следует требуемая формула.

Свойство 3. *Если $НОД(n,m)=1$, то $\varphi(n\cdot m)=\varphi(n)\cdot\varphi(m)$.*

Доказательство. Согласно следствию из теоремы 1.4.1 натуральное число взаимно просто с nm тогда и только тогда, когда оно взаимно просто и с n и с m. Определим количество натуральных чисел на отрезке $[1, nm]$, взаимно простых и с n, и с m. Для этого натуральные числа от 1 до nm расположим в виде следующей прямоугольной таблицы:

$$\begin{array}{cccccc}
1 & 2 & \dots & k & \dots & n \\
n+1 & n+2 & \dots & n+k & \dots & 2n \\
\dots & \dots & \dots & \dots & \dots & \dots \\
sn+1 & sn+2 & \dots & sn+k & \dots & (s+1)n \\
\dots & \dots & \dots & \dots & \dots & \dots \\
(m-1)n+1 & (m-1)n+2 & \dots & (m-1)n+k & \dots & mn
\end{array}$$

В первой строке этой таблицы имеется в точности $\varphi(n)$ чисел, взаимно простых с n. Отметим, что если одним из них является число k, то и все числа $k-$го столбца также взаимно просты с n. Следовательно, таблица содержит $m\varphi(n)$ чисел, взаимно простых с n. Отметим также, что числа $k-$го столбца (а их в каждом столбце ровно m) имеют попарно различные остатки от деления на m. Если бы для различных целых $t, s;\ 1 \le t < s \le m,$ выполнялось равенство $(sn+k)-(tn+k)=(s-t)n=mq$ для некоторого целого q, то натуральное число $s-t$, меньшее m, должно делиться на m, так как по условию $НОД(n,m)=1,$ что невозможно. Следовательно, каждый столбец содержит столько же взаимно простых с m чисел, сколько их имеется среди всевозможных остатков от деления на m, то есть $\varphi(m)$. Таким образом, в таблице имеется $\varphi(n)\cdot\varphi(m)$ чисел, взаимно простых и с n, и с m и, следовательно, взаимно простых с их произведением nm. Свойство доказано.

Свойство 4. *Если* $n = p_1^{s_1} p_2^{s_2} \cdot \dots \cdot p_t^{s_t}$ *– каноническое разложение числа* n, *то*

$$\varphi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdot\dots\cdot(1-\frac{1}{p_t}).$$

Пример 1.9.1. Вычислим $\varphi(48)$. Поскольку $48 = 3\cdot 2^4$, то согласно свойству 4

$\varphi(48) = 48\cdot(1-1/3)\cdot(1-1/2) = 16.$

Пример 1.9.2. Из теоремы 1.7.1 следует, что в кольце Z/mZ имеется в точности $\varphi(m)$ обратимых классов. Например, $\varphi(12)=4$. Значит, в кольце $Z/12Z$ имеется именно 4 обратимых элемента. Непосредственная проверка показывает, что этими классами являются $\overline{1}, \overline{5}, \overline{7}, \overline{11}.$

Теорема 1.9.1 (Эйлера). *Если для целого числа* a *и натурального* m $НОД(a,m)=1,$ *то* $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m).$

Доказательство аналогично доказательству малой теоремы Ферма.

Следствие. *В кольце* Z/mZ *с составным* m *всякий обратимый элемент* $\overline{k}$ *обладает свойствами:*

1) $\overline{k}^{\varphi(m)} = 1;$

2) обратным к $\overline{k}$ *является класс* $\overline{k}^{\varphi(m)-1}$.

2. Элементы теории групп

2.1. Понятие алгебраической системы

Предмет алгебраических исследований выкристаллизовывался на протяжении более тысячи лет. Об этом свидетельствуют факты истории. Точку по данному вопросу поставила группа Н. Бурбаки в 30-х гг. XX в. Это международная группа математиков, поставившая перед собой амбициозную задачу – изложить с единых позиций все богатство накопившихся к тому времени математических знаний. Плодом их труда явилась знаменитая серия книг «Элементы математики», не завершенная и до настоящего времени. В основу всей математики они положили теорию множеств. Критикуемый с разных сторон теоретико-множественный подход оказался в высшей степени плодотворным для математики XX в. Вслед за Н. Бурбаки математическое сообщество пришло к следующему соглашению.

Определение 2.1.1. *Алгебра – это математическая наука, изучающая алгебраические системы.*

Приведем необходимые определения и пояснения.

Определение 2.1.2. *Пусть* X *– непустое множество. Если на* X *задана одна или несколько алгебраических операций, то говорят, что* X *есть алгебраическая система с данными операциями.*

Более общее определение и основные свойства алгебраических систем приведены в [14]. Из всего спектра алгебраических операций наиболее применимыми оказались бинарные.

Определение 2.1.3. *Бинарной алгебраической операцией на множестве* X *называется всякое правило, по которому каждой упорядоченной паре* (x, y) *элементов* $x, y \in X$ *ставится в соответствие один вполне определённый элемент* z *из* X.

Обычно операции обозначаются знаками $*$, $\times$, $\bullet$, ϵ, $+$, $-$ и т.п. Воспользуемся первым из обозначений операции. Тот факт, что элемент z множества X является результатом бинарной операции $*$ над элементами $x, y \in X$ в указанном порядке обозначают равенством $z = x * y$.

Пример 2.1.1. $(Z, +, \cdot)$ – алгебраическая система целых чисел с операциями сложения и умножения, называемая кольцом целых чисел.

Алгебраические системы различают по операциям и свойствам этих операций.

Определение 2.1.4. *Алгебраическая система* $(X,*)$ *с одной алгебраической операцией* $*$ *на множестве* X *называется группоидом.*

Если у группоида $(X,*)$ *операция* $*$ *ассоциативна:* $a*(b*c)=(a*b)*c$, *то такую алгебраическую систему называют полугруппой.*

Моноидом $(X,*)$ *называют полугруппу с единицей или нейтральным элементом, т.е. таким элементом* n, *что* $n*x=x*n=x$ *для каждого* $x\in X$.

Пример 2.1.2. $(N,\cdot)$ – множество натуральных чисел с операцией умножения – моноид; $(N,+)$ – множество натуральных чисел с операцией сложения – полугруппа, а алгебраическая система $(N,-)$ – группоид.

Пример 2.1.3. R_3 – множество всех свободных векторов трехмерного пространства с операцией векторного умножения – группоид, но не полугруппа, поскольку операция векторного умножения, как известно, не ассоциативная.

Лемма 2.1.1. *Если в полугруппе имеется нейтральный элемент, то он один.*

Доказательство. Если n и n' – два нейтральных элемента в полугруппе $(X,\cdot)$, то $n=n\cdot n'=n'$. Лемма доказана.

В дальнейшем достаточно подробно будем рассматривать кольца, поля, тела – алгебраические системы с двумя бинарными алгебраическими операциями. А сейчас рассмотрим наиболее популярные в алгебре XX в. алгебраические системы с одной операцией – группы [8, 24].

2.2. Группы, их основные свойства и типы

Определение 2.2.1. *Моноид* $(X,*)$, *у которого каждый элемент обратим, то есть для всякого* $x\in X$ *существует* $y\in X$, *такой, что* $x*y=y*x=n$ *(тогда пишут* $y=x^{-1}$*), называется группой.*

Пример 2.2.1. Группами являются следующие моноиды: (Z,+); $\{\pm1,\cdot\}$; $(V_3,+)$ – множество классических векторов – направленных отрезков, выходящих из начала координат в пространство, с операцией сложения векторов.

Пример 2.2.2. Пусть M – непустое множество и $\Omega(M)$ – множество всех подмножеств множества M. На $\Omega(M)$ определены бинарные алгебраичес-кие операции объединения и пересечения множеств, дополнение одного множества до другого, которые традиционно обозначаются символами $\cup$ и $\cap$, $\setminus$ соответственно, а также производная от них алгебраическая операция – симметрическая разность $\overset{\bullet}{\longleftrightarrow}$. По определению для произвольных множеств $A,B\in\Omega(M)$ их симметрическая

разность $A \overset{\bullet}{\longleftrightarrow} B = (A \cup B) \setminus (A \cap B)$. Прямая проверка показывает, что следующие алгебраические системы $(\Omega(M), \cup)$, $(\Omega(M), \cap)$ являются моноидами, $(\Omega(M), \setminus)$ – группоидом, а $(\Omega(M), \overset{\bullet}{\longleftrightarrow})$ – группой.

Дадим независимое определение группы.

Определение 2.2.2. *Группой называется непустое множество G с определённой на нём бинарной алгебраической операцией $\bullet$, которая обладает свойствами:*

1) ассоциативность: $a \bullet (b \bullet c) = (a \bullet b) \bullet c$ для любых $a, b, c \in G$;

2) существует нейтральный элемент (единица), то есть такой элемент $e \in G$, что $g \bullet e = e \bullet g = g$ для каждого $g \in G$;

3) каждый элемент $g \in G$ имеет обратный, то есть такой элемент $h \in G$, что $g \bullet h = h \bullet g = e$.

В силу леммы 2.1.1 в любой группе единица определяется однозначно. Это свойство дополняет

Лемма 2.2.1. *В любой группе обратный к каждому элементу определен однозначно.*

Доказательство методом от противного. Предположим, что элемент g группы $(G, \cdot)$ имеет два различных обратных элемента f и h. Тогда $fgh = (fg)h = nh = h = f(gh) = fn = f$. Таким образом, $f = h$ в противоречие с предположением. Следовательно, обратный элемент определен однозначно.

Пример 2.2.3. (Q,+); (R,+); (C,+) множества всех рациональных, вещественных и, соответственно, комплексных чисел с операцией сложения. Это так называемые аддитивные группы (то есть группы относительно сложения). Исторически сложилось, что все аддитивные группы являются коммутативными.

Определение 2.2.2. *Абелевыми, или коммутативными, называют группы $(G, \bullet)$ со свойством*

4) $a \bullet b = b \bullet a$ для произвольных $a, b \in G$.

По исторической традиции нейтральный элемент аддитивной группы называют нулём и обозначают 0, а обратный элемент к a – противоположным и обозначают через $-a$.

К аддитивным относятся группы: $(M_{m \times n}(R), +)$ – множество прямоугольных $m \times n$ матриц с вещественными коэффициентами с операцией сложения матриц, $(P[x], +)$ – множество всех полиномов с вещественными коэффициентами и с операцией сложения, V_n – множество всех n-мерных векторов с вещественными коэффициентами и с операцией векторного сложения. Абелевыми являются все группы из примеров 2.2.1 и 2.2.2. Всякий линейный код является абелевой группой относительно операции сложения.

Пример 2.2.4. Мультипликативные группы – группы с операцией умноже-ния: $(Q^*,\cdot)$, $(R^*,\cdot)$, $(C^*,\cdot)$ и т.д., где $C^* = C \setminus \{0\}$, $R^* = R \setminus \{0\}$, $Q^* = Q \setminus \{0\}$.

По свойству 4 группы делятся на абелевы и неабелевы.

Пример 2.2.5. $GL_n(R)$ – множество квадратных матриц порядка $n > 1$ с вещественными коэффициентами и ненулевым определителем относительно операции матричного умножения является неабелевой группой.

По количеству элементов группы делятся на конечные и бесконечные.

Определение 2.2.3. *Порядком конечной группы называется количество элементов этой группы. Если G – конечная группа, то $|G|$ – ее порядок.*

Пример 2.2.6. Группа $(Z/nZ, \oplus)$ является конечной абелевой аддитивной группой из n элементов; в силу теоремы 1.7.1 множество $(Z/nZ)^*$ обратимых относительно умножения классов вычетов по модулю n, где n – натуральное число, большее единицы, образует группу порядка $\varphi(n)$. Алгебраическая система $(M_{m\times n}(Z/kZ),+)$ из $m \times n$ – матриц с операцией матричного сложения являются конечной абелевой группой порядка k^{mn}.

Замечание. В частном случае, при $m = 1$ группа $(M_{1\times n}(Z/kZ),+)$ состоит из k^n элементов. Ее называют пространством k-значных векторов и обычно обозначают через V_n. Они популярны в приложениях, в частности, в защите информации, особенно пространства двоичных векторов, то есть пространства V_n с координатами из $Z/2Z$.

Предложение 2.2.1. *Для каждого натурального n существует абелева группа порядка n, то есть группа из n элементов с коммутативной операцией умножения.*

Доказательство. Для каждого натурального $n > 1$ множество C_n комплексных корней n-й степени из 1, то есть чисел $Z_n = \exp(i2\pi k/n)$ для $k = 0, 1, \ldots, n-1$, образует коммутативную группу порядка n. Такой же является группа $(Z/nZ, \oplus)$ из примера 2.2.6.

Упражнение 2.2.1. Доказать, что все группы порядка $n \le 5$ являются абелевыми.

2.3. Подгруппы

Определение 2.3.1. *Подгруппой в группе $(G,\cdot)$ называется всякое непустое подмножество H элементов множества G, которое в свою очередь является группой относительно той же операции.*

Тот факт, что H есть подгруппа группы G отмечают так: $H \le G$ или $H < G$, если включение $H \subset G$ строгое.

Пример 2.3.1. Аддитивные группы целых, рациональных, вещественных и комплексных чисел образуют систему подгрупп: (Z,+)<(Q,+)<(R,+)<(C,+).

Пример 2.3.2. Для любых натуральных n и k из доказательства предложения 2.2.1 следует, что $C_n < C_{kn} < C^*$.

Пример 2.3.3. Подмножество всех целых чисел, делящихся на натуральное число $n > 1$, образует подгруппу в группе целых чисел с операцией сложения. Эту подгруппу обозначают через $(nZ,+)$. Следовательно, имеют место бесконечные цепочки аддитивных подгрупп типа (Z,+)>(2Z,+)>(4Z,+)>… .

Теорема 2.3.1 (Критерий подгруппы). *Непустое подмножество H группы $(G,\cdot)$ является подгруппой тогда и только тогда, когда для произвольных элементов $a, b \in H$ имеет место включение $a \cdot b^{-1} \in H$.*

Доказательство. Пусть H – подгруппа группы $(G,\cdot)$. Это означает, в частности, что H замкнута относительно операции умножения, определенной в группе $(G,\cdot)$. Следовательно, если $a, b \in H$, то b^{-1} принадлежит H, и произведение $a \cdot b^{-1}$ также принадлежит H. Обратно, пусть для произвольных элементов $a, b \in H$ имеет место включение $a \cdot b^{-1} \in H$. Тогда для $b = a$ элемент $a \cdot a^{-1} = e$ группы G принадлежит H. Далее, для $a = e$ и произвольного $b \in H$ произведение $e \cdot b^{-1} = b^{-1}$ принадлежит, по условию, подмножеству H. Ассоциативность операции справедлива для всех элементов группы G, а следовательно, и для всех элементов множества H. Таким образом, H удовлетворяет всем аксиомам группы. Теорема доказана.

Пример 2.3.4. В силу критерия в любой группе G подмножество $\{e\}$ из одного нейтрального элемента e этой группы является подгруппой.

Определение 2.3.2. *Подгруппа H группы G называется собственной, если $H \neq G$ и $H \neq \{e\}$.*

Пример 2.3.5. С помощью критерия легко убедиться, что $SL_n(R)$ – подмножество квадратных матриц порядка n с определителем, равным 1, образуют подгруппу в $GL_n(R)$. Действительно, для произвольных матриц $A, B \in SL_n(R)$ по свойствам определителей $\det(B^{-1}) = 1$ и $\det(AB^{-1}) = \det A \cdot \det(B^{-1}) = 1$. Следовательно, $AB^{-1} \in SL_n(R)$ и согласно критерию 2.3.1 $SL_n(R)$ является подгруппой в группе $GL_n(R)$.

Упражнение 2.3.1. Выяснить, являются ли подгруппой: а) объединение подгрупп; б) дополнение к подгруппе: в) симметрическая разность двух подгрупп; г) пересечение подгрупп.

Наиболее популярными подгруппами являются циклические, нормальные и центральные подгруппы. Переходим к их изучению.

2.4. Циклические подгруппы

Теорема 2.4.1. *Пусть a – фиксированный элемент произвольной группы G. Пусть $<a>=\{a^0=e,a,a^2,...,a^{-1},a^{-2},...\}$ – множество всевозможных степе-ней элемента a. Тогда $<a>$ – подгруппа группы G, причём абелева.*

Доказательство следует из критерия подгруппы: для произвольных $a^k, a^l \in <a>$ произведение $a^k \cdot a^{-l} = a^{k-l}$ принадлежит, очевидно, множеству $<a>$.

Определение 2.4.1. *Подгруппа $<a>$ из теоремы 2.4.1 называется циклической подгруппой группы G, порождённой элементом a. Если в группе G найдётся такой элемент b, что $G=<b>$, то такую группу называют циклической.*

Пример 2.4.1. Следующие группы являются циклическими: (Z,+) = <1>; (Z/nZ,+) = $<\bar{1}>$; $C_n = <Z_n>$ для $Z_n = \exp(i2\pi k/n)$.

Теорема 2.4.2. *Пусть элемент $a \in G$ обладает свойством: $a^n = e$ для некоторого целого n и $a^k \neq e$ для всех целых k, $1 \le k < n$. Тогда циклическая подгруппа $<a>$ имеет порядок n и $<a>=\{a,a^2,...,a^n=e\}$.*

Доказательство. Заметим, что для целых k, $1 \le k < n$, $(a^k)^{-1} = a^{n-k}$.

Определение 2.4.2. *Величина n из теоремы 2.4.2 называется порядком элемента $a \in G$. Если же для элемента $a \in G$ такого n не существует, то говорят, что элемент $a \in G$ имеет бесконечный порядок.*

Пример 2.4.2. Любое ненулевое целое число имеет бесконечный порядок в аддитивной группе целых чисел.

Пример 2.4.3. Возьмём матрицу $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL_2(R)$. Здесь $A^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$; $A^3 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$;… . Степени матрицы A попарно различны и образуют бесконечную последовательность. Определитель матрицы A равен 1 ≠ 0. $A^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$, $A^{-2} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$,… . Таким образом, циклическая подгруппа, порож-денная матрицей A в группе $GL_2(R)$, является бесконечной.

Пример 2.4.4. Матрица $H \in GL_2(R)$ вида $H = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ имеет степени $H^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$; $H^3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$; $H^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E$ – единичная матрица. Согласно теореме 2.4.2 подгруппа $<H>$ есть конечная подгруппа порядка четыре.

Упражнение 2.4.1. Пусть элементы a и b абелевой группы имеют порядки m и k соответственно. Показать, что произведение ab является элементом этой же группы порядка $d = НОК(m,k)$, где $НОК(m,k)-$ наименьшее кратное натуральных чисел m и k.

Упражнение 2.4.2. Доказать, что мультипликативная группа рациональных чисел не является циклической.

Из определения циклической группы следует, что она содержит счетное или конечное множество элементов и во втором случае имеет четкую структуру, выражаемую теоремой 2.4.2. Отметим другие основные свойства циклических групп.

Теорема 2.4.3. *Всякая циклическая группа абелева.*

Доказательство очевидно.

Теорема 2.4.4. *Всякая подгруппа циклической группы является циклической.*

Доказательство. Пусть $G =< a >$ и $H -$произвольная собственная подгруппа этой группы. Тогда найдется натуральное k, такое, что $a^k \in H$. Следовательно, найдется наименьшее натуральное k, такое, что $a^k \in H$. Тогда для всякого $h \in H$ справедливо соотношение: $h = (a^k)^l$ для подходящего целого l. Как элемент циклической группы G элемент $h = a^s$ для некоторого целого s. По теореме о делении с остатком $s = kq + r$ для подходящих целых q, r, $0 \le r < k$. Тогда $h = (a^k)^q \cdot a^r$. Следовательно, $a^r = h \cdot (a^k)^{-q} \in H$, что противоречит минимальности k. Значит, $r = 0$ и $h = (a^k)^q$, следовательно, выполняется равенство $H =< a^k >$. Таким образом $H -$циклическая группа. Теорема доказана.

Итак, в любой группе много циклических подгрупп: каждый элемент порождает свою циклическую подгруппу. Тем не менее следует заметить, что чаще группы циклическими не являются. Например, все некоммутативные группы не могут быть циклическими. Циклическими не являются аддитивные и мультипликативные группы вещественных и комплексных чисел в силу их несчетности. Множество рациональных чисел счетно, то есть равномощно множеству целых чисел. Однако абелева группа (Q,+) в отличие от группы $(Z,+)$ (пример 2.4.1) также не циклична, ведь для каждого рационального числа $q = \frac{n}{m} \in Q$ подгруппа $< q >= \{0; \pm\frac{n}{m}; \pm\frac{2n}{m}; \pm\frac{3n}{m}; ...\}$ не содержит рациональных несократимых дробей $\frac{r}{s}$, $r \in Z, s \in N$, у которых знаменатель $s > m$, следовательно, $< q > \neq (Q,+)$.

В доказательстве предложения 2.2.1 обе конечные абелевы группы на самом деле являются циклическими согласно примеру 2.4.1. Однако существуют конечные коммутативные и нециклические группы.

Упражнение 2.4.3. Показать, что мультипликативная группа $Z/8Z^*$ абелева, но не циклична, а $Z/9Z^*$ – циклична.

В отличие от составного модуля n группы Z/pZ^* для простых p в определенном смысле одинаковы.

Теорема 2.4.5. *Для каждого простого числа p мультипликативная группа Z/pZ^* содержит $p-1$ элементов и является циклической.*

Доказательство следует из более общего факта, который будет доказан в четвертом разделе.

Проблема нерешенная [14]**:** конечно или бесконечно множество простых чисел p, для которых $Z/pZ^* = <\overline{2}>$, т. е. мультипликативная группа Z/pZ^* совпадает с циклической подгруппой, порожденной классом вычетов $\overline{2}$?

2.5. Смежные классы по подгруппе

Определение 2.5.1. *Пусть H – собственная подгруппа группы $(G,\cdot)$. Пусть $a \in G$. Через aH обозначим множество элементов $\{ah | h \in H\}$ и назовем его левым смежным классом группы G по подгруппе H.*

Если существует $b \in G$, $b \notin H \cup aH$, можно построить новый левый смежный класс bH и так далее. Аналогично строят правые смежные классы. Если каждый левый смежный класс совпадает с правым: $aH = Ha$, то тогда смежные классы называют двусторонними. Такими являются смежные классы в любой абелевой группе G. Смежные классы обладают рядом важных свойств, которые отражает

Теорема 2.5.1. *Пусть H – собственная подгруппа группы G. Тогда:*

1) каждый элемент $g \in G$ принадлежит какому-нибудь левому смежному классу по подгруппе H;

2) два элемента $a,b \in G$ принадлежат одному левому смежному классу тогда и только тогда, когда $a^{-1} \cdot b \in H$;

3) любые два левых смежных класса либо не пересекаются, либо совпадают;

4) для всякого $a \in G$ мощности множеств aH и H совпадают;

5) G есть объединение попарно непересекающихся левых (правых) смежных классов по подгруппе H.

Доказательство. Первое утверждение очевидно: поскольку любая подгруппа H содержит нейтральный элемент, то каждый элемент $g \in G$ принадлежит порожденному им смежному классу gH.

Докажем второе свойство. Пусть элементы $a,b \in G$ принадлежат одному смежному классу gH. Следовательно, $a = gh_1$, $b = gh_2$ для подходящих $h_1, h_2 \in H$. Тогда $a^{-1}b = (h_1^{-1}g^{-1}) \cdot (gh_2) = h_1^{-1}(g^{-1}g)h_2 = h_1^{-1}h_2 \in H$, что и требовалось доказать.

Докажем третье свойство. Предположим, что смежные классы aH и cH имеют общий элемент d. В таком случае $d = ah_1 = ch_2$ для подходящих $h_1, h_2 \in H$. Следовательно, $a = ch_2 h_1^{-1} = ch_3$. Отсюда следует, что $aH \subseteq cH$. Но точно так же доказывается обратное включение. Следовательно, $aH = cH$.

Докажем четвёртое свойство о равномощности различных смежных классов по данной подгруппе. Отображение $\varphi_a : h \to ah$ устанавливает взаимно однозначное соответствие между классами смежности H и aH. Действительно, отображение φ_a сюръективно, как нетрудно видеть. Также φ_a инъективно: если бы $ah_1 = ah_2$, то тогда $a^{-1}(ah_1) = a^{-1}(ah_2)$, следовательно, $h_1 = h_2$. Таким образом, φ_a – биективное, т.е. взаимно однозначное соответствие между смежными классами.

Пятое утверждение после доказанных свойств становится очевидным. Таким образом, теорема полностью доказана.

Пример 2.5.1. Пусть $G = M_{1\times 4}(Z/2Z)$ – множество всевозможных строк-матриц с четырьмя координатами из $Z/2Z$. Это группа по сложению (см. пример 2.2.5). Обычно ее обозначают через V_4. Легко проверить, что множество

$$H = \left\{ \underbrace{(0\ \ 0\ \ 0\ \ 0)}_{\overline{0}}, \underbrace{(1\ \ 0\ \ 1\ \ 1)}_{e_1}, \underbrace{(0\ \ 1\ \ 0\ \ 1)}_{e_2}, \underbrace{(1\ \ 1\ \ 1\ \ 0)}_{e_1 \cdot e_2} \right\}$$

образует подгруппу в группе V_4. Очевидно, |G|=2^4=16, |H|=4. Согласно теореме 2.5.1 группа G представляет собой объединение четырёх смежных классов по подгруппе H. Эти классы представлены в таблице.

Смежные классы группы G по подгруппе H

№	Класс a+H	$\overline{a} + \overline{0}$	$\overline{a} + \overline{e}_1$	$\overline{a} + \overline{e}_2$	$\overline{a} + (\overline{e}_1 + \overline{e}_2)$
1	$\overline{0} + H = H$	(0000)	(1011)	(0101)	(1110)
2	(1000)+H	(1000)	(0011)	(1101)	(0110)
3	(0100)+H	(0100)	(1111)	(1001)	(1010)
4	(0010)+H	(0010)	(1001)	(0111)	(1100)

Лемма 2.5.1. *Пусть H – собственная подгруппа группы G. Мощности множеств всех левых и соответственно правых смежных классов группы G по подгруппе H равны.*

Доказательство. Построим соответствие между названными множествами по правилу $gH \leftrightarrow Hg$. Очевидно такое соответствие является взаимно однозначным, что и доказывает лемму.

Доказанное утверждение позволяет ввести следующее

Определение 2.5.2. *Индексом подгруппы H в группе G называется мощность множества всех смежных классов группы G по данной подгруппе и обозначается через $|G:H|$.*

Пример 2.5.2. Индекс подгруппы $(nZ,+)$ в группе $(Z,+)$ равен n. Действительно, в данном случае множество всех смежных классов есть множество $\{nZ, 1+nZ, 2+nZ, \ldots, (n-1)+nZ\}$.

Замечание. Таблицы смежных классов играют важную роль в теории и практике помехоустойчивого кодирования. Простейший метод коррекции ошибок базируется на основе таблиц смежных классов, аналогичных приведенной выше. В современных цифровых каналах связи принято информацию передавать в виде двоичных блоков с определенной фиксированной длиной n, то есть n-мерных векторов с координатами из $Z/2Z$. Они получаются разбиением исходной информации, уже преобразованной в двоичный текст, на блоки по k двоичных символов, $k<n$. К каждому k-мерному блоку присоединяется специальным образом $n-k$ проверочных разрядов. В результате предназначенные для передачи слова принадлежат некоторому k-мерному подпространству H пространства V_n всех n-мерных векторов. С точки зрения теории групп H – подгруппа аддитивной группы V_n. Ее называют группой кодовых слов. В процессе передачи по каналу связи конкретного кодового слова $\overline{h}$ может наложиться «шум» – некоторый n-мерный двоичный вектор $\overline{e} \in V_n$. Тогда принятое по каналу связи слово-сообщение $\overline{x} = \overline{h} + \overline{e}$ является одним из элементов таблицы смежных классов группы V_n, образующая смежного класса и есть наложившийся в процессе передачи на $\overline{h}$ вектор ошибок $\overline{e}$. Если мы имеем в своем распоряжении таблицу смежных классов группы V_n по подгруппе H, то по полученному $\overline{x}$ мы легко определяем вектор ошибок $\overline{e}$ (первый элемент строки, содержащей $\overline{x}$) и истинное сообщение $\overline{h}$ (первый элемент столбца, в который попадает $\overline{x}$).

2.6. Теорема Лагранжа

К важнейшим в теории групп относится следующая теорема.

Теорема 2.6.1 (Лагранжа). *Порядок конечной группы делится на порядок любой ее подгруппы.*

Доказательство. Пусть H – подгруппа конечной группы G. Пусть $|G| = n$, $|H| = m$. Согласно теореме 2.5.1 группа G есть объединение непересекающихся смежных классов (левых или правых) по подгруппе H, каждый мощностью m. Пусть имеется всего k различных классов. Тогда $n = km$. Следовательно, $|G|$ делится $|H|$, что и требовалось доказать.

Следствие 1. *В конечной группе индекс подгруппы равен частному от деления порядка группы на порядок подгруппы.*

Следствие 2. *Любая группа простого порядка является циклической и не содержит собственных подгрупп.*

Пример 2.6.1. Всякая группа, порядок которой равен одному из следующих чисел: 1949, 1951, 1973, 1979, 1987, 1993, 1997, 1999, 2003, 2011, 2017, является циклической.

Следствие 3. *Если G – конечная группа из n элементов, то для каждого $a \in G$ $a^n = e$. Другими словами, в конечной группе порядок любого ее элемента делит порядок самой группы.*

В связи с теоремой Лагранжа возникает следующий вопрос: существует ли для всякого делителя m порядка n конечной группы G подгруппа H порядка m? В дальнейшем будет показано, что ответ на данный вопрос отрицателен. Тем не менее для циклических групп ответ положителен.

Теорема 2.6.2. *В циклической группе G для каждого делителя m порядка $|G|$ найдется подгруппа из m элементов.*

Доказательство. По условию $G = < b >$ для подходящего элемента $b \in G$. Это означает, что $n = |G|$ – наименьшее натуральное число, для которого $b^n = e$. Пусть $k = n : m$ и $c = b^k$. Тогда подгруппа $< c >$ имеет порядок m. В самом деле, $c^m = (b^k)^m = b^{km} = b^n = e$. Если бы $c^r = e$ для натурального $r < m$, то тогда $b^{kr} = e$ для натурального числа $kr < n$, что противоречит выбору b. Таким образом, $|< c >| = m$. Теорема доказана.

2.7. Нормальные подгруппы

Определение 2.7.1. *Собственная подгруппа H группы G называется нормальной, если для всякого $a \in G$ $a \cdot H = H \cdot a$, то есть каждый левый смежный класс по подгруппе H совпадает с правым смежным классом. В этом случае пишут* $H \lhd G$.

Ясно, что у абелевых групп все подгруппы нормальные. Очевидно, всякая подгруппа индекса 2 является нормальной.

Теорема 2.7.1. $H \lhd G$ *тогда и только тогда, когда для каждого $a \in G$ $aHa^{-1} = H$.*

Доказательство. Пусть для всякого $a \in G$ $a \cdot H = H \cdot a$, то есть для каждого $h \in H$ существует такой $h_1 \in H$, что $ah = h_1 a$. Тогда $h_1 = aha^{-1}$. Следовательно, $aHa^{-1} \subseteq H$. С другой стороны, для каждого $h \in H$ существует такой элемент $h_2 \in H$, что $ah_2 = ha$ или $h = ah_2 a^{-1}$. Следовательно, $H \subseteq aHa^{-1}$. Таким образом, $aHa^{-1} = H$. Обратное утверждение очевидно: если $aHa^{-1} = H$, то $aH = Ha$.

Пример 2.7.1. Подгруппа $SL_n(R)$ является нормальной подгруппой группы $GL_n(R)$, поскольку для всякой матрицы $B \in SL_n(R)$ и произвольной матрицы $A \in GL_n(R)$ $\det(ABA^{-1}) = \det(A) \cdot \det(B) \cdot \det(A^{-1}) = \det(B) = 1$.

Известно, что в группе $GL_n(R)$ для всякой матрицы B, отличной от скалярной, циклическая группа $< B >$ не является нормальной подгруппой.

Упражнение 2.7.1. Показать, что циклическая группа $< B >$ для матрицы $B = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$ не принадлежит классу нормальных подгрупп группы $GL_2(R)$.

2.8. Симметрическая группа

Пусть Ω – конечное множество из n элементов. Поскольку природа его элементов для нас несущественна, удобно считать, что $\Omega = \{1,2,\ldots,n\}$. Всякая биекция, то есть взаимно однозначное отображение Ω в себя называется подстановкой на Ω. Подстановку $f : i \to f(i)$, $i = 1,2,\ldots,n$, удобно изображать в развернутой и наглядной форме в виде двустрочной таблицы: $f = \begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}$. В этой таблице каждый i-й столбец четко указывает в какой элемент $f(i)$ преобразуется элемент i, $1 \le i \le n$.

Подстановки перемножаются в соответствии с общим правилом композиции отображений: $(gf)(i) = g(f(i))$.

Пример 2.8.1. Пусть $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$; $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$. Тогда

$$fg = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = f \begin{matrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 3 & 2 & 1 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 4 & 3 & 2 \end{matrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.$$

Вычислим $gf = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$. Как видим $gf \neq fg$, то есть композиция подстановок не обладает свойством коммутативности. Очевидно, тождественная подстановка $e = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$ играет роль единицы относительно композиции подстановок. Как известно, композиция отображений является ассоциативной операцией, поэтому и композиция подстановок ассоциативна. Каждая подстановка – обратимая операция. Чтобы найти для подстановки f обратную подстановку f^{-1}, достаточно в таблице $\begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}$ переставить строки местами, а затем столбцы упорядочить по возрастанию элементов первой строки.

Пример 2.8.2. Для подстановки $f=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$ найдем обратную под-становку f^{-1}. $f^{-1}=\begin{pmatrix}2&3&4&1\\1&2&3&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}$. Чтобы убедиться в правиль-ности, найдем их композицию:

$$f^{-1}f=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}=e.$$

Таким образом, подстановки на Ω образуют группу с операцией композиции подстановок.

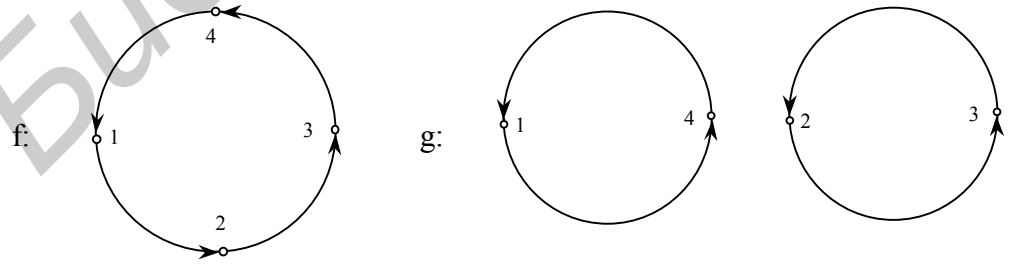
Определение 2.8.1. *Симметрической группой степени n называют группу подстановок на n элементах относительно операции умножения подстановок (композиции отображений) и обозначают через S_n.*

Теорема 2.8.1. *Порядок группы S_n равен $n!$*

Доказательство методом математической индукции. При $n=2$ на множестве $\Omega=\{1,2\}$ существует в точности $2!=2$ различных подстановок – это тождественная подстановка e и подстановка f, такая, $f(1)=2,\quad f(2)=1.$ Предположим по индукции, что $|S_{n-1}|=(n-1)!$ Перечислим все возможные подстановки на $n-$элементном множестве. В качестве $f(1)$ можно взять любой из элементов множества $\Omega=\{1,2,...,n\}$. На долю остальных значений остается по предположению индукции $(n-1)!$ возможностей. Таким образом, $|S_n|=n(n-1)!=n!,$ что и требовалось доказать.

Пример 2.8.2. В силу теоремы 2.8.1 $|S_2|=2;\quad |S_3|=6;\quad |S_4|=24;\quad |S_5|=120.$

Разложим подстановки из S_n в произведение более простых подстановок. Идею разложение поясним на примере подстановок f и g, указанных выше.



Подстановка f кратко записывается в виде $f=(1,2,3,4)$ или, если это не вызывает разночтений, в виде $f=(1234)$ и носит название цикла длиной 4, а подстановка g записывается в виде $g=(14)(23)$ произведения двух независимых (непересекающихся) циклов (14) и (23) длиной два.

Перейдем к общему случаю. Пусть S_n – произвольная симметрическая

группа степени n и f – произвольный элемент из S_n. Пусть $\Gamma_f =< f >$ – циклическая подгруппа, порожденная подстановкой f. Элементы $i, j \in \Omega = \{1,2,\ldots,n\}$ назовем Γ_f-эквивалентными, если найдется подстановка $g = f^k$ для подходящего целого k, что $g(i) = j$. Тогда $g^{-1}(j) = i$. Очевидно, отношение Γ_f-эквивалентности рефлексивно, транзитивно, симметрично. Тогда Ω разбивается на попарно непересекающиеся классы Γ_f-эквивалентных друг другу элементов, называемых f-орбитами, или Γ_f-орбитами: $\Omega = \Omega_1 \cup \ldots \cup \Omega_p$. Каждая точка $i \in \Omega$ принадлежит в точности одной f-ор-бите, и если $i \in \Omega_k$ то Ω_k состоит из образов точки i при действии степеней f: $i, f(i), f^2(i),..., f^{t-1}(i)$, где $t = t_k = |\Omega_k|$ – длина f-орбиты Ω_k. Очевидно, $t_k \le |< f >|$ – порядок подгруппы $< f >$. Ясно, что $f^t(i) = i$, причем $t = t_k$ – наи-меньшее натуральное число с таким свойством.

Положим $f_k = (i, f(i), \ldots, f^{t_k-1}(i)) = \begin{pmatrix} i & f(i) & \ldots & f^{t_k-1}(i) \\ f(i) & f^2(i) & \ldots & i \end{pmatrix}$. Тем самым получим подстановку, называемую циклом длиной t_k, действующую тождественно на остальные элементы из Ω. Вопрос вкуса и удобства – писать
(1 2 ….. m) или (1,2,…,m). Итак, f_k действует как f на Ω_k и тождественно на $\Omega \setminus \Omega_k$. Это дает основание считать циклы f_k и f_l, $k \ne l$, независимыми или непересекающимися (так как они действуют на непересекающихся множествах). Таким образом, разбиению $\Omega = \Omega_1 \cup \ldots \cup \Omega_p$ соответствует разложение в произведение $f = f_1 f_2 \ldots f_p$, при этом циклы-сомножители перестановочны.

Естественно в произведении $f = f_1 f_2 \ldots f_p$ опускать сомножители, соответствующие Ω_i из одного элемента, так как $f_i = e$ – тождественная подстановка на Ω.

Например, $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix} \in S_8$ можно записать в виде произведения циклов $f = (12345)(67)(8) = (12345)(67)$.

Итогом проведенных рассуждений является

Теорема 2.8.2. *Каждая подстановка $f \in S_n$, $f \ne l$, является произведением независимых циклов длиной $l \ge 2$. Это разложение в произведение определено однозначно с точностью до порядка следования циклов.*

Следствие. *Порядок подстановки $f \in S_n$ (равный порядку циклической группы Γ_f) равен наименьшему общему кратному длин независимых циклов, входящих в разложение f.*

Доказательство следует из коммутативности умножения независимых

циклов и того факта, что каждый цикл $f=(i_1 i_2 ... i_k)$ является подстановкой порядка k, иными словами, $k-$наименьшее натуральное число, для которого $f^k = e.$

Определение 2. 8.2. *Цикл длиной 2 называется транспозицией.*

Теорема 2.8.3. *Каждая подстановка $f \in S_n$ раскладывается в произве-дение транспозиций.*

Доказательство. Согласно теореме 2.8.2 f раскладывается в произведение независимых циклов. Каждый цикл раскладывается в произведение транспозиций. Примером такого разложения является следующее легко проверяемое равенство: $(i_1\ i_2 \dots\ i_k) = (i_1\ \ i_k)\cdot(i_1\ i_{k-1})\cdot\dots\cdot(i_1\ i_3)\ (i_1\ i_2).$

Пример 2.8.4. Разложить в произведение циклов и транспозиций подстановку

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 5 & 3 & 1 & 7 & 9 & 6 & 8 \end{pmatrix}.$$

Решение.

$$g = (1\ \ 2\ \ 3\ \ 5)(6\ \ 7\ \ 9\ \ 8) = (1\ \ 5)(1\ \ 3)(1\ \ 2)(6\ \ 8)(6\ \ 9)(6\ \ 7).$$

Разложение подстановки в произведение транспозиций неоднозначно. К примеру, вышеприведенную подстановку можно представить в виде иного, следующего произведения транспозиций:

$$g = (1\ \ 5)(1\ \ 3)(1\ \ 2)(6\ \ 8)(3\ \ 4)(6\ \ 9)(3\ \ 4)(6\ \ 7).$$

Тем не менее справедливо следующее утверждение.

Теорема 2.8.4. *Любые два разложения данной подстановки в произведе-ние транспозиций содержат либо четное число сомножителей, либо нечетное.*

Доказательство использует следующее утверждение.

Лемма 2.8.1. *Если $f = \tau_1\tau_2\cdot\ldots\cdot\tau_k -$разложение подстановки в произведе-ние транспозиций, то обратная подстановка $f^{-1} = \tau_k\tau_{k-1}\cdot\ldots\cdot\tau_1.$*

Доказательство леммы осуществляется непосредственным перемножением данных произведений транспозиций с учетом того, что квадрат каждой транспозиции τ равен $e.$

Доказательство теоремы 2.8.4 проведем методом от противного. Предположим, что подстановка f имеет два разложения в произведения транспозиций различной четности. Тогда тождественная подстановка $e = f^{-1}f = \tau_1\tau_2\cdot\ldots\cdot\tau_m -$разложение в произведение транспозиций с нечетным числом сомножителей $m = 2s+1.$ В этом произведении две транспозиции всегда можно сократить. Это так, если рядом стоят две одинаковые транспозиции, как отмечено в доказательстве леммы 2.8.1. Если же в данном произведении нет одинаковых рядом стоящих транспозиций, то перестановкой транспозиций можно добиться требуемой ситуации. В самом деле, если рядом стоят независимые транспозиции, то их можно переставить местами; если рядом стоят транспозиции вида $\tau_l\tau_{l+1} = (su)(st),$ то такое

произведение можно преобразовать следующим образом: $(su)(st)=(st)(ut)$. Действительно, легко убедиться, что обе части этого равенства равны одной и той же подстановке $g=\begin{pmatrix} s\ t\ u \\ t\ u\ s \end{pmatrix}$. Если же $\tau_l\tau_{l+1}=(ut)(st)$, то это произведение можно преобразовать так: $(ut)(st)=(su)(ut)$, ведь обе части равенства равны подстановке $h=\begin{pmatrix} u\ s\ t \\ t\ u\ s \end{pmatrix}$.

В результате таких преобразований обязательно встретятся одинаковые транспозиции, иначе получим равенство $e=(st)\tau_1\tau_2\cdot\ldots\cdot\tau_k$, где произведение $\tau_1\tau_2\cdot\ldots\cdot\tau_k$ не содержит s. Но тогда произведение $(st)\tau_1\tau_2\cdot\ldots\cdot\tau_k$ не может быть тождественной подстановкой. Получено противоречие с исходным предположением, что завершает доказательство.

Определение 2.8.3. *Подстановка f называется четной (нечетной), если ее разложение в произведение транспозиций содержит четное (нечетное) количество сомножителей.*

2.9. Знакопеременная группа

Теорема 2.9.1. *Все четные подстановки группы S_n образуют подгруппу A_n порядка* $0{,}5n!$.

Доказательство. Произведение четных подстановок является четной подстановкой. A_n содержит, очевидно, тождественную подстановку и в силу леммы 2.8.1 вместе с каждым своим элементом f множество A_n содержит и обратный элемент f^{-1}. Следовательно, A_n – подгруппы группы S_n.

Смежный класс $(12)A_n$ принадлежит подмножеству $H_н$ всех нечетных подстановок. Значит, $|A_n|\le|H_н|$. С другой стороны, преобразование $\varphi: f\to(12)f$ инъективно отображает множество $H_н$ в A_n. Значит, $|A_n|\ge|H_н|$. Таким образом, $|A_n|=0{,}5|S_n|$, что и требовалось доказать.

Следствие. *A_n - нормальная подгруппа группы S_n индекса 2.*

Определение 2.9.1. *Знакопеременной группой A_n порядка n называется подгруппа всех четных подстановок группы S_n.*

Упражнение 2.9.1. Показать, что A_3 – абелева группа, а для всех $n>3$ группа A_n – не абелева.

Упражнение 2.9.2. Показать, что в группе A_n при $n\ge4$ существует единственная подстановка f, для которой для всех $g\in A_n$ выполняется равенство $fg=gf$ - это тождественная подстановка.

Упражнение 2.9.3. Убедиться, что группа A_4 порядка 12 не содержит подгрупп порядка 6.

Данное упражнение показывает, что обращение теоремы Лагранжа невозможно: существуют конечные группы, в которых для некоторых делителей d их порядка отсутствуют подгруппы порядка d.

Упражнение 2.9.4. Показать, что A_4 содержит нормальную подгруппу порядка 4 – так называемую группу Квайна $K = \{e, (12)(34), (13)(24), (14)(23)\}$.

Данный факт оттеняет доказанная в середине XX века

Теорема 2.9.2. *При $n \geq 5$ группа A_n проста, то есть не содержит нормальных подгрупп.*

Пример 2.9.1. "Игра в пятнадцать": на квадратной доске, разделенной на 16 полей, размещены 15 фишек, пронумерованных от 1 до 15 и занимающих целиком соответствующее поле. Двигая фишки по горизонтали и вертикали с использованием свободного поля, требуется привести доску в состояние $\rightarrow$

i_1	i_2	i_3	i_4
i_5	i_6	i_7	i_8
i_9	i_{10}	i_{11}	i_{12}
i_{13}	i_{14}	i_{15}	

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Можно показать, что задача разрешима тогда и только тогда, когда подстановка $f = \begin{pmatrix} 1 & 2 & \dots & 15 \\ i_1 & i_2 & \dots & i_{15} \end{pmatrix}$ четная.

Следовательно, задача $\rightarrow$ за которую 120 лет назад предлагали большой денежный приз, не имеет решения.

2	1	3	4
5	6	7	8
9	10	11	12
13	14	15	

2.10. Нормальные подгруппы и фактор-группы

Определение 2.10.1. *Пусть $(G,\cdot)$ – группа и H – ее подгруппа. Фактор-множеством (левым) группы G по подгруппе H называется - множество всех левых смежных классов $\{H, aH, bH, \dots\}$ и обозначается через G/H.*

Пусть H – нормальная подгруппа. Определим умножение на фактор-множестве G/H по следующему правилу: $aH \cdot bH = (ab)H$. Операция полностью определяется умножением элементов группы G, поэтому ее называют индуцированной операцией умножения на фактор-множестве. Возникает вопрос о корректности таким образом определенной операции. Ведь в качестве элемента a, определяющего класс смежности aH, можно взять любой элемент этого класса. Пусть $\tilde{a} \in aH$, $\tilde{b} \in bH$. По свойствам смежных классов $\tilde{a}H = aH$, $\tilde{b}H = bH$. Однако будет ли $(\tilde{a}\tilde{b})H = (ab)H$? Ответ утвердительный,

если произведение $\tilde{a}\tilde{b} \in (ab)H$. Действительно, $\tilde{a} = ah, \tilde{b} = bh$ для подходящих $h, \tilde{h} \in H$. Тогда произведение $\tilde{a}\tilde{b} = (ah)(b\tilde{h}) = a(hb)\tilde{h} = a(bh_1)\tilde{h} = (ab)h_2 \in (ab)H$, где $h_2 = h_1\tilde{h}$, h_1 – такой элемент из H, что $hb = bh_1$, существующий в силу равенства смежных классов bH и Hb, гарантированного нормальностью подгруппы H.

Теорема 2.10.1. *Относительно индуцированной операции фактор-множество G/H по нормальной подгруппе H является группой.*

Доказательство. Выше доказано, что в силу нормальности подгруппы H операция определена корректно, то есть все произведения любых представителей классов aH и bH принадлежат в точности одному классу смежности. Операция ассоциативна по причине ассоциативности умножения в самой группе G. Единицей относительно индуцированной операции является, очевидно, группа H, а обратным к данному классу aH является класс смежности $a^{-1}H$.

Пример 2.10.1. Группа $(Z,+)$ содержит для всякого натурального $n>1$ нормальную подгруппу $(nZ,+)$. Следовательно, определена фактор-группа G/H. Это не что иное, как исследованная в первом разделе $(Z/nZ,\oplus)$, – группа классов вычетов по модулю n относительно операции сложения классов.

2.11. Гомоморфизмы групп

Определение 2.11.1. *Пусть $(G,\cdot)$ и $(H,\cdot)$ – две группы. Всякое отображение $\varphi: G \to H$, сохраняющее операции, то есть обладающее свойством $\varphi(g_1g_2) = \varphi(g_1)\cdot\varphi(g_1)$, называется гомоморфизмом из группы G в группу H.*

Перечислим основные свойства гомоморфизмов.

Свойство 1. $\varphi(e_G) = e_H$.

Доказательство. Для каждого $g \in G$ $\varphi(g) = \varphi(ge_G) = \varphi(g)\varphi(e_G)$. Полученное равенство означает, что $\varphi(e_G)$ ведет себя как нейтральный элемент группы H по отношению ко всем элементам $\varphi(g) \in H$. В силу единственности нейтрального элемента в группе заключаем, что $\varphi(e_G) = e_H$.

Свойство 2. *Если $\varphi(x) = y$, то $\varphi(x^{-1}) = y^{-1}$.*

Доказательство. По свойству 1 $\varphi(x^{-1}x) = \varphi(e_G) = e_H$. С другой стороны, $\varphi(x^{-1}x) = \varphi(x^{-1})\varphi(x) = \varphi(x^{-1})y = e_H$. Следовательно, $\varphi(x^{-1}) = y^{-1}$, что и требова-лось доказать.

Определение 2.11.2. *Ядром гомоморфизма* $\varphi: G \to H$ *называется множество всех элементов группы* G, *которые под действием данного гомоморфизма переходят в нейтральный элемент группы* H, *то есть множество* $Ker\varphi = \{x \in G \mid \varphi(x) = e_H\}$.

Свойство 3. $Ker\varphi$ *– нормальная подгруппа группы* G.

Доказательство. Множество $Ker\varphi$ не пусто, так как содержит, по меньшей мере, e_G согласно свойству 1. Если $x \in Ker\varphi$, то есть $\varphi(x) = e_H$, то $\varphi(x^{-1})\varphi(x) = \varphi(x^{-1}) = \varphi(x^{-1}x) = \varphi(e_G) = e_H$. Следовательно, $x^{-1} \in Ker\varphi$. Таким образом, $Ker\varphi$ – подгруппа группы G. Для произвольных $g \in G$ и $x \in H$ $\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g^{-1}) = \varphi(g)\varphi(g^{-1}) = e_H$. Следовательно, $gxg^{-1} \in H$ и в силу теоремы 2.7.1 $Ker\varphi$ – нормальная подгруппа группы G.

Определение 2.11.3. *Полный образ группы* G *при гомоморфизме* φ *- это множество* $\operatorname{Im} G = \{h \in H \mid \exists\, g \in G, что\ \varphi(g) = h\}$ *всех элементов группы* H, *для каждого из которых существует прообраз в группе* G *относительно отображения* φ.

Свойство 4. $\operatorname{Im} G$ *- подгруппа группы* H.

Доказательство вытекает из определения гомоморфизма и свойств 1 и 2.

Свойство 5. *Для каждой нормальной подгруппы* H *группы* G *сущест-вуют группа* $\overline{G}$ *и гомоморфизм* $\varphi: G \to \overline{G}$, *ядро которого совпадает с* H.

Доказательство. Пусть $\overline{G} = G/H$ и $\varphi: G \to G/H$ действует по правилу $\varphi(g) = g \cdot H$. Ясно, что $Ker\varphi = H$.

Определение 2.11.4. *Мономорфизмом или вложением группы* G *в группу* H *называется инъективный гомоморфизм групп, то есть такой гомоморфизм* $\varphi: G \to H$, *что для произвольных* $g_1, g_2 \in G$ *из условия* $g_1 \neq g_2$ *следует неравенство* $\varphi(g_1) \neq \varphi(g_2)$.

Свойство 6. *Гомоморфизм* $\varphi: G \to H$ *инъективен тогда и только тог-да, когда* $Ker\,\varphi = \{e_G\}$.

Доказательство очевидно.

Определение 2.11.5. *Гомоморфизм* $\varphi: G \to H$ *называется сюръектив-ным, если* $\operatorname{Im}\varphi = H$, *то есть для всякого* $h \in H$ *найдется прообраз – такой элемент* $g \in G$, *что* $\varphi(g) = h$.

Отметим, что применяемый в доказательстве свойства 5 гомоморфизм φ – сюръективный, его называют обычно каноническим гомоморфизмом.

Определение 2.11.6. *Группы* G *и* H *называются изоморфными, если существует инъективный и сюръективный гомоморфизм из одной группы в другую.*

Изоморфизм является взаимно однозначным отображением групп. В математике изоморфные объекты считаются одинаковыми. Основная цель теории групп - классифицировать все группы с точностью до изоморфизма.

Теорема 2.11.1. *Все циклические группы одного и того же порядка – изоморфны.*

Доказательство очевидно.

Теорема 2.11.2 (Кели). *Всякая конечная группа изоморфна некоторой подгруппе группы* S_n.

Теорема 2.11.3. *Существует мономорфизм* $f : S_n \to GL_n(R)$, *причем такой, что* $\det f(\sigma) = 1$, *если* σ *- четная подстановка и* $\det f(\sigma) = -1$, *если* σ *- нечетная подстановка.*

Отображение f в теореме 2.11.3 ставит подстановке g в соответствие мономиальную, то есть перестановочную матрицу A_g, получаемую из единичной матрицы $E_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ & \dots & \dots & \\ 0 & 0 & \dots & 1 \end{pmatrix}$ соответствующей перестановкой столбцов.

2.12. Автоморфизмы групп

Определение 2.12.1. *Если гомоморфизм* φ *отображает группу* G *в себя, то его называют эндоморфизмом данной группы. Автоморфизм – это взаимно однозначный гомоморфизм группы в себя.*

Тождественное отображение любой группы в себя, очевидно, является автоморфизмом этой группы. Его называют тривиальным автоморфизмом.

Теорема 2.12.1. *Всякая группа* G *порядка* $|G| > 2$ *имеет нетривиальный автоморфизм.*

Доказательство. Пусть G – некоммутативная группа. В ней найдутся по крайней мере два элемента a и b, такие, что $ab \neq ba$. Отображение $\varphi : G \to G$, такое, что $\varphi(x) = axa^{-1}$ для каждого $x \in G$, является эндоморфизмом группы G. Действительно, для произвольных $x, y \in G$ образ $\varphi(xy) = a(xy)a^{-1} = ax(a^{-1}a)ya^{-1} = (axa^{-1})(aya^{-1}) = \varphi(x)\varphi(y)$. При этом гомоморфизм φ инъективен в силу свойства 6 гомоморфизмов, поскольку $Ker\varphi = \{e\}$. В самом деле, если $\varphi(x) = axa^{-1} = e$, то отсюда следует, что $x = a^{-1}ea = e$. Гомоморфизм φ сюръективен, поскольку для каждого элемента $g \in G$ образ $\varphi(a^{-1}ga) = g$. Таким образом, φ – автоморфизм группы G.

Пусть G – абелева группа. Отображение $f: G \to G,$ такое, что $f(x) = x^{-1},$ является автоморфизмом группы. Действительно, в силу коммутативности $f(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = f(x)f(y),$ а биективность f очевидна. Данный автоморфизм будет нетривиальным, если в группе G найдется хотя бы один такой элемент $x,$ что $x^{-1} \neq x,$ то есть $x^2 \neq e.$

Пусть G – абелева 2-группа, то есть группа, у которой каждый элемент x обладает свойством: $x^2 = e.$ В такой группе каждый неединичный элемент g образует циклическую подгруппу $< g >= \{g, e\}$ из двух элементов. По условию порядок $|G| > 2$. Поэтому в данной группе найдутся по крайней мере два неединичных элемента $g, h \in G.$ Согласно теореме 2.11.1 существует изоморфизм ψ между циклическими группами $< g >$ и $< h >$. Он определяет автоморфизм в нециклической подгруппе группы $G,$ порожденной элементами g и $h.$ Это подгруппа $< g, h >= \{g, h, gh, e\},$ состоящая из четырех элементов. Действие автоморфизма ψ продолжим тривиальным образом на все остальные элементы группы $G.$ Таким образом, получим нетривиальный автоморфизм группы $G.$ Теорема полностью доказана.

Теорема 2.12.2. *Множество $Aut\, G$ всех автоморфизмов данной группы G является группой относительно операции композиции отображений.*

Доказательство. Множество $Aut\, G$ не является пустым в силу теоремы 2.12.1, замкнуто относительно операции композиции отображений, содержит нейтральный элемент – тривиальный автоморфизм. Каждый автоморфизм в силу своей биективности имеет обратное отображение, также взаимно однозначное. Несложно проверить, что оно также является гомоморфизмом и, следовательно, автоморфизмом данной группы. Тем самым теорема доказана.

Теорема 2.12.3. *Пусть $(G, \cdot)$ - конечная абелева группа порядка $|G| = n$, тогда для всякого целого k с условием НОД(k,n)=1, отображение $\varphi: g \to g^k$ есть автоморфизм группы G.*

Доказательство. В силу абелевости группы G отображение φ является гомоморфизмом. Покажем методом от противного, что в условиях теоремы $Ker\varphi$ тривиально. Предположим, что в группе G существуют различные элементы $g_1, g_2,$ такие, что $g_1^k = g_2^k.$ В таком случае $(g\ g_2^{-1})^k = e.$ Согласно теореме Лагранжа $(g_1 g_2^{-1})^n = 1.$ В силу взаимной простоты целых чисел n и k найдутся такие целые u и $v,$ что $nu + kv = 1.$ Тогда $g_1 g_2^{-1} = ((g_1 g_2^{-1})^n)^u \cdot ((g_1 g_2^{-1})^k)^v = e^u \cdot e^v = e,$ то есть $g_1 = g_2.$ Это означает, что $Ker\varphi$ содержит единственный элемент e группы

G. Тогда согласно свойству 6 гомоморфизмов групп отображение φ является инъективным, а следовательно, автоморфизмом группы G.

Методом от противного легко доказывается

Теорема 12.4. *Для произвольного автоморфизма φ любой группы G и для каждого $a \in G$ порядки элементов a и $\varphi(a)$ совпадают.*

2.13. Криптосистема RSA

Понятие группы считается основополагающим в математике XX века. Группы широко применяются в физике (от кристаллографии до теории элементарных частиц), химии, биологии, теории информации. Новейшие методы защиты информации от несанкционированного доступа называют групповыми, так как они базируются на понятии группы. Ярким примером является криптосистема RSA, предложенная в 1977 г. американскими исследователями Ривестом, Шамиром и Адлеманом (Rivest R.L., Shamir A., Adleman L.). Суть ее в следующем.

Находятся два больших простых числа (60-70 десятичных знаков) p и q. Вычисляется их произведение $n = pq$. Тогда $\varphi(n) = (p-1)(q-1)$. Фиксируется натуральное число e, $0 < e < n$, $НОД(e, \varphi(n)) = 1$. Пара (e, n) называется открытым ключом. Передаваемая информация переводится в цифровую форму (в первоисточнике буквы латинского алфавита заменяются двузначными числами: “a”=01, “b”=02 и так далее, пробел = 00), шифруется в виде числа c – сообщения, $0 < c < n$, $НОД(c, n) = 1$. Тогда c есть обратимый элемент кольца Z/nZ, то есть элемент абелевой группы $(Z/nZ)^*$ порядка $\varphi(n)$. Сообщение шифруется и передается числом $m = c^e (\mathrm{mod}\, n)$. Таким образом, m есть e-я степень числа c в кольце Z/nZ. Согласно теореме 2.12.3 операция возведения в e-ю степень является автоморфизмом группы $(Z/nZ)^*$.

Адресат получает сообщение m. Он, как и все, знает величины n и e. Он также должен знать секретный ключ – такое натуральное число $d < n$, что $e \cdot d \equiv 1 (\mathrm{mod}(\varphi(n))$. Это означает, что $e \cdot d = \varphi(n) \cdot q + 1$ для некоторого целого n. Тогда $\overline{m}^d = \overline{c}^{ed} = \overline{c}^{\varphi(n) \cdot r + 1} = \left(\overline{c}^{\varphi(n) \cdot}\right)^r \cdot \overline{c} = 1 \cdot \overline{c} = \overline{c}$. Чтобы расшифровать m, адресат должен возвести m в d-ю степень по модулю n. Это простая задача.

Перехватчик, чтобы расшифровать сообщение m, должен разложить n на множители: $n = pq$. Тогда вычисляется $\varphi(n)$ и d легко находится по открытому ключу e. Именно разложение ключа n на множители и составляет основную сложность предлагаемой криптосистемы. Как отмечено в первом разделе, разложение натурального числа на множители является, по

всей видимости, экспоненциальной относительно n задачей, эквивалентной перебору всех возможных кандидатов на делители.

Чтобы продемонстрировать стойкость своей криптосистемы, изобретатели зашифровали сообщение «The magic words squeamish suffrage», используя в качестве n – 129-значное число и в качестве e – 4-значное число. Их сообщение m было 128-значнным числом. Всемирно известный американский специалист по головоломкам М. Гарднер опубликовал этот криптотекст в журнале «Scientific American» в августе 1977 г., предложив 1000 дол. тому, кто его расшифрует. Текст был расшифрован лишь в апреле 1994 г. Задействованы были ресурсы 1600 компьютеров более 20 стран (через Internet). Организаторы вычислений использовали суперкомпьютер – MasPar. Данные были занесены в 0-1 матрицу из 188346 строк и 188146 столбцов. Файл с этой матрицей превосходил 4 Гбайта. Причем каждый бит был существенным. 129-значное число n было разложено на 64- и 65-значные множители p и q. Непосредственно факторизация числа n заняла полтора года вычислений. После этого расшифровка сообщения не составила труда.

3. Кольца, многочлены и поля

3.1. Основные понятия о кольцах

Определение 3.1.1. *Кольцом называется непустое множество K с двумя бинарными алгебраическими операциями сложения (+) и умножения (·); относительно операции сложения K является абелевой группой, а умножение и сложение связаны законами дистрибутивности:*

$(a+b)\cdot c=a\cdot c+b\cdot c;\ a(b+c)=ab+ac$ *для произвольных* $a,b,c\in K$.

Рассмотрим типичные примеры колец.

Пример 3.1.1. $(Z,+,\cdot)$ – кольцо целых чисел.

Пример 3.1.2. $(Z/nZ,+,\cdot)$ – кольцо классов вычетов по модулю $n>1$.

Названные кольца достаточно глубоко изучены в первом разделе. Следующие три примера в той или иной степени известны каждому студенту уже с первого курса.

Пример 3.1.3. Множество всех квадратных матриц данного порядка n с рациональными, вещественными или же комплексными коэффициентами относительно операций матричного сложения и умножения. Общепринятые обозначения этих колец: $M_n(Q)$, $M_n(R)$, $M_n(C)$ соответственно.

Пример 3.1.4. Множество всех подмножеств $\Omega(M)$ непустого множества M. Оно является абелевой группой относительно операции симметрической разности $\overset{\bullet}{\longleftrightarrow}$ (см. пример 2.2.2). Здесь операция пересечения множеств играет роль умножения. В теории множеств известно тождество: $(A\overset{\bullet}{\longleftrightarrow}B)\cap C=(A\cap C)\overset{\bullet}{\longleftrightarrow}(B\cap C)$, которое означает, что симметрическая разность и пересечение связаны законом дистрибутивности. Данное кольцо носит название – булеан в честь английского математика XIX в. Джорджа Буля, основателя математической логики.

Пример 3.1.5. Множество $F(a,b)$ всех вещественных функций, определенных на данном интервале (a,b) числовой оси с обычными операциями сложения и умножения функций.

Пример 3.1.6. Кольцо полиномов $R[x]$ с вещественными коэффициен-тами от переменной x с естественными операциями сложения и умножения полиномов.

Многообразие колец чрезвычайно широко. Предложенную выборку из пяти простейших примеров нельзя считать репрезентативной. По числу элементов кольца делятся на конечные (пример 3.1.2) и бесконечные (примеры 3.1.1, 3.1.3, 3.1.5). Основная классификация колец ведется по свойствам умножения. Соответственно определяются направления исследований колец, со своими методами и техникой. Наиболее развитой следует считать теорию ассоциативных колец.

Определение 3.1.2. *Кольцо K называется ассоциативным кольцом, если определенная на нем операция умножения обладает свойством:* $(ab)c=a(bc)$ *для произвольных* $a,b,c\in K$.

Кольцо K называется кольцом с единицей, если оно ассоциативно и имеет нейтральный элемент относительно операции умножения.

Кольцо K называется коммутативным, если $ba = ab$ для произвольных $a, b \in K$.

Приведенные выше примеры колец 3.1.1 – 3.1.6 являются ассоциативными. Неассоциативные кольца также являются серьёзным объектом исследований. К ним относятся важные для приложений йордановы кольца (квантовая механика, генетика, геометрия), кольца Ли (теория алгебраических групп, геометрия, дифференциальные уравнения). Приведем простейший пример кольца Ли.

Пример 3.1.7. Множество всех классических векторов V_3 трехмерного пространства с операциями сложения и векторного умножения векторов. Как известно, векторное умножение неассоциативно. К примеру, здесь $(\bar{i}\bar{i})\bar{k} = \bar{0}$, $\bar{i}(\bar{i}\bar{k}) = \bar{i}(-\bar{j}) = -\bar{k} \neq 0$. Отметим также, что данное кольцо $(V_3, +, \times)$, как и в примере 3.1.3, не является коммутативным.

Общих свойств у колец немного. Приведем некоторые из них. Как и во всякой аддитивной группе, в любом кольце K определена обратная алгебраическая операция – вычитание: $a - b = a + (-b)$. Это неассоциативная операция, без нейтрального элемента. Тем не менее справедлива

Теорема 3.1.1. *Во всяком кольце K операции вычитания и умножения связаны законами дистрибутивности, то есть для произвольных $a, b, c \in K$*

$$a(b-c) = ab - ac; \quad (a-b)c = ac - bc.$$

Доказательство.

$b = 0 + b = (c - c) + b = c + (-c) + b = c + b + (-c) = c + (b - c)$. Следовательно, $ab = a(c + (b - c)) = ac + a(b - c)$. Этим доказано первое дистрибутивное равенство из теоремы. Аналогично доказывается второе соотношение дистрибутивности.

Лемма 3.1.1. *В любом кольце K любое произведение, в котором хотя бы один из сомножителей равен нулю, само равно нулю. Иными словами, для произвольного $a \in K$ произведение $0a = a0 = 0$.*

Доказательство. В силу теоремы 3.1.1 $a0 = a(b - b) = ab - ab = 0$, что и требовалось доказать.

Теорема 3.1.2. *В любом кольце K для произвольных $a, b \in K$ справедливы равенства $(-a)b = a(-b) = -ab$; $(-a)(-b) = ab$.*

Доказательство. $ab + (-a)b = (a + (-a))b = 0b = 0$. Отсюда следует первая часть первого доказываемого соотношения. Так же проверяется и вторая ее часть. Используя доказанное, получаем: $(-a)(-b) = -(a(-b)) = -(-ab) = ab$.

Теорема 3.1.3. *Пусть K – кольцо с единицей, содержащее более одного элемента. Тогда $0 \neq 1$.*

Доказательство. Пусть в кольце K нейтральные элементы совпадают: $0=1$. Тогда для произвольного $a \in K$ согласно лемме 3.1.1 $a = a \cdot 1 = a \cdot 0 = 0$. Следовательно, K состоит из единственного элемента 0. Теорема доказана.

Ассоциативные кольца делятся на кольца с единицей и без единицы, коммутативные и некоммутативные. Теория коммутативных колец лежит в основе теории полей, алгебраической теории чисел, современной алгебраической геометрии [11].

3.2. Мультипликативная группа кольца

Теорема 3.2.1. *Пусть K – ассоциативное кольцо с единицей. Множест-во K^* обратимых относительно умножения элементов кольца K есть группа (её называют мультипликативной группой кольца K).*

Доказательство состоит в скрупулезной проверке аксиом группы.

Пример 3.2.1. Легко видеть, что в кольце целых чисел обратимы относительно умножения только два числа: 1 и –1. Следовательно, $Z^* = \{1, -1\}$.

Пример 3.2.2. $M_n(R)^* = GL_n(R)$.

Пример 3.2.3. Мультипликативная группа $(Z/nZ)^*$ кольца классов вычетов Z/nZ по модулю n состоит из $\varphi(n)$ классов, порожденных целыми числами, взаимно простыми с модулем, согласно теореме 1.7.1.

Определение 3.2.1. *Если в кольце K с единицей мультипликативная группа $K^* = K \setminus \{0\}$, то кольцо K называют телом или алгеброй с делением. Коммутативное тело называют полем.*

Пример 3.2.4. Следующие кольца являются полями:

а) Q – кольцо рациональных чисел;

б) R – кольцо вещественных чисел;

в) C – кольцо комплексных чисел;

г) Z/pZ – кольцо классов вычетов по простому модулю p.

Пример 3.2.5. Пример некоммутативного тела. H – тело кватернионов – множество выражений вида $h=a+bi+cj+dk$, где $a,b,c,d \in R$, $i^2 = -1$; $j^2 = -1$; $k^2 = -1$; $ij = k = -ji$; $jk = i = -kj$; $ki = j = -ik$. Кватернионы складываются и перемножаются почленно с учетом указанных выше формул. Поэтому H – ассоциативное, но не коммутативное кольцо с единицей. Непосредственно проверяется, что для всякого $h \neq 0$ обратный кватернион находится по формуле $h^{-1} = \dfrac{a - bi - ij - dk}{a^2 + b^2 + c^2 + d^2}$.

Теория некоммутативных тел является разделом теории простых алгебр. Во всяком теле T коммутирующие со всеми элементы образуют поле Z, называемое центром тела T. Тело T является векторным пространством над этим центром, а точнее, алгеброй над Z. Наиболее

развита теория конечномерных тел (у которых $\dim(T:Z)<+\infty$)). Известно, что размерность T над Z всегда является квадратом: $\dim(T:Z)=n^2$ для некоторого натурального n; что T содержит максимальные подполя размерностью n над центром Z. Свойства тела существенно зависят от свойств центра. Следующая теорема дает описание конечных тел.

Теорема 3.2.2 (Веддерберна). *Всякое конечное тело является полем.*

3.3. Делители нуля в кольцах

Лемма 3.1.1 отмечает, что в каждом кольце произведение элементов, среди которых есть нулевые, обязательно равно нулю. В числовых кольцах верно и обратное: если произведение $ab=0,$ то крайней мере один из сомножителей равен нулю. Однако в общем случае это не так.

Определение 3.3.1. *Если в кольце K найдутся ненулевые элементы a и b, такие, что произведение $ab=0$, то их называют делителями нуля.*

Пример 3.3.1. В кольце $(V_3,+,\times)$ каждый отличный от нуля элемент является делителем нуля: $\overline{v}\times\overline{v}=\overline{0}$.

Пример 3.3.2. В кольце матриц $M_3(R)$ примерами делителей нуля являются матрицы $A=\begin{pmatrix}0&0&1\\0&0&0\\0&0&0\end{pmatrix}$ и $B=\begin{pmatrix}0&1&0\\0&0&1\\0&0&0\end{pmatrix}$, так как $A\cdot B=0$.

Пример 3.3.3. В кольце Z/nZ с $n=pq$ классы $\overline{p}$ и $\overline{q}$ являются делителями нуля.

Пример 3.3.4. Кольцо $F(a,b)$, рассмотренное в примере 3.1.5, – с делителями нуля. Примером могут служить функции $f(x)=\begin{cases}0, & a<x\le c<b;\\ 1, & c\le x<b\end{cases}$ и $g(x)=\begin{cases}1, & a<x\le c;\\ 0, & c\le x<b.\end{cases}$ Очевидно, произведение $f(x)g(x)$ – нулевая на отрезке (a,b) функция.

Теорема 3.3.1. *В любом ассоциативном кольце K с единицей делители нуля необратимы относительно умножения.*

Доказательство. Пусть для ненулевых элементов $a,b\in K$ их произведение $ab=0$ и пусть в кольце K существует обратный элемент b^{-1}. Тогда в силу ассоциативности умножения $abb^{-1}=(ab)b^{-1}=0b^{-1}=0.$ С другой стороны, $abb^{-1}=a(bb^{-1})=a\cdot 1=a.$ Таким образом, $a=0,$ что противоречит условию $a\neq 0.$ Теорема доказана.

Примеры 3.3.2 и 3.3.3 имеют более общую природу.

Теорема 3.3.2. *В кольце Z/nZ с составным n всякий ненулевой класс или обратим или является делителем нуля.*

Доказательство. Пусть k – натуральное число, $1 \le k \le n$, и $\overline{k}$ – соответствующий класс вычетов в кольце Z/nZ. Если k и n взаимно просты, то $\overline{k}$ – обратимый элемент кольца Z/nZ согласно теореме 1.7.1. Пусть k и n не взаимно просты, то есть $НОД(k,n) = d > 1$. Тогда $n = n_1 d$, $k = k_1 d$ для подходящих натуральных чисел n_1 и k_1. Тогда $\overline{k}, \overline{n}_1$ – ненулевые классы кольца Z/nZ, а их произведение $\overline{k} \cdot \overline{n}_1 = \overline{0}$, поскольку произведение $n_1 k = n_1(dk_1) = (n_1 d)k_1 = nk_1$ – кратно n. Тем самым теорема доказана.

Теорема 3.3.3. *В матричном кольце $M_n(R)$ всякая ненулевая матрица либо обратима, либо является делителем нуля.*

Доказательство. Пусть A – произвольная ненулевая квадратная матрица порядка n с вещественными коэффициентами. Если $\det A \neq 0$, то она обратима, как известно каждому первокурснику. Пусть $\det A = 0$. Тогда найдется такая матрица $X \in M_n(R)$, что произведение $AX = 0$. В самом деле, выписанное матричное уравнение относительно неизвестной матрицы X эквивалентно n системам линейных уравнений относительно неизвестных – координат каждого из столбцов матрицы X с одной и той же матрицей коэффициентов при неизвестных – матрицей A. Согласно теории линейных уравненных уравнений, каждая из таких систем имеет ненулевое решение. Это означает существование искомой ненулевой матрицы X. Теорема доказана.

3.4. Идеалы колец

Определение 3.4.1. *Подкольцо кольца K –- это подгруппа аддитивной группы $(K,+)$, в свою очередь являющаяся кольцом, то есть замкнутая относительно операции умножения в кольце K.*

Пример 3.4.1. $(nZ,+,\cdot)$ – подкольцо кольца Z целых чисел; Z – подкольцо кольца Q рациональных чисел; Q – подкольцо кольца R вещественных чисел. Первое из них - это кольцо без единицы, хотя само кольцо Z с единицей.

Пример 3.4.2. Матричное кольцо $M_2(R)$ содержит подкольцо матриц $C=\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a,b \in R\right\}$, оно в свою очередь содержит подкольцо скалярных матриц $S=\left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in R\right\}$. Это коммутативные подкольца некоммутативного кольца $M_2(R)$. Само кольцо содержит много делителей нуля согласно теореме 3.3.3, а подкольца C и S их не содержат и, более

того, являются полями. Второе из них по своим свойствам идентично полю вещественных чисел, а первое – полю комплексных чисел.

Подкольцами кольца $M_2(R)$ являются также множества матриц $J_1=\left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} | \, a,b \in R\right\}$; $J_2=\left\{\begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix} | \, c,d \in R\right\}$; $J_3=\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} | \, a,b \in R\right\}$; $J_4=\left\{\begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix} | \, c,d \in R\right\}$. Это некоммутативные кольца. Ни одно их этих четырех подколец не содержит единицы, однако имеют односторонние нейтральные элементы. Например, в кольце J_4 левыми единицами являются матрицы $\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$ и $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

Приведенные примеры показывают, что подкольца, в общем случае, практически не наследуют свойства колец. Поэтому в теории колец наибольшее значение имеют подкольца специального вида – идеалы.

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

Ясно, что в коммутативном кольце все идеалы двусторонние.

Пример 3.4.3. *$mZ=\{mq | q \in Z\}$* – двусторонний идеал кольца целых чисел Z для всякого натурального m. Очевидно, *$mZ \neq Z$,* если $m>1$. Ясно, что *$2z>4z>8z>16z>\ldots$; $2z>6z>12z>\ldots$* .

Пример 3.4.4. В кольце Z/nZ с составным модулем *$n=pq$,* $p>1, q>1$, легко видеть, что множество классов вычетов $\left\{\overline{p}, \overline{2p}, \ldots, \overline{(q-1)p}, \overline{0}\right\}$ замкнуто относительно операций сложения и умножения классов вычетов и, следовательно, образует подкольцо. Обозначим его через $J_{\overline{p}}$. Легко видеть, что $J_{\overline{p}}$ – идеал. Аналогично идеалом является множество $J_{\overline{q}}=\left\{\overline{q}, \overline{2q}, \ldots, \overline{(p-1)q}, \overline{0}\right\}$.

Пример 3.4.5. В матричном кольце $M_2(R)$ подкольца J_1 и J_2 есть правые идеалы, а J_3 и J_4 – левые идеалы.

Пример 3.4.6. В любом кольце K множество $\{0\}$ и K формально также являются идеалами кольца K. Их называют несобственными, или тривиальными, в отличие от остальных – собственных идеалов.

Отметим основные свойства идеалов.

Теорема 3.4.1. *1. Пересечение идеалов данного кольца K есть идеал этого же кольца.*

2. Если J_1, J_2 *– левые (правые) идеалы кольца* K, *то их сумма, то есть множество всех сумм* $\{j_1 + j_2 \mid j_1 \in J_1; j_2 \in J_2\}$, *есть левый (правый) идеал кольца* K.

3. Произведение $J_1 J_2 = \{j_1 \cdot j_2 \mid j_1 \in J_1; j_2 \in J_2\}$ *левых (правых) идеалов* J_1, J_2 *кольца* K *есть левый (правый) идеал этого же кольца.*

4. Для каждого элемента a *кольца* K *множество* $aK=\{ak|k \in K\}$ *есть левый идеал кольца* K.

5. Если в кольце K *с единицей элемент* $a \in K^*$, *то* $<a>=K$; *если же* $a \notin K^*$, *то* $<a>$ *– собственный идеал кольца* K.

6. Если K *– коммутативное кольцо и* $a=bc$ *для необратимых элементов* $a,b,c \in K$, *то* $< a > \subset < c >$, $< a > \subset < b >$.

Доказательство состоит в прямой проверке всех аксиом идеалов.

Следствие. *В каждом поле отсутствуют делители нуля и собственные идеалы.*

Доказательство. Поскольку в поле все элементы, кроме 0, обратимы, то из 5-й части теоремы 3.4.1 следует, что в поле нет собственных идеалов. С другой стороны, из 5-й части теоремы 3.4.1 следует, что делители нуля (необратимые элементы кольца) порождают собственные идеалы. Отсюда следует, что в поле нет делителей нуля.

Определение 3.4.2. *Левым главным идеалом* $< a >$ *кольца* K, *порожденным элементом* $a \in K$, *называется идеал из 4-го пункта теоремы 3.4.1, то есть подкольцо кольца* K, *состоящее из всех элементов* ak, $k \in K$. *Правый главный идеал* $< a >$ *состоит из всех элементов* ka, $k \in K$.

Теорема 3.4.2. *В кольце целых чисел* Z *– всякий идеал,* J *– главный.*

Доказательство. Пусть J – ненулевой идеал кольца Z. Так как J – группа относительно сложения, то J обязательно содержит натуральные числа. Пусть t – наименьшее натуральное число из J. Пусть m – произвольное целое число из идеала J. Тогда m делится на t. В противном случае по теореме о делении с остатком $m = tq + r$ для подходящих целых q и r, причем $0 < r < t$. Тогда $r = m - tq \in J$, что противоречит минимальности t. Следовательно, $m = tq$ для каждого $m \in J$. Это означает, что идеал $J =< t >$ – главный. Теорема доказана.

На множестве идеалов каждого кольца существует отношение частичного порядка по включению их друг в друга как множеств. Особую роль играют максимальные идеалы.

Определение 4.3. *Идеал* M *(левый, правый, двусторонний) кольца* K *называется максимальным, если в* K *не существует собственного идеала* J *с условием* $M \subset J$.

Теорема 3.4.3. *В кольце целых чисел идеал* J *максимален тогда и только тогда, когда существует простое число* p, *такое, что* $J =< p >$.

Доказательство следует из 6-й части теоремы 3.4.1.

Упражнение 3.4.1. В кольце $Z/12Z$ выписать все иделы, расположить их в порядке включения, указать максимальные идеалы.

3.5. Арифметические свойства полиномов

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

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

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

Доказательство. Пусть $f(x)=a_nx^n+a_{n-1}x^{n-1}+...+a_0$, а $g(x)=b_mx^m+b_{m-1}x^{m-1}+...+b_0$. Если $n<m$, то $q(x)=0, r(x)=f(x)$. Пусть $n\geq m$. Тогда для $c_{n-m}=a_n/b_m$ разность $f(x)-g(x)\cdot c_{n-m}x^{n-m}=d_kx^K+d_{k-1}x^{k-1}+...+d_0=d(x)$ является полиномом кольца $P[x]$ степени $k\leq n-1$. Если $\deg d(x)<\deg g(x)$, то теорема доказана, так как в качестве $q(x)$ можно взять $c_{n-m}x^{n-m}$, а в качестве $r(x)-$полином $d(x)$. Если же $k\geq m$, то для $c_{k-m}=d_k/b_m$ вычислим разность $d(x)-g(x)\cdot c_{k-m}x^{k-m}=e_sx^s+e_{s-1}x^{s-1}+...+e_0=e(x)$. Если $\deg e(x)<\deg g(x)$, то теорема доказана: $q(x)=c_{n-m}x^{n-m}+c_{k-m}x^{k-m}$, $r(x)=e(x)$. Если $\deg e(x)\geq\deg g(x)$, то продолжаем аналогичное рассуждение с $e(x)$ и так далее. В конце концов, самое большее на $n-m+1-$м шаге мы получим равенство $f(x)=g(x)\cdot(c_{n-m}x^{n-m}+...+c_0)+r(x)$, где $\deg r(x)<\deg g(x)$ или же $r(x)=0$. Таким образом, теорема доказана.

Замечание. Доказательство теоремы 3.5.1 конструктивно, из него непосредственно вытекает известный алгоритм деления многочлена на многочлен «уголком».

Определение 3.5.1. *В условиях теоремы 3.5.1 многочлен* $q(x)$ *называют частным, а полином r(x) - остатком от деления* $f(x)$ *на* $g(x)$. *Если r(x)=0, то говорят, что* $f(x)$ *делится на* $g(x)$, *а* $g(x)$ *и* $q(x)$ *называют делителями или множителями полинома* $f(x)$.

Если в равенстве $f(x)=g(x)\cdot q(x)$ *степени сомножителей не меньше* 1, *то* $q(x)$ *и* $g(x)$ *называют нетривиальными делителями многочлена* $f(x)$.

Очевидно, каждый ненулевой элемент поля P является делителем любого многочлена из кольца $P[x]$. Поэтому элементы полей называют тривиальными делителями полиномов.

Теорема 3.5.2. *Обратимыми многочленами в кольце полиномов* $P[x]$ *являются многочлены нулевой степени, отличные от нуля, и только они, то есть* $P[x]^* = P^*$.

Определение 3.5.2. *Наибольшим общим делителем многочленов* $f_1)x), f_2(x),..., f_s(x)$ *называется их общий делитель со старшим коэффициентом* 1, *который делится на любой другой общий делитель. Его обозначают* $НОД(f_1(x), f_2(x),..., f_s(x))$.

Алгоритм Евклида нахождения наибольшего общего делителя, рассмотренный в первом разделе для целых чисел, справедлив и для полиномов.

Теорема 3.5.3. *Наибольший общий делитель многочленов* $f(x)$ *и* $g(x)$ *из кольца* $P[x]$ *(с точностью до множителей из поля* P*) совпадает с последним отличным от нуля остатком* $r_n(x)$ *следующей цепочки равенств:*

$$\begin{cases} \{f(x) = g(x)q_1(x) + r_1(x); \\ \{g(x) = r_1(x)q_2(x) + r_2(x); \\ \{ \ \ldots\ldots\ldots\ldots\ldots \\ \{r_{n-2}(x) = r_{n-1}(x)q_n(x) + r_n(x); \\ \{r_{n+1}(x) = r_n(x)q_{n+1}(x). \end{cases}$$

Доказательство аналогично доказательству теоремы 1.2.2.

Пример 3.5.1. Найдем наибольший общий делитель многочленов $f(x) = x^4 + 3x^3 - 4x - 3$ и $g(x) = 3x^3 + 10x^2 + 2x - 3$ в кольце $Q[x]$. Согласно теореме 3.5.3 наибольший общий делитель по алгоритму Евклида получается с точностью до константы. Поэтому и сам алгоритм будем реализовывать с точностью до множителей из Q с целью проведения вычислений преимущественно с целыми коэффициентами. Последовательным делением «уголком» с учетом сказанного получаем следующую систему равенств алгоритма Евклида:

$3f(x) = g(x)(x - 1/3) + (-1/3)(5x^2 + 25x + 30) = g(x)q_1(x) + r_1(x)$;

$g(x) = (x^2 + 5x + 6)(3x - 5) + (9x + 27) = \tilde{r}_1(x)q_2(x) + r_2(x)$; здесь

$\tilde{r}_1(x) = (-3/5)r_1(x)$;

$x^2 + 5x + 6 = (x + 3)(x + 2)$, то есть $\tilde{r}_1(x) = \tilde{r}_2(x)q_3(x)$ для

$\tilde{r}_2(x) = (1/9)r\ (x)$.

Таким образом, $НОД(f(x), g(x)) = (1/9)r_2(x) = x + 3$.

Определение 3.5.2. *Многочлены f(x) и g(x) называют взаимно простыми, если их наибольший общий делитель равен* 1.

Обратной прогонкой алгоритма Евклида получается следующее утверждение – критерий взаимной простоты двух многочленов.

Теорема 3.5.4. *Многочлены* $f(x)$ *и* $g(x)$ *являются взаимно простыми тогда и только тогда, когда найдутся такие полиномы* $u(x), v(x),$ *для которых выполняется следующее равенство (соотношение Безу для многочленов):* $f(x)u(x) + g(x)v(x) = 1.$

С помощью этого критерия получается ряд следствий, имеющих независимое значение. Приведем их в виде отдельных предложений.

Предложение 3.5.1. *Если многочлен* $f(x)$ *взаимно прост с каждым из многочленов ц(x) и ш(x), то он взаимно прост и с их произведением.*

Доказательство. Согласно критерию взаимной простоты полиномов имеют место следующие соотношения: $f(x)u(x) + \varphi(x)v(x) = 1,$ $f(x)\tilde{u}(x) + \psi(x)\tilde{v}(x) = 1.$ Перемножим друг на друга соответственно левые и правые части этих равенств. Получим $f(x)U(x) + (\varphi(x)\psi(x))V(x) = 1$ для $V(x) = v(x)\tilde{v}(x)$ и $U(x) = f(x)u(x)\tilde{u}(x) + \psi(x)u(x)\tilde{v}(x) + \varphi(x)\tilde{u}(x)v(x),$ что в силу теоремы 3.5.4 означает взаимную простоту $f(x)$ и произведения $\varphi(x)\psi(x).$

Предложение 3.5.2. Если произведение многочленов f(x) и g(x) делится на многочлен φ(x), но $НОД(f(x), \varphi(x)) = 1,$ то g(x) делится на $\varphi(x).$

Доказательство дословно повторяет доказательство леммы 1.4.1.

Предложение 3.5.3. *Если многочлен* $f(x)$ *делится на каждый из попарно взаимно простых полиномов* $\varphi_1(x), \varphi_2(x), ..., \varphi_m(x),$ *то* $f(x)$ *делится и на их произведение* $\varphi_1(x)\varphi_2(x) \cdot ... \cdot \varphi_m(x).$

Доказательство в силу предложения 3.5.1 достаточно провести для случая $m = 2.$ Пусть $f(x)$ делится на многочлены $\varphi_1(x), \varphi_2(x),$ которые взаимно просты друг с другом. По теореме о делении с остатком $f(x) = \varphi_1(x)q(x).$ Произведение $\varphi_1(x)q(x)$ делится на $\varphi_2(x),$ но $НОД(\varphi_1(x), \varphi_2(x)) = 1.$ Согласно предложению 3.5.2 многочлен $q(x)$ должен делиться на $\varphi_2(x).$ Следовательно, $f(x) = \varphi_1(x)\varphi_2(x)\tilde{q}(x)$ для подходящего полинома $\tilde{q}(x).$ Таким образом, $f(x)$ делится на произведение $\varphi_1(x)\varphi_2(x)$ и предложение 3.5.3 доказано.

Определение 3.5.3. *Многочлен* $f(x) \in P[x]$ *степени* $n \geq 1$ *называется неприводимым в кольце* $P[x],$ *если в любом его представлении в виде произведения* $f(x) = g(x)q(x)$ *сомножителей* $g(x), q(x) \in P[x]$ *один из этих сомножителей является константой, то есть элементом поля* $P.$

Структура неприводимых полиномов существенно зависит от поля $P.$ Если $P = C$ – поле комплексных чисел, то неприводимыми полиномами в $C[x]$ являются только полиномы 1-й степени согласно основной теореме алгебры. Отсюда следует, что в кольце $R[x]$ неприводимыми являются

лишь полиномы первой степени, а также второй степени с отрицательным дискриминантом. Что касается кольца $Q[x]$, то здесь для каждого натурального $n \geq 1$ существуют (причём бесконечно много) неприводимые полиномы степени n. К примеру, таковыми являются полиномы $x^n \pm p$, где $p -$ простое число согласно следующему критерию Эйзенштейна.

Теорема 3.5.5 (критерий Эйзенштейна). *Пусть* $f(x) = a_n x^n + \ldots + a_0 -$ *полином степени* $n > 1$ *с целыми коэффициентами и* $p -$ *такое простое число, что* $a_i \equiv 0 (\mathrm{mod}\, p)$ *для всех* $i < n$, *но* a_n *не делится на* p, *и* a_0 *не делится на* p^2. *Тогда* $f(x) -$ *неприводимый в кольце* $Q[x]$ *полином.*

Доказательство см. в [8], с. 101 или в [17], гл. 5, п. 7.

В кольце $(Z/pZ)[x]$ также существуют неприводимые полиномы любой степени $n \geq 1$. Только в отличие от $Q[x]$ здесь произвольных полиномов степени n имеется лишь конечное множество (в количестве p^{n+1}), тем более неприводимых полиномов данной степени всегда конечно. Обычно неприводимость полинома над конечным полем определяется процедурой просеивания, напоминающей решето Эратосфена для целых чисел – последовательным делением на неприводимые (или все) меньшей степени от 1 до $[n/2]$. В качестве примера приведём список всех неприводимых полиномов в кольце $(Z/2Z)[x]$ степени, меньшей шести.

1) x;
2) $x+1$;
3) $x^2 + x + 1$;
4) $x^3 + x + 1$;
5) $x^3 + x^2 + 1$;
6) $x^4 + x^3 + x^2 + x + 1$;
7) $x^4 + x + 1$;
8) $x^4 + x^3 + 1$;
9) $x^5 + x^2 + 1$;
10) $x^5 + x^3 + 1$;
11) $x^5 + x^3 + x^2 + x + 1$;
12) $x^5 + x^4 + x^2 + x + 1$;
13) $x^5 + x^4 + x^3 + x + 1$;
14) $x^5 + x^4 + x^3 + x^2 + 1$.

Неприводимые полиномы играют роль простых чисел кольца целых чисел. Аналогично теореме 1.5.1 доказывается

Теорема 3.5.6. *Всякий многочлен* $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in P[X]$ *степени* $n \geq 1$ *представим в виде произведения* $f(x) = a_n p_1(x) p_2(x) \cdot \ldots \cdot p_s(x)$, *где* $p_i(x) -$ *неприводимые полиномы со старшим коэффициентом, равным* 1. *Такое представление единственно с точностью до порядка сомножителей.*

Процедура конкретной факторизации полинома в произведение неприводимых достаточно трудоемка, зависит существенным образом от поля коэффициентов, имеет массу методик и подходов. Над полем комплексных она эквивалентна, в силу основной теоремы алгебры и теоремы Безу, решению алгебраических уравнений. Над другими полями решение алгебраических уравнений включается лишь как один из этапов

факторизации. Над конечными полями факторизовать полиномы можно аналогом решета Эратосфена. Существует полиномиальный алгоритм Берлекемпа факторизации полиномов над конечными полями [12,17]. В 1982 г. на его основе разработан полиномиальный алгоритм Ленстры-Ленстры-Ловаса [17] факторизации полиномов над кольцом целых чисел.

3.6. Многочлены и их корни

Определение 3.6.1. *Корнем многочлена* $f(x) \in P[x]$ *называется такой элемент поля* $\alpha \in P$ *(или другого поля, содержащего* P*), что при подстановке* $x = \alpha$ *в* $f(x)$ *получаем равенство:* $f(\alpha) = 0$.

Теорема 3.6.1 (Безу). *Элемент* $\alpha \in P$ *(или* $\alpha \in F \supset P$*) является корнем полинома* $f(x) \in P[x]$ *степени* $n \geq 1$ *тогда и только тогда, когда* $f(x)$ *делится без остатка на* $x - \alpha$, *то есть когда выполняется равенство* $f(x) = (x - \alpha)q(x)$ *для некоторого полинома* $q(x) \in P[x]$ *(для* $q(x) \in F[x]$*).*

Доказательство. По теореме о делении с остатком для многочленов $f(x) = (x - \alpha)q(x) + r(x)$, где $r(x)$ – многочлен степени, меньшей 1, то есть элемент r поля P. Из полученного равенства следует, что $f(\alpha) = 0$ тогда и только тогда, когда $r = 0$. Теорема доказана.

Следствие. *Неприводимый полином кольца* $P[x]$ *степени* $n \geq 2$ *не имеет корней в поле* P.

Теорема Безу имеет важное теоретическое значение. На практике она позволяет существенно упростить решение алгебраических уравнений: если найден один из корней β полинома $f(x)$, то следует разделить $f(x)$ на $x - \beta$. Тогда остальные корни полинома $f(x)$ являются корнями полинома $q(x)$ – частного от деления $f(x)$ на $x - \beta$.

Определение 3.6.2. *Пусть* α *полинома* $f(x) \in P[x]$. *Кратностью корня* α *называется такое натуральное* $k \geq 1$, *что* $f(x)$ *делится на* $(x - \alpha)^k$, *но не делится на* $(x - \alpha)^{k+1}$. *При* $k = 1$ *корень* α *называется простым, а при* $k > 1$ – *кратным.*

Теорема 3.6.2. *Пусть* $f(x) \in P[x]$ – *многочлен степени* $n \geq 1$. *Если* $\alpha_1, \alpha_2, ..., \alpha_m$ – *корни* $f(x)$ *кратностей* $k_1, k_2, ..., k_m$ *соответственно, то* $f(x)$ *делится на произведение* $(x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2} \cdot ... \cdot (x - \alpha_m)^{k_m}$. *Следовательно,* $k_1 + k_2 + ... + k_m \leq n$ *и многочлен* $f(x)$ *имеет не более* n *корней.*

Доказательство. По определению кратного корня $f(x)$ делится на $(x - \alpha_i)^{k_i}$ для каждого целого i, $1 \leq i \leq m$. По условию $\alpha_i \neq \alpha_j$ при $i \neq j$. Тогда биномы $(x - \alpha_i)^{ki}$ и $(x - \alpha_j)^{k_j}$ попарно взаимно просты при $i \neq j$.

Тогда согласно предложению 3.5.3 $f(x)$ делится на произведение $(x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}\cdot\ldots\cdot(x-\alpha_m)^{k_m}$. Такое деление возможно только в случае, когда $m \le k_1+k_2+\ldots+k_m \le n$. Следовательно, $f(x)$ может иметь не более чем n корней. Теорема доказана.

Определение 3.6.3. *(Формальной) производной многочлена* $f(x)=a_0+a_1x+\ldots+a_nx^n \in P[x]$ над произвольным полем P называется многочлен $f'(x)=a_1+2a_2x+\ldots+na_nx^n \in P[x]$.

Формальность производной здесь объясняется тем, что не во всех полях имеет место понятие предела. Это отражается и на свойствах формальной производной. Обычно производная полинома степени n есть полином $(n-1)-$й степени. Однако если $charP=p>0$, то полиномы некоторых достаточно больших степеней могут иметь нулевую формальную производную.

Пример 3.6.1. В поле P характеристики $p>0$ $(ax^{p^2}+bx^p+c)'=0$; $(f(x^p))'=0$ для произвольного полинома $f(x)\in P[x]$.

Тем не менее формальная производная наследует основные свойства производных. Непосредственная проверка позволяет убедиться в справедливости следующих свойств формальной производной для полиномов:

1) $(cf(x))'=c(f(x))'$ для произвольного $c\in P$;

2) $(f(x)+g(x))'=(f(x))'+(g(x))'$;

3) $(f(x)\cdot g(x))'=(f(x))'\cdot g(x)+f(x)\cdot(g(x))'$.

Методом математической индукции доказывается свойство

4) $((x-\alpha)^n)'=n(x-\alpha)^{n-1}$.

С помощью отмеченных свойств 3 и 4 доказывается

Теорема 3.6.3. *Корень α полинома $f(x)\in P[x]$ является кратным корнем этого полинома тогда и только тогда, когда он одновременно является корнем производной $f'(x)$.*

Следствие. *Если производная $f'(x)$ не имеет корней, то полином $f(x)$ не имеет кратных корней. В частности, в поле характеристики $p>0$ полином $x^{p^n}-x$ не имеет кратных корней.*

Упражнение 3.6.1. Доказать, что неприводимый полином $g(x)\in P[x]$, степень которого взаимно проста с характеристикой поля P, не имеет кратных корней ни в поле P, ни в любом поле $F\supset P$.

Теорема 3.6.4. *Для неприводимости полинома степени 2 или 3 в кольце $P[x]$ необходимо и достаточно, чтобы он не имел корней в поле P.*

Для неприводимости полинома степени 4 или 5 в кольце $P[x]$ необходимо и достаточно, чтобы он не имел корней в поле P и не делился ни на какой (неприводимый) полином второй степени. И так далее.

Данная теорема позволяет, в частности, реализовать «решето Эратосфена» для нахождения неприводимых полиномов той или иной степени над конечным полем. По теореме Безу нахождение у полинома делителей первой степени эквивалентно проверке элементов поля на корень полинома. Как показано в предыдущем разделе, список неприводимых полиномов малых степеней над конечным полем достаточно ограничен.

3.7. Характерные свойства кольца полиномов

Теорема 3.7.1. *Кольцо полиномов* $P[x]$ *с коэффициентами из поля* P *является ассоциативным коммутативным кольцом с единицей и без делителей нуля.*

Доказательство заключается в скрупулезном умножении полиномов с учетом того, что полином равен нулю тогда и только тогда, когда все его коэффициенты при всех степенях переменной x равны нулю, а два полинома равны между собой тогда и только тогда, когда равны коэффициенты при одинаковых степенях x. На основании сказанного докажем методом от противного отсутствие делителей нуля в кольце $P[x]$. Предположим, что найдутся в кольце $P[x]$ два полинома $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0$ и $g(x) = b_k x^k + b_{k-1}x^{k-1} + ... + b_0$, где $a_n \neq 0$, $b_k \neq 0$, такие, что их произведение равно нулю. Но произведение $f(x)g(x)$ есть полином степени $n+k$ со старшим коэффициентом, равным $a_n b_k$ и, следовательно, отличным от нуля, так как в поле нет делителей нуля. Получается противоречие с условием равенства нулю полинома.

Теорема 3.7.2. *Кольцо полиномов* $P[x]$ *с коэффициентами из поля* P *является кольцом главных идеалов.*

Доказательство. Теорема утверждает, все идеалы в кольце полиномов являются главными. Пусть $J -$ собственный идеал кольца $P[x]$. Пусть $m(x) -$ полином наименьшей степени, принадлежащий идеалу J. Степень $\deg m(x)$ полинома $m(x)$ больше нуля, иначе $J = P[x]$. Любой полином $f(x) \in J$ должен делиться на $m(x)$. В противном случае по теореме о делении с остатком $f(x) = m(x)q(x) + r(x)$ для некоторого полинома $r(x)$, степень которого меньше $\deg m(x)$. Но тогда $r(x) = f(x) - m(x)q(x) \in J$, что противоречит выбору $m(x)$. В таком случае, $J =< m(x) > -$ главный идеал, порожденный полиномом $m(x)$. Теорема доказана.

Упражнение 3.7.1. Убедиться, что множество всех полиномов кольца $P[x]$ с коэффициентами из поля P без свободных членов, включая и нулевой полином, является идеалом. Указать порождающий этот идеал полином $m(x)$.

Замечание. Теорема 3.7.1 останется справедливой, если P заменить на коммутативное ассоциативное кольцо K без делителей нуля, например, кольцом целых чисел Z или другим кольцом полиномов $P[t]$. Теорема 3.7.2 при этом, вообще говоря, перестает быть верной.

Пример 3.7.1. Кольцо полиномов $Z[x]$ с целыми коэффициентами не является кольцом главных идеалов. Действительно, все полиномы вида $2n + xf(x)$ образуют собственный идеал J, однако он не является главным. Если $J =< g(x) >$ для некоторого полинома с целыми коэффициентами, то 2 делится на $g(x)$. Следовательно, $g(x) -$ многочлен нулевой степени, а точнее или 1, или -1, или 2. Первые два случая невозможны, ибо тогда $J = Z[x]$, но и третий случай невозможен, так как тогда идеал J должен состоять из всех полиномов с четными коэффициентами и, следовательно, не может содержать полинома x. Полученное противоречие означает, что идеал J не является главным.

Пример 3.7.2. Кольцо полиномов $R[t,x]$ с двумя независимыми переменными t, x не принадлежит к классу колец главных полиномов. Аналогично примеру 3.7.1 доказывается, что множество полиномов вида $tf(t,x) + xg(t,x)$ для произвольных $f(t,x), g(t,x) \in R[t,x]$ является идеалом, но не главным идеалом.

Теорема 3.7.3. *В кольце полиномов $P[x]$ с коэффициентами из поля P идеал $J =< m(x) >$ максимален тогда и только тогда, когда порождающий его полином $m(x)$ неприводим над полем P.*

Доказательство следует из шестого пункта теоремы 3.4.1.

Упражнение 3.7.2. Максимальны ли идеалы, порожденные полиномами:

а) $x^4 + 81, \quad x^4 + 13x^2 + 49, \quad x^3 + 2004x - 2005$ в кольце $R[x]$;

б) $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \quad x^6 + x^5 + x^4 + x + 1$ в кольце $(Z/2Z)[x]$?

3.8. Фактор-кольца

Пусть $K -$ кольцо с собственным двусторонним идеалом J. По определению J является подгруппой аддитивной группы $(K,+) = K^+$. Следовательно, на K определено отношение сравнения по модулю J: элементы $a, c \in K$ сравнимы по модулю J тогда и только тогда, когда $a - c \in J$, то есть когда $a = c + iu$ для некоторых $u \in K, i \in J$. Это отношение является отношением эквивалентности и, следовательно, разбивает K на непересекающиеся классы сравнимых друг с другом по модулю J элементов кольца K. Идеал $J -$ нормальная подгруппа группы K^+ в силу абелевости K^+. Тогда согласно теореме 2.10.1 фактор-множество $K/J = \{\overline{0} = J, \overline{a} = a + J, \overline{b} = b + J, ...\}$ является абелевой группой

относительно индуцированной операции сложения $\oplus$: $\bar{a} \oplus \bar{b} = (a+J)+(b+J) = (a+b)+J = \overline{a+b}$ – тот класс эквивалентности по модулю J, в который попадает элемент $a+b$.

На фактор-множестве K/J определена индуцированная операция умножения $\otimes$: произведением классов $\bar{a}$ и $\bar{b}$ является тот единственный класс $\bar{c} \in K/J$, который содержит произведения $a_1 b_1$ любых представителей $a_1 \in \bar{a}$ и $b_1 \in \bar{b}$. Докажем единственность класса $\bar{c}$. Пусть $a_1 b_1 \in \bar{c}$ и $a_2 \in \bar{a}, b_2 \in \bar{b}$. Тогда $a_2 = a_1 + i, b_2 = b_1 + j$ для подходящих $i, j \in J$. В таком случае произведение $a_2 b_2 = (a_1 + i)(b_1 + j) = a_1 b_1 + a_1 j + i b_1 + ij = a_1 b_1 + j_1$ для некоторого $j_1 \in J$ в силу нормальности идеала J. Полученное равенство означает, что $a_2 b_2$ также принадлежит классу $\bar{c}$, что и требовалось доказать. Таким образом, $\bar{a} \otimes \bar{b} = (a+J)(b+J) = ab + J = \overline{ab}$.

Поскольку операции $\oplus$ и $\otimes$ полностью определяются сложением и умножением в кольце K, то свойства этих операций переносятся на $(K,+)/(J,+)$. Поэтому, в частности, индуцированные операции связаны свойством дистрибутивности: $(\bar{a} \oplus \bar{b}) \otimes \bar{c} = (\bar{a} \otimes \bar{b}) \oplus (\bar{b} \otimes \bar{c})$; если K – ассоциативное кольцо (с единицей), то и K/J также будет ассоциативным кольцом (с единицей $\bar{1}$); если K – коммутативно, то и K/J – коммутативно. Таким образом, доказана

Теорема 3.8.1. *Пусть K – ассоциативное кольцо с единицей и с собственным двусторонним идеалом J. Тогда фактор-множество K/J является ассоциативным кольцом с единицей относительно индуцированных с кольца K операций. Если при этом кольцо K коммутативно, то и фактор-кольцо K/J коммутативно.*

Определение 3.8.1. *Фактор-кольцом кольца K по двустороннему идеалу J называется кольцо из теоремы 8.1, то есть фактор-множество K/J с индуцированными операциями $\oplus$ и $\otimes$.*

Пример 3.8.1. Кольцо классов вычетов Z/nZ есть фактор-кольцо кольца целых чисел Z по двустороннему идеалу $J = nZ$.

Пример 3.8.2. Возьмем в кольце полиномов $P[x]$ с коэффициентами из поля P произвольный собственный идеал J. Согласно теореме 3.7.2 идеал $J = < f(x) >$ для некоторого полинома $f(x)$ степени $n \geq 1$. Согласно второму пункту теоремы 2.5.2 в один класс смежности по модулю J попадают те и только те полиномы, разность которых делится на $f(x)$, то есть те, которые имеют один и тот же остаток $r(x)$ от деления на $f(x)$. Отсюда следует, что фактор-кольцо $P[x]/J$ состоит из классов $\overline{r(x)} = r(x) + J = \{r(x) + f(x)q(x);\ q(x) \in P[x]\}$, где степень $r(x)$ меньше степени полинома $f(x)$.

Пример 3.8.3. Пусть в примере 3.8.2 $P = Z / pZ$. В кольце $(Z / pZ)[x]$ имеется, как не трудно заметить, в точности p^n различных полиномов степени, меньшей n. Поэтому для полинома $f(x)$ степени $n \geq 1$ фактор-кольцо $(Z / pZ)[x] / < q(x) >$ конечно (иной, отличный от Z / nZ пример конечного коммутативного кольца с единицей) и состоит из p^n элементов. Следовательно, сложение и умножение в этом кольце можно задать конкретно в виде таблиц.

Пример 3.8.4. Кольцо $F = (Z / 2Z)[x] / < x^2 + x + 1 >$ состоит из смежных классов $\bar{0}, \bar{1}, \bar{x}, \overline{x+1}$. Напишем таблицы сложения и умножения в этом кольце.

		$\bar{1}$		
		$\bar{1}$		
		$\bar{0}$		
		$\bar{x}$		
		$\bar{x}$		

$\otimes$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{1}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{1}$	$\bar{x}$

Из таблицы умножения следует, что в кольце F все ненулевые элементы обратимы относительно умножения, то есть $F^* = F \setminus \{0\}$. Следовательно, F – поле из четырёх элементов.

Развитием примера 3.8.4 и теоремы 3.8.1 является следующий результат.

Теорема 3.8.2. *Фактор-кольцо K / M ассоциативного и коммутативного кольца K с единицей по максимальному идеалу M есть поле.*

Доказательство. Возьмем произвольный ненулевой класс $\bar{a} \in K / M$. В силу максимальности идеала M найдутся такие $m \in M, k \in K$, что выполняется равенство $ak + m = 1$. Тогда $\overline{ak + m} = \overline{ak} + \bar{m} = \overline{ak} + M =$

$= \overline{ak} + \overline{0} = \overline{ak} = \overline{a}\overline{k} = \overline{1}$. Отсюда следует, что $\overline{a}^{-1} = \overline{k}$. Таким образом, в фактор-кольце K/M каждый ненулевой класс обратим относительно индуцированной операции умножения. С учетом теоремы 3.7.1 это означает, что K/M – поле. Теорема доказана.

Из теорем 3.7.3 и 3.8.2 вытекает

Следствие 1. *Для произвольного поля P фактор-кольцо $P[x]/<q(x)>$, где $q(x)$ – неприводимый полином, является полем.*

Следствие 2. *Для неприводимого над полем Z/pZ полинома $q(x)$ степени n фактор-кольцо $(Z/pZ)[x]/<q(x)>$ является конечным полем из p^n элементов.*

3.9. Гомоморфизмы колец и полей

Определение 3.9.1. *Гомоморфизмом колец называется всякое отображение φ из одного кольца K в другое кольцо K', обладающее для произвольных $x, y \in K$ свойствами: 1) $\varphi(x+y) = \varphi(x) + \varphi(y)$; 2) $\varphi(xy) = \varphi(x)\varphi(y)$. Если при этом φ – биекция, то такой гомоморфизм называется изоморфизмом колец.*

Всякий гомоморфизм $\varphi : K \to K$ называют эндоморфизмом кольца K, а взаимно однозначный эндоморфизм – автоморфизмом кольца K.

Пример 3.9.1. Для любых двух колец K и K' найдется гомоморфизм из K в K'. Примером такого гомоморфизма является нулевое отображение или аннулятор кольца K, то есть такое отображение $\varphi : K \to K'$, что $\varphi(x) = 0$ для всякого $x \in K$.

Пример 3.9.2. В любом кольце K найдутся по крайней мере два различных эндоморфизма. К ним относятся: 1) аннулятор кольца K; 2) тождественное отображение $e_K : K \to K$, такое, что $e_K(x) = x$ для каждого $x \in K$.

Пример 3.9.3. Пусть $K = K' = C$ – поле комплексных чисел. Для каждого комплексного числа $z = a + bi; a, b \in R$, положим $\varphi(z) = \overline{z} = a - bi$, то есть каждому комплексному числу отображение φ ставит в соответствие комплексно сопряженное число. Очевидно, операция сопряжения взаимно однозначна и удовлетворяет обоим условиям гомоморфизма колец. Следовательно, φ – автоморфизм поля комплексных чисел, причём $\varphi^2 = e_C$.

Пример 3.9.4. Внутренний автоморфизм матричного кольца $M_n(R)$ – это отображение $f : X \to AXA^{-1}$ для произвольной квадратной матрицы X порядка n и фиксированной невырожденной матрицы $A \in M_n(R)$. В силу дистрибутивности сложения и умножения матриц $\varphi(X+Y) = \varphi(X) + \varphi(Y)$; $\varphi(XY) = AXYA^{-1} = (AXA^{-1})(AYA^{-1}) = \varphi(X)\varphi(Y)$. Таким образом оба условия из определения гомоморфизма колец выполняются.

Пример 3.9.5. Пусть K – кольцо с двусторонним идеалом J. Сюръективный гомоморфизм аддитивных групп $\varphi: K^+ \to K^+/J^+$, который каждому элементу $a \in K$ ставит в соответствие элемент $\overline{a} = a + J$ фактор-группы K^+/J^+ (см. раздел 2) продолжается до гомоморфизма колец. Это так называемый канонический гомоморфизм.

Пример 3.9.6. Пусть $K = C$ – поле комплексных чисел, $K' = M_2(R)$ – кольцо матриц. Отображение $\varphi: C \to M_2(R)$, такое, что $\varphi(a+bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, как легко проверить, является инъективным гомоморфизмом.

Отметим основные свойства кольцевых гомоморфизмов.

Теорема 3.9.1. *Для произвольного ненулевого гомоморфизма $\varphi: K \to K'$ справедливы следующие соотношения:*

1) $\varphi(0_K) = 0_{K'}$;

2) $\varphi(-a) = -\varphi(a)$;

3) $\varphi(e_K) = e_{K'}$;;

4) $\varphi(a^{-1}) = (\varphi(a))^{-1}$;

5) $Ker\varphi = \{x \in K;\ \varphi(x) = 0_{K'}\}$ – *двусторонний идеал кольца* K;

6) $\mathrm{Im}\varphi$ – *образ кольца* K *в* K' *при отображении* φ – *множество всех тех* $y \in K'$, *для каждого из которых существует* $x \in K$, *такой, что* $\varphi(x) = y$, – *подкольцо кольца* K'.

Доказательство. Для произвольного $a \in K$ $\varphi(a) = \varphi(0 + a) = \varphi(0) + \varphi(a)$. Следовательно, $\varphi(0) = \varphi(a) - \varphi(a) = 0_{K'}$ Тем самым доказано первое соотношение. Далее, $\varphi(0) = \varphi(a - a) = \varphi(a + (-a)) = \varphi(a) + \varphi(-a) = 0_{K'}$. Это доказывает второе соотношение. Существуют такие $a \in K$, что $\varphi(a) \neq 0$. При этом $\varphi(a) = \varphi(e_K a) = \varphi(e_K)\varphi(a) = \varphi(ae_K) = \varphi(a)\varphi(e_K)$. Следовательно, $\varphi(e_K)$ является нейтральным элементом в кольце K'. В силу единственности нейтрального элемента отсюда получаем доказательство третьего соотношения. Пусть a – обратимый элемент кольца K. Четвертое соотношение вытекает из равенства: $e_{K'} = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$. Пятое утверждение теоремы следует из леммы 3.1.1 и определения двустороннего идеала.

Следствие 1. *Гомоморфизм $\varphi: K \to K'$ является инъективным тогда и только тогда, когда $Ker\varphi = 0_{K'}$.*

Доказательство. Для различных элементов $x, y \in K$ их образы равны $\varphi(y) = \varphi(x)$ тогда и только тогда, когда $\varphi(y - x) = 0_{K'}$, то есть когда ненулевой элемент $y - x$ кольца K принадлежит $Ker\varphi$, то есть когда ядро гомоморфизма φ отлично от нуля.

Из пятой части теоремы 3.9.1 и отсутствия собственных идеалов у полей вытекает

Следствие 2. *Любой гомоморфизм произвольных полей является либо нулевым, либо инъективным, в частности, любой ненулевой эндоморфизм поля является автоморфизмом. Если* $\varphi: P \to P' -$ *инъективный гомоморфизм поля* P *в поле* P', *то* $\varphi(P) -$ *поле, изоморфное полю* P.

Гомоморфизмы полей позволяют произвести отождествления полей, установить между ними отношения частичного порядка – по включению.

Пример 3.9.7. Пусть $f -$ естественное вложение поля P в кольцо $P[x]$ (всякий элемент $\alpha \in P$ отождествляется с полиномом нулевой степени из $P[x]$). Пусть $p(x) -$ произвольный неприводимый полином из $P[x]$. Пусть $\varphi: P[x] \to \tilde{P} = P[x]/ < p(x) > -$ сюръективный гомоморфизм из примера 3.9.5. Он является ненулевым на P $(\varphi(1) = \overline{1} \neq \overline{0})$.

Согласно следствию 1 из теоремы 3.7.2 кольцо $\tilde{P}$ является полем. Следовательно, композиция отображений $g = \varphi f: P \to \tilde{P}$ является, в силу сказанного выше, инъективным отображением P в $\tilde{P}$, иначе говоря, вложением P в $\tilde{P}$. В этом смысле можно говорить, что P является подполем поля $\tilde{P}$. Отсюда следует, что если $p(x) = x + b -$ полином 1-й степени из $P[x]$, то $\tilde{P} = P$, точнее, $\tilde{P}$ изоморфно полю коэффициентов P в кольце полиномов. Если же $\deg p(x) > 1$, то отображение g является настоящим вложением поля P в большее поле $\tilde{P}$.

Теорема 3.9.2. *Для всякого двустороннего идеала* J *кольца* K *существует кольцо* K' *и гомоморфизм* $\varphi: K \to K'$ *с ядром* $Ker\varphi = J$.

Доказательство. Требованиям теоремы удовлетворяет кольцо $K' = K/J$ и канонический гомоморфизм $\varphi: K \to K'$, ставящий в соответствие каждому $a \in K$ класс смежности $\overline{a} = a + J$ (см. пример 3.9.5).

4. Теория полей и конечных полей

4.1. Характеристика поля

Поля выделяются из общего многообразия коммутативных колец наличием максимально возможной мультипликативной группы – в нее входят все ненулевые элементы, отсутствием делителей нуля, отсутствием собственных идеалов. Неотъемлимым атрибутом, важнейшим из свойств каждого поля является его характеристика.

Определение 4.1.1. *Если в поле* P *существует такое натуральное* n, *что равна нулю сумма* n *единиц (*n *раз складывается с самим собой* 1 – *нейтральный элемент относительно умножения):* $1+1+...+1=0$, *то наименьшее* n *с таким свойством называется характеристикой поля* P *и обозначается через* $charP$. *Если в поле* P *любая конечная сумма единиц отлична от нуля, то говорят, что характеристика поля* P *равна 0.*

Теорема 4.1.1. *Если характеристика поля отлична от нуля, то она является числом простым.*

Доказательство. Предположим, что поле P имеет конечную характеристику n, причем $n=km$ – число составное. По определению это означает, что в поле P некоторые конечные суммы из одной единицы равны нулю, причем наименьшая из таких сумм содержит n слагаемых, n единиц. Эту, равную нулю, сумму n единиц можно, пользуясь свойством ассоциативности сложения сгруппировать в m групп по k единиц в каждой. Сумма k единиц – это какой-то ненулевой элемент $b\in P$. Таким образом, равная нулю сумма n единиц равна сумме m элементов b, то есть произведению b на сумму из k единиц, равную какому-то отличному от нуля элементу $c\in P$. Значит, мы имеем произведение $bc=0$ для ненулевых $b,c\in P$. Это противоречит отсутствию делителей нуля в поле (см. следствие из теоремы 3.4.1). Следовательно, $charP=n$ не может быть составным числом. Теорема доказана.

Пример 4.1.1. В поле $P=Z/pZ$, p – простое число, характеристика равна p. В самом деле, Z/pZ является аддитивной группой из p элементов и, следовательно, циклической группой порядка p, порожденной любым ненулевым элементом, в частности, единицей – нейтральным элементом относительно умножения. Согласно теореме 2.4.2 о структуре циклических групп $Z/pZ=\{\overline{1},\overline{1}+\overline{1}=\overline{2},...,\overline{1}+\overline{1}+...+\overline{1}=\overline{p-1},\overline{1}+\overline{1}+...+\overline{1}=\overline{0}\}$. Это и означает, что $char(Z/pZ)=p$.

Пример 4.1.2. Поля Q,R,C имеют, очевидно, характеристику 0.

Определение 4.1.2. *Поле* P *называется подполем поля* P', *если все его элементы принадлежат полю* P'.

Теорема 4.1.2. *Если подполе поля P имеет характеристику p, то и поле P имеет ту же характеристику. Все подполя поля P имеют ту же характеристику.*

Доказательство следует из единственности нейтрального элемента в группе и, следовательно, из единственности единицы в любом поле.

Со школьной скамьи мы привыкли к полям характеристики 0. С их точ-ки зрения арифметика полей положительной характеристики весьма экзотична.

Теорема 4.1.3. *Пусть P – произвольное поле положительной характеристики p. Пусть n – произвольное целое число и r – остаток от деления n на p. Тогда для каждого элемента $a \in P$ имеет место равенство: $na = ra$. В частности, при $n = pq$ произведение $na = pqa = 0$. Если $p = 2$, то при $n = 2k$ произведение $na = 2ka = 0$, а при $n = 2k + 1$ произведение $na = (2k + 1)a = a$.*

Доказательство. Произведение $na = a + a + ... + a = a(1 + 1 + ... + 1)$ – сумма n одинаковых слагаемых, равных a. В силу закона дистрибутивности эта сумма представима в виде произведения a на сумму из n единиц. В силу ассоциативности сложения и определения характеристики в последней сумма каждых p единиц равна нулю. Отсюда и вытекает утверждение теоремы.

Мы хорошо знаем формулу бинома Ньютона: $(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k$. (Здесь уместно отметить факт исторической несправедливости: формула, носящая имя Ньютона, была известна ещё в X в., например, знаменитому среднеазиатскому поэту и философу Омару Хайяму). В полях характеристики p при $n = p^k$ формула бинома Ньютона выглядит совершенно по-другому.

Теорема 4.1.4. *Пусть $charP = p > 0$. Тогда для любых $a, b \in P$ $(a+b)^p = a^p + b^p$; $(a-b)^p = a^p - b^p$; а для каждого целого $k \geq 1$ $(a+b)^{p^k} = a^{p^k} + b^{p^k}$; $(a-b)^{p^k} = a^{p^k} - b^{p^k}$.*

Доказательство. Заметим, что все биномиальные коэффициенты $C_p^k, 1 \leq k < p$, являются целыми числами и вычисляются по формуле: $C_p^k = p(p-1) \cdot ... \cdot (p-k+1) \big/ 1 \cdot 2 \cdot ... \cdot k$. Числитель данной дроби делится на p, ни один из множителей знаменателя не может быть делителем p в силу простоты этого числа. Следовательно, C_n^k делится на p. Тогда, согласно теореме 1.3, соответствующие слагаемые бинома Ньютона равны нулю, что доказывает первую формулу для бинома Ньютона в характеристике p. Остальные формулы доказываются аналогично.

Пример 4.1.3. Пусть P – поле характеристики p и g – вложение P в поле $\tilde{P} = P[x]/ < p(x) >$ (см. пример 2.8.6) для неприводимого полинома $p(x) \in P[x]$. Тогда, согласно теореме 4.1.2, $\tilde{P}$ – также поле характеристики p.

Заметим, что существуют бесконечные по количеству элементов поля конечной характеристики. Примером такого поля является поле рациональных функций, то есть дробей $\frac{f(x)}{g(x)}$, где $f(x)$ и $g(x) \neq 0$ – полиномы из $(Z/pZ)[x]$, с естественными операциями сложения и умножения дробей.

4.2. Подполя и минимальные подполя

Обычно поле имеет достаточно большой спектр подполей.

Пример 4.2.1. Поле рациональных чисел Q – подполе поля вещественных чисел R, а оно в свою очередь является подполем поля комплексных чисел C. Между C и Q, между R и Q существует бесконечно много промежуточных подполей. Для каждого простого числа p полином $x^2 - p$ неприводим над Q, согласно критерию Эйзенштейна (теорема 3.5.5 ; впрочем, можно и непосредственно убедиться, что $\sqrt{p}$ не является рациональным числом); непосредственнными вычислениями можно убедиться, что множество $K = \{a + b\sqrt{p}; a,b \in Q\}$ является полем. Это подполе поля R, содержащее Q в качестве своего подполя. Аналогично образует поле множество $F = \{a + bi; a,b \in Q\}$ комплексных рациональных чисел. Оно содержит Q и принадлежит полю комплексных чисел C.

На многообразии всех подполей данного поля определено отношение частичного порядка по включению, обладающее свойством транзитивности. Также имеет место

Теорема 4.2.1. *Пересечение подполей поля P' является подполем поля P'.*

Доказательство следует из соответствующего свойства групп.

Определение 4.2.2. *Минимальным, или простым, называется поле, не содержащее собственных подполей.*

Теорема 4.2.2. *Поле рациональных чисел Q – минимальное поле характеристики 0; Z/pZ – минимальное поле характеристики p.*

Доказательство. Пусть P – подполе поля Q. Оно содержит обязательно 0 и 1. Следовательно, P содержит циклическую аддитивную группу, порожденную числом 1, то есть группу целых чисел Z. В таком случае P содержит обратные относительно умножения ко всем целым

числам, то есть все рациональные числа вида $1/n$. Но тогда любое рациональное число k/n как произведение целого числа k на рациональное число $1/n$ принадлежит полю P. Это означает, что $Q = P$, то есть что Q – минимальное поле.

Пусть P – подполе поля Z/pZ. Оно содержит обязательно $\overline{0}$ и $\overline{1}$. Следовательно, P содержит циклическую аддитивную группу, порожденную числом $\overline{1}$, то есть группу $<\overline{1}>=\{\overline{1}, \overline{1}+\overline{1}=\overline{2},..., \overline{1}+\overline{1}+...+\overline{1}=\overline{p-1}, \overline{1}+\overline{1}+...+\overline{1}=\overline{0}\}$, состоящую из p элементов. Это означает, что P содержит все элементы поля Z/pZ и, следовательно, совпадает с ним. Теорема доказана.

Теорема 4.2.3. *В любом поле P имеется в точности одно минимальное подполе, изоморфное либо Q, либо Z/pZ в зависимости от характеристики поля P.*

Доказательство. Докажем существование минимального поля. Пусть K – пересечение множества M всех подполей данного поля P. Если бы K содержало собственное подполе F, то F принадлежало бы M, но тогда пересечение подполей не может быть большим, чем F, поэтому $K = F$, что доказывает минимальность поля K.

Докажем единственность минимального поля. Если бы в поле P существовало несколько различных минимальных подполей, то их пересечение было бы меньшим подполем, что противоречило бы минимальности пересекающихся подполей.

Пусть характеристика поля P равна нулю. Согласно теореме 4.1.2 ее минимальное подполе K имеет ту же характеристику. Пусть $\tilde{1}$ – нейтральный элемент этого поля относительно умножения. По определению характеристики циклическая группа $<\tilde{1}>$, порожденная этим элементом относительно сложения, бесконечна и изоморфна группе Z целых чисел относительно сложения. Построим ненулевой гомоморфизм $\varphi: Q \to K$ по следующему правилу: $\varphi(0)=0; \varphi(1)=\tilde{1}; \varphi(n)=\tilde{1}+\tilde{1}+...+\tilde{1}$ – сумма из n единиц поля K. Из последнего соотношения следует, что $\varphi(n+m)=\varphi(n)+\varphi(m), \varphi(nm)=\varphi(n)\varphi(m)$ для любых целых n, m. При этом $\varphi(n) \neq 0$ для каждого целого ненулевого n, иначе получили бы противоречие с равенством $charP = 0$. Продлим гомоморфизм φ с кольца Z на Q, полагая $\varphi(1/n)=1/\varphi(n); \varphi(m/n)=\varphi(m)/\varphi(n)$. Такое определение корректно – нетрудно убедиться, что под действием φ все эквивалентные дроби имеют одинаковый образ. Тогда простая проверка показывает, что для произвольных $q_1, q_2 \in Q$ $\varphi(q_1 q_2)=\varphi(q_1)\varphi(q_2)$; $\varphi(q_1+q_2)=\varphi(q_1)+\varphi(q_2)$, то есть φ – ненулевой гомоморфизм поля Q в поле K. Согласно следствию 2

из теоремы 3.8.1 $\varphi(Q)$ – подполе поля K, изоморфное Q. В силу минимальности K имеем: $\varphi(Q) = K$ – изоморфизм полей.

Пусть характеристика поля P равна $p > 0$. Согласно теореме 4.1.2 ее минимальное подполе K имеет ту же характеристику. По определению характеристики циклическая группа $<\tilde{1}>$, порожденная этим элементом относительно сложения, конечна и изоморфна аддитивной группе Z/pZ классов вычетов по модулю p. Построим ненулевой гомоморфизм $\varphi: Z/pZ \to K$ по следующему правилу: $\varphi(\bar{0}) = 0; \varphi(\bar{1}) = \tilde{1}; \varphi(\bar{n}) = \tilde{1} + \tilde{1} + ... + \tilde{1}$ – сумма из n единиц поля K для каждого натурального $n, 1 \le n \le p-1$. Из последнего соотношения следует, что $\varphi(\bar{n} + \bar{m}) = \varphi(\bar{n}) + \varphi(\bar{m}), \varphi(\bar{n}\bar{m}) = \varphi(\bar{n})\varphi(\bar{m})$ для произвольных классов $\bar{n}, \bar{m} \in Z/pZ$. Согласно следствию 2 из теоремы 3.8.1 полный образ $\varphi(Z/pZ)$ есть подполе поля K, изоморфное полю Z/pZ. В силу минимальности поля K мы имеем равенство $\varphi(Z/pZ) = K$, что и означает изоморфизм полей K и Z/pZ. Теорема полностью доказана.

4.3. Векторные пространства и расширения полей

Определение и основные свойства векторных пространств над полем R переносятся на произвольные поля. При этом векторное пространство над конечным полем имеет свои особенности.

Теорема 4.3.1. *Пусть V – n-мерное линейное пространство над полем $F(q)$ из q элементов. Тогда V состоит из q^n векторов.*

Доказательство индукцией по размерности n пространства V. При $n = 1$ все векторы коллинеарны одному ненулевому вектору, то есть отличаются от него множителем из $F(q)$, следовательно, мощность $|V| = q$.

Предположим, что для $n = k \ge 1$ мощность $|V| = |V_k| = q^k$, докажем, что $|V_{k+1}| = q^{k+1}$. Действительно, все векторы пространства V_{k+1} размерности $k+1$ представляют собой всевозможные линейные комбинации $x_1\bar{e}_1 + x_2\bar{e}_2 + ... + x_k\bar{e}_k + x_{k+1}\bar{e}_{k+1}$ векторов фиксированного базиса $\bar{e}_1, \bar{e}_2, ..., \bar{e}_{k+1} \in V_{k+1}$ с коэффициентами $x_i \in F(q)$. При каждом конкретном значении x_{k+1} имеется по предположению индукции q^k различных таких линейных комбинаций. Таким образом, в пространстве V_{k+1} имеется всего $q^k \cdot q = q^{k+1}$ векторов, что и требовалось доказать.

Определение 4.3.1. *Если P является подполем поля F, то F называют расширением поля P.*

Очевидно, любое расширение произвольного поля P является векторным пространством над P.

Определение 4.3.2. *Расширение F поля P называется конечным (степени n), если размерность векторного пространства F над полем P конечна (и равна n). Степень расширения принято обозначать через* $[F:P]$.

Пример 4.3.1. Уже первокурсники знают, что поле комплексных чисел является расширением степени два поля вещественных чисел.

Из теоремы 4.3.1 получаем, что расширение F степени n конечного поля $F(q)$ из q элементов состоит из q^n элементов.

Теорема 4.3.2 (о башне расширений полей). *Если поле F есть расширение поля P степени n, а поле H – расширение F степени m, то H есть расширение P степени $[H:P]=mn$.*

Доказательство. Пусть $f_1, f_2, ..., f_n$ – базис пространства F над полем P, пусть $h_1, h_2, ..., h_m$ – базис пространства H над полем F. Система элементов поля H

$$\begin{array}{cccc} h_1f_1 & h_2f_1 & \ldots & h_mf_1 \\ h_1f_2 & h_2f_2 & \ldots & h_mf_2 \\ \ldots & \ldots & \ldots & \ldots \\ h_1f_n & h_2f_n & \ldots & h_mf_n \end{array}$$

линейно независима над полем P, является системой образующих линейного пространства H над полем P. Иными словами, – это базис H над P. Следовательно, $[H:P]=mn$. Теорема доказана.

Следствие. *Если степень расширения $[F:P]=q$ – число простое, то поле F не содержит подполей, промежуточных между F и P.*

Упражнение 4.3.1. Выяснить, может ли расширение степени два поля P (поля Q) быть подполем расширения того же поля P (поля Q) степени 3?

Упражнение 4.3.2. Какие подполя содержит расширение 127-й степени поля $Z/2Z$, а расширение 4-й степени того же поля?

4.4. Алгебраические элементы и алгебраические расширения полей

Определение 4.4.1. *Элемент $\alpha \in F$ – расширения поля P является алгебраическим над полем P, если существует полином $f(x) \in P[x]$, корнем которого является α, то есть $f(\alpha)=0$. В противном случае α называют трансцендентным над P элементом. Поле F называется алгебраическим расширением поля P, если всякий элемент из F является алгебраическим над полем P.*

Пример 4.4.1. Всем хорошо известно, что числа π, e – трансцендентные над Q вещественные числа. К ним относятся числа π^e, 0,123456789… - число, содержащее после запятой последовательно записанные числа натурального ряда, многие другие. Известно, что мощность множество вещественных чисел – континуум, а множество всех алгебраических над Q чисел – счетное. Поэтому трансцендентных вещественных чисел существенно больше, чем вещественных алгебраических, чем рациональных чисел.

Теорема 4.4.1. *Всякое конечное расширение произвольного поля P является алгебраическим над P.*

Доказательство. Пусть $[F:P]=n>1$. Пусть α – произвольный элемент поля F, не принадлежащий P. Система $1,\alpha,\alpha^2,...,\alpha^n$ из $n+1$ векторов линейного n – мерного пространства F над полем P обязательно линейно зависима. Поэтому найдутся такие элементы $c_0,c_1,...,c_n \in P$, что $c_0+c_1\alpha+...+c_n\alpha^n=0$. Это означает, что α – корень полинома $f(x)=c_0+c_1x+...+c_nx^n \in P[x]$, то есть $\alpha \in F$ – алгебраический над P элемент.

Следствие 1. *Если расширение F поля P содержит трансцендентные над полем P элементы, то степень этого расширения бесконечна.*

Следствие 2. *Степень расширения* $[R:Q]=+\infty$.

Упражнение 4.4.1. Показать непосредственно, что каждое конкретное комплексное число $z=a+bi$ является алгебраическим над полем вещественных чисел R.

Теорема 4.4.2. *Пусть α – алгебраический над полем P элемент. Множество J_α полиномов $f(x)\in P[x]$, для которых $f(\alpha)=0$, есть максимальный идеал кольца $P[x]$.*

Доказательство. Легко проверяется, что множество полиномов с корнем α образует группу относительно сложения и идеал в кольце $P[x]$. Согласно теореме 3.6.2 идеал J_α – главный. Пусть $J_\alpha =< g(x) >$. Предположим, что $g(x)$ приводим, раскладывается в произведение неприводимых полиномов: $g(x)=a_n p_1(x)^{t_1} p_2(x)^{t_2} \cdot ... \cdot p_s(x)^{t_s}$. Поскольку в поле нет делителей нуля, то из условия: $g(\alpha)=0$ следует, что для некоторого целого $i, 1\le i\le s$, $p_i(\alpha)=0$. Это означает, что $p_i(x)$ принадлежит идеалу J_α. Степень полинома $p_i(x)$ меньше $\deg(g(x))$. Поэтому $p_i(x)$ может делиться на $g(x)$ только в том случае, когда отличается от него лишь множителем из поля P. Получено противоречие с предположением. Следовательно, J_α – максимальный идеал.

Следствие. *Пусть* $f(x)$ *– неприводимый полином из* $P[x]$ *с корнем* α *из расширения* F *поля* P. *Пусть для* $g(x) \in P[x]$ $g(\alpha) = 0$. *Тогда* $g(x)$ *делится на* $f(x)$.

Определение 4.4.2. *Пусть* $\alpha \in F$ *– алгебраический над полем* P *элемент. Минимальным полиномом элемента* α *над полем* P *называется неприводимый полином* $Irr(\alpha, P, x)$ *в кольце* $P[x]$, *старший коэффициент которого равен 1, а одним из корней является элемент* α.

Теорема 4.4.3. *Пусть* F *– расширение поля* P, *пусть* $\alpha \in F$ *– алгебраический над* P *элемент с минимальным над* P *полиномом степени* $n > 1$. *Пусть* $P(\alpha)$ *– минимальное подполе поля* F, *содержащее* P *и* α. *Тогда степень расширения* $[P(\alpha) : P] = n$, *а поле* $P(\alpha)$ *имеет следующую структуру:* $P(\alpha) = \{a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}; a_i \in P, 0 \le i \le n-1\}$.

Доказательство. Тот факт, что $P(\alpha)$ содержит всевозможные выражения вида $a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}$ с коэффициентами $a_i \in P$, не вызывает сомнений. Пусть $Irr(\alpha, P, x) = g(x) = x^n + c_{n-1}x^{n-1} + ... + c_1x + c_0$. α является корнем этого полинома. Следовательно, $\alpha^n = -c_{n-1}\alpha^{n-1} - ... - c_1\alpha - c_0$. Тогда $\alpha^{n+1}, \alpha^{n+2}$ и так далее, все степени элемента α, большие n – й, выражаются аналогичным образом в виде линейных комбинаций элементов $1, \alpha, ..., \alpha^{n-1}$. Произвольное выражение $a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}$ с коэффициентами $a_i \in P$ есть значение полинома $\varphi(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1}$ при $x = \alpha$. $НОД(\varphi(x), g(x)) = 1$, поскольку $g(x)$ – неприводим. Согласно критерию взаимной простоты полиномов (теорема 3.5.4), существуют такие полиномы $u(x), v(x)$, что $\varphi(x)u(x) + g(x)v(x) = 1$. Подставим в это равенство вместо x значение α. Получим: $\varphi(\alpha) \cdot u(\alpha) = 1$. Следовательно, $(\varphi(\alpha))^{-1} = u(\alpha) = b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1}$ для подходящих $b_j \in P, 0 \le j \le n-1$. Таким образом, множество $K = \{a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}; a_i \in P, 0 \le i \le n-1\}$ является полем, содержащим $P(\alpha)$. Однако $P(\alpha)$ не может быть собственным подполем поля K, поскольку элементы $1, \alpha, ..., \alpha^{n-1}$ образуют линейно независимую систему (в противном случае α было бы корнем полинома степени, меньшей $n = \deg g(x)$). Следовательно, $P(\alpha) = K$, что и требовалось доказать.

Пример 4.4.2. С точки зрения теоремы 4.4.3 поле комплексных чисел C – алгебраическое расширение поля R – минимальное поле, содержащее R и алгебраическое над ним комплексное число $\alpha = i$ – корень неприводимого полинома $x^2 + 1$. В полном согласии с утверждением теоремы 4.4.3 поле C имеет следующую структуру $C = R(i) = \{a + bi; a, b \in R\}$.

Теорема 4.4.4. *В условиях теоремы 4.4.3 поле* $P(\alpha)$ *изоморфно полю – фактор-кольцу* $P[x]/<Irr(\alpha,P,x)>$.

Доказательство. Согласно примеру 3.7.2 названное в теореме фактор-кольцо состоит из классов смежности, порожденных остатками от деления многочленов на $g(x)=Irr(\alpha,P,x),$ а с учетом примера 3.8.6 – из выражений вида: $a_0+a_1\overline{x}+...+a_{n-1}\overline{x}^{n-1}$ для произвольных коэффициентов $a_i\in P.$ Класс смежности $\overline{Irr(\alpha,P,x)}=\overline{x^n+c_{n-1}x^{n-1}+...+c_1x+c_0}=\overline{0}.$ Поэтому названные выражения в фактор-кольце умножаются с учетом того, что $\overline{x}^n=-c_{n-1}\overline{x}^{n-1}-...-c_1\overline{x}-c_0.$ Построим отображение $\varphi: P(\alpha)\to K=P[x]/<Irr(\alpha,P,x)>$ по следующему правилу: $\varphi(a_0+a_1\alpha+...+a_{n-1}\alpha^{n-1})=a_0+a_1\overline{x}+...+a_{n-1}\overline{x}^{n-1}.$ Такое отображение является, очевидно, взаимно однозначным гомоморфизмом соответствующих аддитивных групп. Отображение φ удовлетворяет также и мультипликативному свойству кольцевых гомоморфизмов: для произвольных $z,t\in P(\alpha)$ $\varphi(zt)=\varphi(z)\varphi(t),$ поскольку и $P(\alpha)$ и в фактор-кольце K умножение подчинено одинаковому соотношению для степеней α и $\overline{x}$ соответственно. Поэтому $\varphi-$изоморфизм полей, что и требовалось доказать.

Теорема 4.4.5. *Для всякого неприводимого полинома* $f(x)\in P[x]$ *степени* $n>1$ *существует расширение поля* P *степени n, содержащее корень этого полинома.*

Доказательство. Пусть $f(x)=d_nx^n+d_{n-1}x^{n-1}+...+d_0\in P[x].$ Фактор-кольцо $K=P[x]/<f(x)>$ состоит из всевозможных выражений $\overline{a}_0+\overline{a}_1\overline{x}+...+\overline{a}_{n-1}\overline{x}^{n-1};a_i\in P,$ содержит корень $\overline{x}$ полинома $\overline{f(x)}=\overline{d}_n\overline{x}^n+\overline{d}_{n-1}\overline{x}^{n-1}+...+\overline{d}_0.$ Классы смежности $\overline{d}$ в поле K для всех $d\in P$ образуют поле, изоморфное полю $P.$ Присоединим к полю P символ $\alpha,$ то есть рассмотрим группу Φ относительно сложения всевозможных выражений вида $a_0+a_1\alpha+...+a_{n-1}\alpha^{n-1}$ с произвольными коэффициентами $a_i\in P.$ Построим изоморфизм аддитивных групп $h: K\to\Phi$ по правилу: для произвольного элемента фактор-кольца $K-$класса смежности $\overline{m}(\overline{x})=\overline{a}_0+\overline{a}_1\overline{x}+...+\overline{a}_{n-1}\overline{x}^{n-1}\in K$ положим $h(\overline{m}(\overline{x}))=h(\overline{a}_0+\overline{a}_1\overline{x}+...+\overline{a}_{n-1}\overline{x}^{n-1})=a_0+a_1\alpha+...+a_{n-1}\alpha^{n-1}=m(\alpha).$ Группу Φ наделим структурой поля, определив на ней умножение по формуле: $m_1(\alpha)m_2(\alpha)=h(\overline{m}_1(\overline{x})\overline{m}_2(\overline{x}))$ для произвольных $m_1(\alpha),m_2(\alpha)\in\Phi.$ Ясно, что поля K и Φ изоморфны и Φ содержит корень α полинома $f(x).$

Замечание. Тот факт, что поле $P(\alpha)$ содержит корень α полинома $g(x)=Irr(\alpha,P,x),$ вовсе не означает, что $P(\alpha)$ содержит все корни этого полинома.

Пример 4.4.3. Уравнение $x^3 - 2 = 0$ не имеет рациональных корней согласно критерию Эйзенштейна. Это уравнение имеет следующие три иррациональные корня: $\sqrt[3]{2}; (-1 + i\sqrt{3})\sqrt[3]{2}/2; (-1 - i\sqrt{3})\sqrt[3]{2}/2.$ Поле $Q(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4}; a, b, c \in Q\}$ содержит только первый из перечисленных корней.

Определение 4.4.3. *Расширение F поля P называется полем разложения полинома $f(x) \in P[x]$, если оно содержит все корни этого полинома.*

Такое название мотивировано теоремой Безу о корнях полиномов – при наличии в поле F всех корней полинома $f(x)$ последний раскладывается в произведение полиномов 1-й степени – двучленов вида $x - \alpha$.

Теорема 4.4.6. *Для всякого полинома $f(x) \in P[x]$ существует поле $F \supseteq P$ – конечное расширение поля P – поле разложения полинома $f(x)$.*

Доказательство применением теоремы 4.4.5 в сочетании с теоремой Безу.

4.5. Свойства конечных полей: существование и единственность

Конечные поля были впервые введены в математическую практику в начале XIX в. гениальным французским математиком Эваристом Галуа. Поэтому конечные поля часто называют полями Галуа, а также на письме обозначают через $GF(q)$ – поле Галуа из q элементов. Будем использовать и более краткое обозначение этого же поля – $F(q)$. Из предыдущих результатов данного раздела следует

Теорема 4.5.1. *Любое конечное поле $GF(q)$ элементов имеет конечную характеристику $p > 0$, является конечным расширением поля Z/pZ, содержит $q = p^k$ элементов, при этом k – степень расширения $[GF(q) : Z/pZ]$.*

Из теоремы Лагранжа о конечных группах следует, что все элементы мультипликативной группы $GF(q)^*$ удовлетворяют уравнению $x^{q-1} - 1 = 0$. На самом деле имеет место

Теорема 4.5.2 (о существовании и единственности конечного поля). *Для каждого простого числа p и для любого натурального $n \geq 1$ существует конечное поле из $q = p^n$ элементов. Это поле единственно с точностью до изоморфизма состоит из корней уравнения $x^q - x = 0$ и только из них.*

Доказательство. Если требуемое конечное поле существует, то его элементы обязательно удовлетворяют уравнению $x^q - x = 0$ в силу теоремы Лагранжа и разложения $x^q - x = x(x^{q-1} - 1) = 0.$

Докажем существование требуемого конечного поля. Многочлен $\varphi(x) = x^q - x$ принадлежит кольцу полиномов $(Z / pZ)[x]$. Согласно теореме 4.6 существует конечное расширение F поля Z / pZ, являющееся полем разложения данного полинома. Формальная производная $\varphi'(x) = -1 \neq 0.$ Это означает, согласно следствию из теоремы 3.6.3, что уравнение $x^q - x = 0$ не имеет кратных корней. Следовательно, уравнение $x^q - x = 0$ имеет в поле F в точности q различных корней. Обозначим через S множество всех этих корней. S содержит $0, 1 \in Z / pZ.$ Для произвольных $a, b \in S$ согласно теореме 4.1.4 $(a - b)^q = a^q - b^q$, а по условию $a^q = a, b^q = b.$ Следовательно, $(a - b)^q = a - b,$ то есть $a - b \in S.$ Согласно критерию подгруппы, это означает, что множество S является группой относительно сложения. Аналогично доказывается, что все ненулевые элементы множества S образуют группу относительно умножения. Таким образом, S является полем, полем из q элементов – корней полинома $x^q - x.$

Любое расширение поля Z / pZ может содержать не более q корней уравнения $x^q - x = 0.$ В противном случае полином мог бы иметь в силу теоремы Безу различные разложения в произведения неприводимых полиномов – биномов вида $x - \alpha.$ А это противоречит теореме 3.5.5 о единственности разложения полинома в произведение неприводимых сомножителей. Другое, изоморфное конечное поле из q элементов получается, если только рассматривается и другое минимальное поле, изоморфное по теореме 4.2.3 полю $Z / pZ.$ Теорема доказана.

Теорема 4.5.3. *Пусть $F(p^n)$ и $F(p^k)$ – конечные поля, расширения поля $Z / pZ = F(p)$, причем $1 < k < n.$ Поле $F(p^k)$ является подполем $F(p^n)$ тогда и только тогда, когда k делит $n.$ Для каждого натурального делителя d числа n существует и единственно подполе $F(p^n)$ из p^d элементов.*

Доказательство. Согласно теореме 4.5.1 поля $F(p^k)$ и $F(p^n)$ являются расширениями минимального поля $F(p)$ степени k и n соответственно. Пусть поле $F(p^k)$ является подполем $F(p^n).$ Тогда в силу теоремы 3.2 о башне расширений полей k делит $n.$

Пусть k делит $n,$ то есть $n = ks$ для подходящего натурального $s > 1.$ Согласно одной из формул сокращенного умножения (в чем, впрочем, можно убедиться и непосредственными вычислениями), что справедливо следующее равенство: $p^n - 1 = (p^k)^s - 1 = (p^k - 1)((p^k)^{s-1} + (p^k)^{s-2} + ... + 1) = (p^k - 1)t.$ Таким образом,

$\tilde{q} = p^k - 1$ делит $q = p^n - 1$: $q = \tilde{q}t$. Тогда по той же формуле сокращенного умножения доказывается, что полином $x^{\tilde{q}} - 1$ делит полином $x^q - 1$, то есть корни многочлена $x^{\tilde{q}} - 1$ находятся среди корней полинома $x^q - 1$. Это означает, что $F(p^k)$ является подполем поля $F(p^n)$.

Единственность подполя для каждого d, делящего n, следует из теоремы 4.5.2. Таким образом, утверждение полностью доказано.

4.6. Свойства конечных полей: цикличность мультипликативной группы

Теорема 4.5.2 характеризует ненулевые элементы полей Галуа как корни из 1. Мультипликативные свойства корней из 1 и в полях характеристики 0 (см. пример 2.4.1) и любой характеристики $p > 0$ идентичны.

Теорема 4.6.1. *Мультипликативная группа конечного поля – циклическая.*

Доказательство. Порядок $\left|GF(p^n)^*\right| = p^n - 1$. Согласно теореме Лагранжа порядок каждого элемента этой группы является делителем числа $p^n - 1$. Пусть d – наибольший из этих порядков. $d \le p^n - 1$. Тогда порядок каждого элемента из $GF(p^n)^*$ делит d. Если бы нашелся элемент $\gamma \in GF(p^n)^*$ порядка $\nu < d$, такого, что d не делится на ν и, следовательно, $НОД(d,\nu) = \tilde{d} < \nu$, то для $\beta \in GF(p^n)^*$ порядка d элемент $\beta\gamma$ имеет, как несложно видеть, порядок μ, равный наименьшему общему кратному чисел d и ν, то есть числу $(d\nu)/\tilde{d} > d$. Получаем противоречие с выбором d. Таким образом, порядки всех элементов мультипликативной группы поля Галуа $GF(p^n)$ делят d. Следовательно, все элементы этой группы – корни уравнения $x^d - 1 = 0$. Это означает, что $p^n - 1 \le d$. С учетом отмеченного выше противоположного неравенства получаем: $p^n - 1 = d$. Но тогда циклическая группа, порожденная элементом β, совпадает с $GF(p^n)^*$. Теорема доказана.

Замечание 1. Данная теорема является обобщением теоремы 2.4.5 о цикличности мультипликативной группы $(Z/pZ)^*$.

Замечание 2. Имеет место следующее обобщение теоремы 4.6.1: любая конечная подгруппа мультипликативной группы P^* каждого поля P является циклической.

Замечание 3. Мультипликативные группы бесконечных полей не цикличны (см., в частности, упражнение 2.4.2).

Определение 4.6.1. *Образующие мультипликативной группы конечного поля называют примитивными элементами этого поля.*

4.7. Свойства примитивных элементов конечных полей

Теорема 4.7.1. *Каждый примитивный элемент поля Галуа* $F(p^n)$ *является корнем неприводимого полинома степени* n *из кольца* $F(p)[x]$.

Доказательство. Пусть α – примитивный элемент поля $F(p^n)$. Это расширение поля $F(p)$ степени n согласно теореме 4.5.1. Пусть $F = F(p)(\alpha)$ – минимальное подполе поля $F(p^n)$, содержащее $F(p)$ и α (см. теорему 4.3). Это подполе содержит 0 и все степени элемента α, а значит, все элементы поля $F(p^n)$. Следовательно, $F(p^n) = F$. Согласно теореме 4.4.3 степень расширения $[F : F(p)] = n$ совпадает со степенью минимального полинома элемента α над полем $F(p)$. Таким образом, $\deg Irr(\alpha, F(p), x) = n$. Теорема доказана.

Следствие. *Для каждого натурального* n *над полем* $F(p)$ *существует неприводимый полином степени* n.

Лемма 4.7.1. *Пусть* $f(x)$ – *неприводимый полином над полем* $F(p)$ *степени* m. $f(x)$ *делит полином* $x^{p^n} - x$ *тогда и только тогда, когда* m *делит* n.

Доказательство. Пусть $F(p^m)$ – поле из теоремы 4.7.2, построенное по полиному $f(x)$ и содержащее, согласно следствию 2 из теоремы 4.7.2 все корни этого полинома. Пусть $F(p^n)$ – поле из теоремы 4.5.2, состоящее из корней полинома $x^{p^n} - x$. Согласно теореме 4.5.3 поле $F(p^m)$ является подполем поля $F(p^n)$ тогда и только тогда, когда m делит n. С другой стороны, поле $F(p^m)$ является подполем поля $F(p^n)$ тогда и только тогда, когда $f(x)$ делит полином $x^{p^n} - x$. Лемма доказана.

Лемма 4.7.2. *Для каждого натурального* $n > 1$ *все неприводимые полиномы степени* n *кольца* $Z / pZ[x]$ *раскладываются на линейные множители (имеют все корни) в поле* $F(p^n)$, *причем все корни каждого из названных полиномов попарно различны.*

Доказательство. Любой неприводимый полином $f(x)$ степени n из кольца $Z / pZ[x]$ должен быть делителем полинома $x^{p^n} - x$. Последний раскладывается на линейные множители над полем $F(p^n)$ в силу теоремы 4.5.2. Автоматически тогда раскладывается на линейные множители и данный неприводимый полином. Как отмечено в процессе доказательства

теоремы 4.5.2, полином $x^{p^n} - x$ не имеет кратных корней. Следовательно, и его делитель – полином $f(x)$ также имеет все попарно различные корни. Лемма доказана.

Дальнейшим развитием леммы 4.7.2 является

Теорема 4.7.2. *Пусть α – корень неприводимого полинома $f(x) \in Z/pZ[x]$ степени n, принадлежащий полю $F(p^n)$. Тогда остальными корнями полинома $f(x)$ являются элементы $\alpha^p, \alpha^{p^2}, ..., \alpha^{p^{n-1}} \in F(p^n)$.*

Доказательство. Пусть $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0$. Все коэффициенты этого полинома $a_i \in Z/pZ$ и потому удовлетворяют условию: $a_i^p = a_i$. Подставим α^{p^k} в полином $f(x)$. В силу теоремы 4.1.4 имеем

$$f(\alpha^{p^k}) = a_n(\alpha^{p^k})^n + a_{n-1}(\alpha^{p^k})^{n-1} + ... + a_0 = (a_n\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_0)^{p^k} = 0.$$

Таким образом, названные элементы являются корнями полинома $f(x)$. Осталось доказать, что названные элементы попарно различны. Предположим, что найдутся целые s и $t, 0 \le s < t \le n-1$, для которых $\alpha^{p^s} = \alpha^{p^t}$. Обе части полученного равенства возведем в степень p^{n-t}. Получим $\alpha^{p^{n-t+s}} = \alpha^{p^n} = \alpha$. Тогда, согласно следствию из теоремы 4.4.2, полином $x^{p^{n-t+s}} - x$ делится на $f(x)$. По лемме 4.7.1 это возможно тогда и только тогда, когда $n-t+s$ делится на n. Но $0 < n-t+s < n$ и мы получаем противоречие. Теорема доказана.

Теорема 4.7.2 позволяет доказать другое важное свойство примитивных элементов.

Теорема 4.7.3. *Если α – примитивный элемент поля $F(p^n)$, корень неприводимого полинома $f(x) \in Z/pZ[x]$, то и остальные корни этого полинома являются примитивными элементами поля $F(p^n)$.*

Доказательство. Согласно теореме 4.7.2 остальные корни полинома $f(x)$ имеют вид $\alpha^{p^k}, 1 \le k \le n-1$. Все корни данного полинома принадлежат мультипликативной группе $F(p^n)^*$, имеющей порядок $p^n - 1$. Для каждого целого $k, 1 \le k \le n-1$, число p^k взаимно просто с $p^n - 1$. Тогда согласно теореме 2.12.3 отображение $\varphi_k : F(p^n)^* \to F(p^n)^*$ такое, что для каждого $\beta \in F(p^n)^*$ $\varphi_k(\beta) = \beta^{p^k}$, является автоморфизмом группы $F(p^n)^*$. Тогда согласно теореме 2.12.4 порядки элементов α и $\varphi_k(\alpha)$ совпадают, то есть все они являются примитивными элементами поля $F(p^n)$.

Определение 4.7.1. *Неприводимый полином* $f(x) \in Z/pZ[x]$ *степени* n *называется примитивным полиномом, если его корни – примитивные элементы поля Галуа* $F(p^n)$.

Из теорем 4.6.1, 4.7.1, 4.7.3 вытекает

Теорема 4.7.4. *Для каждого натурального* $n > 1$ *в кольце* $Z/pZ[x]$ *существуют примитивные полиномы степени* n.

Заметим, что в кольце $Z/pZ[x]$ для значений n с условием: число $p^n - 1$ – простое, все неприводимые полиномы степени n являются примитивными, поскольку при таких условиях в мультипликативной группе $F(p^n)^*$ все элементы, кроме 1, являются примитивными элементами поля $F(p^n)$. Если же $p^n - 1$ – составное целое число, то, как показывают эмпирические вычисления, в кольце $Z/pZ[x]$ обязательно находятся неприводимые, как примитивные так и не примитивные полиномы.

Пример 4.7.1. В подразделе 3.5 раздела 3 приведен список неприводимых полиномов над полем $Z/2Z$. Среди них – неприводимые полиномы 4-й степени, всего три полинома. Под № 6 списка фигурирует полином $f(x) = x^4 + x^3 + x^2 + x + 1$. Это не примитивный полином. Действительно,

пусть α – корень $f(x)$, принадлежащий полю $F(2^4)$. Порядок $F(2^4)^* = 15$. Найдем порядок элемента α в этой группе. Согласно следствию 1 из теоремы 4.5.6 $\alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1$. Тогда $\alpha^5 = \alpha \cdot \alpha^4 = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = (\alpha^3 + \alpha^2 + \alpha + 1) + \alpha^3 + \alpha^2 + \alpha = 1$. Таким образом, элемент α имеет мультипликативный порядок 5 и, следовательно, не является примитивным. Но тогда и полином $f(x)$ непримитивен.

По схеме, приведенной в примере 4.7.1, можно разделять неприводимые полиномы на примитивные и непримитивные.

4.8. Формирование конечных полей

Характеризация конечных полей как множеств корней уравнений специального вида позволила доказать единственность таких полей данного порядка. Для организации вычислений в конечных полях требуется явное конструктивное задание полей Галуа, четкая методика формирования элементов этих полей. Данной цели служит

Теорема 4.8.1. *Для каждого натурального* n *и фиксированного простого числа* p *существует единственное расширение* $F(p^n)$ *поля* Z/pZ, *состоящее из* p^n *элементов, оно изоморфно полю* $(Z/pZ)[x]/<p(x)>$ *для любого неприводимого полинома* $p(x)$ *степени* n *из кольца* $Z/pZ[x]$.

Доказательство. Для данных p и $n>1$ обычно существует несколько неприводимых полиномов степени n над полем Z/pZ. Для каждого полинома получается свое фактор-кольцо. Но по теореме 4.5.2 все эти фактор-кольца изоморфны полю, состоящему из корней уравнения $x^{p^n}-x=0$.

Следствие. *Всякое конечное поле $F(p^n)$ состоит из всевозможных полиномов степени, меньшей n, с коэффициентами из поля $F(p)=Z/pZ$. Складываются и вычитаются эти полиномы как обычно, умножаются почленно с учетом равенства $x^n=-a_{n-1}x^{n-1}-...-a_1x-a_0$ для фиксированного неприводимого полинома степени n из кольца $Z/pZ[x]$.*

Согласно следствию из теоремы 4.8.1 неприводимые полиномы необходимы для формирования конечных полей и вычислений в них: данное поле $F(p^n)$ можно рассматривать как множество сумм вида $\{a_0+a_1\alpha+...+a_{n-1}\alpha^{n-1}\,|\,a_i\in F(p)\}$, где $\alpha-$корень неприводимого полинома $f(x)$ степени n из кольца $F(p)[x]$. В отдельных ситуациях для формирования конечных полей пользуются принципиально не примитивными полиномами (например, в криптосистеме AES). Однако тогда умножение элементов поля Галуа требует громоздких выкладок. Для непосредственных вычислений в полях Галуа удобнее формировать их с помощью примитивных полиномов. Ведь если $\alpha-$ примитивный элемент поля $F(p^n)$, то все элементы этого поля исчерпываются множеством $\{0,\alpha,\alpha^2,...,\alpha^{p^n-1}=1\}$ и перемножать степени α друг с другом намного проще и удобнее. Чтобы сочетать оба преимущества следует задавать поле либо в виде системы равенств (отождествляющих оба способа задания поля), либо в виде таблицы степеней и сумм.

Пример 4.8.1. Сформируем поле $F(8)=F(2^3)$. Поскольку $2^3-1=7-$число простое, то над полем из двух элементов все неприводимые полиномы третьей степени являются примитивными. Зафиксируем неприводимый полином степени 3, например, $p(x)=x^3+x+1$. Обозначим через α его корень, принадлежащий $F(8)$. Тогда $\alpha^3=\alpha+1$ (так как характеристика поля $F(8)$ равна 2, то $-1=1$). Тогда $\alpha^4=\alpha^2+\alpha$, $\alpha^5=\alpha^3+\alpha^2=\alpha^2+\alpha+1$, $\alpha^6=\alpha^3+\alpha^2+\alpha=\alpha^2+1$, $\alpha^7=\alpha^3+\alpha=\alpha+\alpha+1=1$, $0=\alpha^{-\infty}$. Следовательно, поле $F(8)$ можно задать в виде таблицы из двух столбцов: в левом столбце запишем все различные степени α, в правом – соответствующие этим степеням суммы вида $a_0+a_1\alpha+a_2\alpha^2$:

Таблица элементов поля $F(8)$

$\alpha^{-\infty}$	0
α^1	α
α^2	α^2

α^3 | $\alpha+1$
α^4 | $\alpha^2+\alpha$
α^5 | $\alpha^2+\alpha+1$
α^6 | α^2+1
α^7 | 1.

Пример 4.8.2. Решить над полем $F(8)$ следующую систему уравнений:

$$\begin{cases}(\alpha^2+1)x+(\alpha^2+\alpha+1)y=1,\\ \alpha^2 x+(\alpha+1)y=\alpha^2+1.\end{cases}$$

Решим систему по правилу Крамера. Для вычислений воспользуемся приведенной выше таблицей задания поля $F(8)$. Определитель матрицы коэффициентов системы

$$\delta=\begin{vmatrix}\alpha^2+1 & \alpha^2+\alpha+1\\ \alpha^2 & \alpha+1\end{vmatrix}=\alpha^3+\alpha^2+\alpha+1+\alpha^4+\alpha^3+\alpha^2=\alpha^2+1.$$

$$\delta_x=\begin{vmatrix}1 & \alpha^2+\alpha+1\\ \alpha^2+1 & \alpha+1\end{vmatrix}=\alpha+1+\alpha^4+\alpha^3+\alpha^2+\alpha^2+\alpha+1=\alpha^4+\alpha^3=(\alpha^2+\alpha)+(\alpha+1)=\alpha^2+1;$$

$\delta_y=\begin{vmatrix}\alpha^2+1 & 1\\ \alpha^2 & \alpha^2+1\end{vmatrix}=\alpha^4+1+\alpha^2=\alpha+1.$ Следовательно, $x=\delta_x/\delta=1;$

$y=\delta_y/\delta=(\alpha+1)/(\alpha^2+1)=1/\alpha^3=\alpha^4=\alpha^2+\alpha.$

Итак, задание элементов поля Галуа суммами удобно при сложении элементов поля, для умножения удобнее пользоваться степенным заданием элементов поля.

Конечные поля имеют многочисленные приложения. Без них немыслимо функционирование практически всех цифровых систем связи.

Пример 4.8.3. В системе связи, построенной на основе БЧХ-кода C с проверочной матрицей $H=(\alpha^i,\alpha^{3i})^T$, $0\le i\le 14$, $\alpha-$примитивный элемент поля Галуа $F(16)$, корень полинома x^4+x+1, (см. [14]), выяснить, не содержит ли ошибок принятое сообщение $\overline{x}=(111011110110101)$.

Решение задачи. Все кодовые слова $\overline{c}\in C$ (и только они) составляют ядро проверочной матрицы: $H\cdot(\overline{c}^T)=\overline{0}.$ Если $\overline{s}=H(\overline{x}^T)\ne\overline{0},$ то сообщение $\overline{x}$ явно содержит ошибки, а вектор $\overline{s}$ называют синдромом этих ошибок. В данном случае $\overline{s}=(s_1,s_2)^T$, где

$s_1=1+\alpha+\alpha^2+\alpha^4+\alpha^5+\alpha^6+\alpha^7+\alpha^9+\alpha^{10}+\alpha^{12}+\alpha^{14};$

$s_2=1+\alpha^3+\alpha^6+\alpha^{12}+\alpha^{15}+\alpha^{18}+\alpha^{21}+\alpha^{27}+\alpha^{30}+\alpha^{36}+\alpha^{42}.$ Читателю предлагается сформировать по аналогии с примером 4.8.1 конечное поле $F(16)$, провести необходимые вычисления и убедиться, что $s_1=\alpha^{11}=\alpha^3+\alpha^2+\alpha;$ $s_2=\alpha.$ Таким образом, полученное сообщение $\overline{x}$ содержит ошибки.

4.9. Автоморфизмы полей. Группа Галуа конечного поля

В конце раздела 3 представлены свойства гомоморфизмов колец. В частности, показано, что ненулевые гомоморфизмы полей инъективны. Следовательно, ненулевые эндоморфизмы полей являются автоморфизмами. Повторяя доказательство теоремы 2.12.2 применительно к кольцам или полям, можно легко убедиться, что автоморфизмы любого поля F образуют группу, обозначаемую через $AutF$. Эварист Галуа первым в истории нашел применение автоморфизмам полей в математике – показал, что алгебраическое уравнение $f(x)=0$ разрешимо в радикалах над полем рациональных чисел тогда и только тогда, когда группа автоморфизмов расширения $Q[x]/<f(x)>$, порожденного полиномом $f(x)$, разрешима. К сожалению, изложение этой в высшей степени интересной теории удвоило бы объемы данного пособия.

Перейдем к изучению свойств автоморфизмов полей.

Теорема 4.9.1. *Пусть φ – автоморфизм поля F. Инварианты автоморфизма φ, то есть те элементы $x\in F$, для которых $\varphi(x)=x$, образуют подполе в поле F.*

Доказательство. Множество $M(\varphi)\subset F$ инвариантов автоморфизма φ не пусто – содержит по крайней мере 0 и 1. Если $x,y\in M(\varphi)$, то в силу свойства 2 из теоремы 3.8.1 гомоморфизмов колец $\varphi(x-y)=x-y$. Следовательно, $M(\varphi)$ – группа относительно сложения. Аналогично доказывается, что ненулевые элементы $M(\varphi)$ образуют группу относительно умножения. Но тогда $M(\varphi)$ – поле. Теорема доказана.

Следствие 1. *Любой автоморфизм поля действует тождественно на минимальном подполе.*

Следствие 2. *Группа автоморфизмов любого минимального поля тривиальна - состоит из единственного тождественного автоморфизма e.*

Определение 4.9.1. *Если $M(\varphi)=K$, то φ называют K – автоморфизмом поля F.*

Легко видеть, что K – автоморфизмы поля F образуют подгруппу в группе $AutF$. Будем ее обозначать через $Aut(F/K)$. Сосредоточимся на изучении $Aut(F/K)$ для конечных расширений F полей K.

Пример 4.9.1. Для поля комплексных чисел C и поля вещественных чисел R группа $Aut(C/R)=\{e,\sigma\}$, где $\sigma(x+iy)=x-iy$ для каждого $x+iy\in C$.

Теорема 4.9.2. *Пусть $[F:K]=n$ и φ – нетождественный K – автоморфизм поля F. Пусть $\alpha\in F$, $\alpha\notin K$. Пусть $f(x)\in K[x]$ – неприводимый полином с корнем α. Тогда $\varphi(\alpha)$ – корень $f(x)$.*

Доказательство является практически дословным повторением первой части доказательства теоремы 4.7.2 и рекомендуется читателю в качестве упражнения.

Следствие. *Пусть* $[F:K]=n$ *и существует такой элемент* $\alpha \in F$, *что* $F=K(\alpha)$. *Тогда* $|Aut(F/K)| \le n$.

Благодаря отмеченным выше историческим обстоятельствам, в алгебре общепринято следующее

Определение 4.9.2. *Если* $|Aut(F/K)|=[F:K]$, *то поле* F *называется расширением Галуа поля* K, *а группа* $Aut(F/K)$ *называется* г*руппой Галуа этого расширения и обозначается через* $Gal(F/K)$ *или* $G(F/K)$.

Теорема 4.9.3. *Пусть* $F(p^n)$ *– конечное поле характеристики p из* p^n *элементов. Отображение* φ *этого поля в себя, такое, что* $\varphi(x)=x^p$ *для каждого* $x \in F(p^n)$ *есть автоморфизм этого поля (называемый автоморфизмом Фробениуса). При этом* $\varphi^n = e$ *– тождественное отображение и* $|<\varphi>|=n$. *Следовательно,* $F(p^n)$ *– расширение Галуа поля* $F(p)$ *с циклической группой автоморфизмов* $AutF(p^n)=<\varphi>$.

Доказательство. Тот факт, что φ – автоморфизм мультипликативной группы, следует из теоремы 2.12.3, поскольку $НОД(p, p^n-1)=1$. Аддитивность φ следует из теоремы 1.4. $\varphi^n(x)=x^{p^n}(x)=x^{p^n-1}\cdot x=1\cdot x=x$. Очевидно, для примитивного элемента $\alpha \in F(p^n)$ $\varphi^k(\alpha)=\alpha$ для каждого целого $k, 1 \le k < n$. Таким образом, $|<\varphi>|=n$. Тогда в силу следствия из теоремы 4.9.2 группа автоморфизмов $Aut(F(p^n)/F(p))=<\varphi>$. Теорема доказана.

4.10. Норма и след в конечном поле

Пусть F – конечное расширение Галуа поля K степени n. Пусть $G=G(F/K)=\{\sigma_1,\sigma_2,...,\sigma_n\}$ – группа Галуа этого расширения. Важным в теории полей Галуа и их приложений является

Определение 4.10.1. *Нормой произвольного элемента* α *из расширения* F *над полем* K *называется произведение* $N_{F/K}(\alpha)=\sigma_1(\alpha)\cdot\sigma_2(\alpha)\cdot...\cdot\sigma_n(\alpha)$, *следом этого же элемента над полем* K *называется сумма* $Tr_{F/K}(\alpha)=\sigma_1(\alpha)+\sigma_2(\alpha)+...+\sigma_n(\alpha)$.

Если из контекста ясно, о каких полях F и K идет речь, то норму и след обозначают соответственно через $N(\alpha)$ и $Tr\alpha$. Если $F=F(q)$ – конечное поле из $q=p^n$ элементов, $n>1$, является расширением минимального поля $K=F(p)$, то соответствующие норма и след имеют свою специфику и называются абсолютными. Пусть

φ – автоморфизм Фробениуса поля $F(q)$, исследованный в теореме 4.9.3. В силу цикличности группы Галуа $G(F(p^n)/F(p))$ абсолютная норма произвольного элемента $c \in F(q)$ вычисляется по формуле $N(c) = c \cdot \varphi(c) \cdot ... \cdot \varphi^{n-1}(c) = cc^p ... c^{p^{n-1}}$, а абсолютный след элемента с есть сумма $Trc = c + c^p + ... + c^{p^{n-1}}$. В дальнейшем слово «абсолютный», если это ясно по контексту, будем опускать.

Теорема 4.10.1. *Пусть F – конечное расширение Галуа поля K. Норма и след данного расширения обладают следующими свойствами.*

1. *Норма и след любого элемента из поля F принадлежат полю K.*
2. *$N(cd) = N(c) \cdot N(d)$; $Tr(cd) = Trc + Trd$ для произвольных $c, d \in F$.*
3. *Если $c \in K$, то $N(c) = c^n$; $Trc = nc$, где $n = [F : K]$. В частности, в полях характеристики два $Tr1 = 1$ при нечетном n и $Tr1 = 0$ при четном n.*
4. *След является линейным оператором из поля F как линейного пространства над полем K в поле K как одномерное линейное пространство над самим собой; другими словами, $Tr(ax + by) = aTrx + bTry$ для произвольных $x, y \in F$ и произвольных $a, b \in K$.*
5. *Если $\alpha \in F$ является корнем неприводимого полинома $p(x) = x^n + a_{n-1}x^{n-1} + ... + a_0 \in K[x]$, где $n = [F : K]$, то $Tr\alpha = -a_{n-1}$; $N(\alpha) = (-1)^n a_0$.*

Доказательство. Пусть σ – произвольный автоморфизм группы Галуа $G(F/K) = \{\sigma_1, \sigma_2, ..., \sigma_n\}$. Покажем, что $\sigma(N(c)) = N(c)$ для каждого $c \in F$. Действительно, совокупность $\sigma\sigma_1, \sigma\sigma_2, ..., \sigma\sigma_n$ состоит из попарно различных элементов группы $G(F/K)$. В этом легко убедиться методом от противного. Следовательно, данная совокупность содержит все элементы группы Галуа $G(F/K)$. Тогда ясно, что $\sigma(N(c)) = N(c)$. И это справедливо для каждого $\sigma \in G(F/K)$. Значит, элемент $N(c)$ поля F принадлежит подполю инвариантов группы $G(F/K)$, то есть принадлежит полю K. Аналогично проверяется, что $\sigma(Trc) = Trc$. Следовательно, Trc также принадлежит полю K.

Вторая, третья и четвертая части теоремы непосредственно следуют из определения нормы и следа и мультипликативного и аддитивного свойств автоморфизмов полей.

Докажем пятую часть теоремы, причем только для конечных полей, так как для доказательства в общем случае требуется более развернутое изложение теории расширений Галуа произвольных полей. Итак, пусть $K = F(p)$ – минимальное конечное поле из p элементов, p – некоторое простое число. В условиях теоремы поле $K(\alpha)$ – подполе поля F, при этом $[K(\alpha) : K] = n$ в силу теоремы 4.4.3. Следовательно, $K(\alpha) = F$. Далее в силу леммы 4.7.2 поле $F = K(\alpha)$ содержит все n попарно различные корни

полинома $p(x)$. Согласно теореме 4.9.3 элементы группы Галуа $G(F/K)$ являются степенями автоморфизма Фробениуса. Поэтому можно считать, что они имеют следующую структуру: $\sigma_1 = \varphi, \sigma_2 = \varphi^2, ..., \sigma_n = \varphi^n = e$. Тогда в соответствии с теоремой 4.7.2 элементы поля $F - \sigma_1(\alpha), \sigma_2(\alpha), ..., \sigma_n(\alpha)$ – все попарно различные корни полинома $p(x) = x^n + a_{n-1}x^{n-1} + ... + a_0 \in K[x]$. В силу теоремы Безу это означает, что в поле F полином $p(x)$ раскладывается в произведение линейных множителей: $p(x) = (x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) \cdot ... \cdot (x - \sigma_n(\alpha))$. Раскрыв скобки в полученном равенстве и приведя подобные относительно степеней x, получим требуемое в утверждении пятой части теоремы.

Следствие 1. *Если $v_1, v_2, ..., v_n$ – базис поля F как линейного пространства над полем K, то для произвольного элемента $\beta \in F$, представленного в виде линейной комбинации базисных элементов: $\beta = b_1 v_1 + b_2 v_2 + ... + b_n v_n$, след $Tr\beta = b_1 Trv_1 + b_2 Trv_2 + ... + b_n Trv_n$.*

Доказательство следует из четвертой части доказанной теоремы.

Следствие 2. *Для каждого $\beta \in F$ и для каждого $\sigma \in G(F/K)$ конечного расширения Галуа F поля K следы (нормы) элементов β и $\sigma\beta$ одинаковы. В частности, в расширении $F(p^n)$ поля $F(p)$ одинаковы следы (нормы) элементов $\beta, \beta^p, \beta^{p^2}, ..., \beta^{p^{n-1}}$.*

Доказательство является повторением начала доказательства теоремы для совокупности элементов $\sigma_1\sigma, \sigma_2\sigma, ..., \sigma_n\sigma$ группы Галуа $G(F/K)$.

Теорема 4.10.2. *В конечных полях отображение следа $Tr : F(p^n) \to F(p)$ сюръективно.*

Доказательство. Найдем те $x \in F(p^n)$, для которых $Trx = 0$, то есть $x + x^p + ... + x^{p^{n-1}} = 0$. Это уравнение степени p^{n-1}. Ему удовлетворяет не более p^{n-1} корней, то есть в p раз меньше, чем элементов в поле $F(p^n)$. Следовательно, существует $y \in F(p^n)$, такой, что $Try = c \neq 0$. Тогда в силу четвертой части теоремы 4.10.1 для каждого $b \in F(p)$ $Tr(by) = bc$. Если b пробегает все элементы поля $F(p)$, то произведение bc также пробегает все элементы этого же поля. Это и доказывает сюръективность функции следа.

Теорема 4.10.3. *В поле $F(2^n)$ ровно половина элементов имеет след, равный нулю, и ровно половина – след, равный единице.*

Доказательство. Функция следа отображает сюръективно согласно теореме 4.10.2 все элементы из $F(2^n)$ на элементы множества $F(2)$, то есть в 0 или в 1. Пусть M – множество тех $x \in F(2^n)$, след которых равен 0, а N – множество тех $x \in F(2^n)$, след которых равен 1. Пусть $Try = 1$, то есть $y \in N$. Тогда множество $y + N$ имеет мощность, равную мощности

множества N, и принадлежит множеству M. Это означает, в частности, что $|N| \le |M|$. Аналогично, $|y + M| = |M| \le |N|$. Значит, $|N| = |M|$.

Замечание. Конкретное вычисление следа в полях Галуа можно реализовать на основе следствия 1 из теоремы 4.10.1 следующим образом. Всякий элемент поля $F(p^n)$ есть выражение вида $a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0$, где $a_i \in F(p), \alpha -$примитивный элемент поля $F(p^n)$. В силу линейности функции следа (четвертый пункт теоремы 4.10.1) $Tr(a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0) = a_{n-1}Tr(\alpha^{n-1}) + ... + a_1Tr(\alpha) + a_0Tr1$. Вычислив предварительно следы $Tr(\alpha^{n-1}), ..., Tr(\alpha), Tr(1),$ по найденной формуле можно быстро вычислить след любого элемента поля. Еще более быстрый способ вычисления следа будет предложен в следующем разделе с помощью нормального базиса.

4.11. Квадратные уравнения в полях Галуа

Квадратные уравнения в полях Галуа характеристики $p > 2$ решаются стандартным образом с помощью дискриминанта. Проблемы возникают в полях характеристики 2, здесь известная формула корней квадратного уравнения не применима, так как надо делить на 2, то есть на 0, что невозможно. Лишь в XX веке математики под давлением потребностей практики занялись исследованием возникшей ситуации.

Лемма 4.11.1. *Всякое квадратное уравнение* $ax^2 + bx + c = 0$ *с коэффициентами* $a, b, c \in F(2^n)$ *приводится к каноническому виду, то есть к виду* $x^2 + x + \gamma = 0$ *для некоторого* $\gamma \in F(2^n)$.

Доказательство. Разделив уравнение на a, приведем его к виду $x^2 + px + q = 0$ для подходящих $p, q \in F(2^n)$. В полученном уравнении делаем следующую замену переменных: $x = py$. Получим уравнение $p^2y^2 + p^2y + q = 0$ или $y^2 + y + \gamma = 0$ для $\gamma = q / p^2$. Лемма доказана.

Преимущества канонического вида отражает следующая, легко проверяемая с помощью непосредственных вычислений,

Лемма 4.11.2. *Если* $x_0 -$*один из корней уравнения* $x^2 + x + \gamma = 0,$ *то другим корнем этого уравнения является* $x_0 + 1 \in F(2^n)$.

Одним из многочисленных применений функции следа является

Теорема 4.11.1 (Берлекемп, Рамсей, Соломон, 1967). *Уравнение* $x^2 + x + \gamma = 0$ *с элементом* $\gamma \in F(2^n)$ *имеет корни в этом же поле тогда и только тогда, когда* $Tr\gamma = 0$.

Доказательство. Пусть $x_0 \in F(2^n)$ является корнем уравнения $x^2 + x + \gamma = 0$. Тогда $\gamma = x_0 + x_0^2$. В таком случае $Tr\gamma = \gamma + \gamma^2 + \gamma^4 + ... + \gamma^{2^{n-1}} =$

$= (x_0 + x_0^2) + (x_0 + x_0^2)^2 + ... + (x_0 + x_0^2)^{2^{n-1}} = x_0 + x_0^{2^n} = x_0 + x_0^{2^n-1} \cdot x_0 = x_0 + x_0 = 0.$

Пусть $Tr\gamma = 0$. Предположим, что уравнение $x^2 + x + \gamma = 0$ не имеет корней в поле $F(2^n)$. Согласно теореме 4.4.5 существует расширение поля $F(2^n)$, содержащее корень x_1 этого уравнения. Тогда $\gamma = x_1 + x_1^2$ и $Tr\gamma = x_1^{2^n} + x_1 = 0$. Следовательно, $x_1^{2^n} = x_1$ или $x_1^{2^n-1} = 1$, то есть $x_1 \in F(2^n)$.

Следствие. *В поле $F(2^n)$ равенство $Tr\beta = 0$ выполняется тогда и только тогда, когда $\beta = \gamma + \gamma^2$ для подходящего $\gamma \in F(2^n)$.*

Формула корней квадратного уравнения в полях Галуа характеристики 2 выводится с помощью нормального базиса.

Определение 4.11.1. *Пусть F – расширение Галуа поля K степени n с группой Галуа $G(F/K) = \{\sigma_1, \sigma_2, ..., \sigma_n\}$. Если существует такой элемент $\gamma \in F$, что $\sigma_1\gamma, \sigma_2\gamma, ..., \sigma_n\gamma$ – базис линейного* пространства *F над полем K, то этот базис называется нормальным.*

Отметим, что если $F = F(p^n)$ – конечное поле, расширение поля $K = F(p)$, то нормальный базис в силу теоремы 4.9.3 должен иметь вид $\gamma, \gamma^p, ..., \gamma^{p^{n-1}}$.

Теорема 4.11.2(Дэвенпорт, 1968). *Всякое конечное расширение поля Галуа обладает нормальным базисом.*

Замечание. Элемент γ, порождающий нормальный базис в конечном поле $F = F(p^n)$, имеет след, равный 1. Если бы $Tr\gamma = 0$, то согласно шестому пункту теоремы 4.10.1 и все элементы нормального базиса имеют нулевой след. Но тогда по четвертому пункту теоремы 4.10.1 нулевой след должны иметь и все элементы поля $F = F(p^n)$, что противоречит сюръективности функции следа.

Лемма 4.11.3. *Пусть β – произвольный элемент поля $F(2^n)$, заданный в нормальном базисе равенством: $\beta = d_0\gamma + d_1\gamma^2 + ... + d_{n-1}\gamma^{2^{n-1}}$, где $d_i \in F(2)$. Тогда $Tr\beta = d_0 + d_1 + ... + d_{n-1}$.*

Доказательство следует из приведенного выше замечания и теоремы 4.10.1.

Теорема 4.11.3 (Чэнь, 1982). *Пусть у квадратного уравнения $x^2 + x + \gamma = 0$ с элементом $\gamma \in F(2^n)$ след $Tr\gamma = 0$. Пусть $\gamma, \gamma^2, ..., \gamma^{2^{n-1}}$ – нормальный базис поля $F(2^n)$ над минимальным полем $F(2)$. Пусть $\beta = d_0\gamma + d_1\gamma^2 + ... + d_{n-1}\gamma^{2^{n-1}}$ – разложение β по нормальному базису*

для $d_i \in F(2)$. *Тогда* $x_0 = d_1\gamma^2 + (d_1 + d_2)\gamma^4 + ... + (d_1 + d_2 + ...d_{n-1})\gamma^{2^{n-1}}$ *является корнем уравнения* $x^2 + x + \gamma = 0.$

Доказательство. Согласно лемме 4.11.3 $Tr\beta = d_0 + d_1 + ... + d_{n-1} = 0.$ Следовательно, $d_1 + d_2 + ... + d_{n-1} = d_0.$ Подставим x_0 в исследуемое уравнение. Имеем:

$$x_0^2 + x_0 + \beta = d_1\gamma^4 + (d_1 + d_2)\gamma^8 + ... + (d_1 + d_2 + ... + d_{n-1})\gamma^{2^n} +$$
$$+d_1\gamma^2 + (d_1 + d_2)\gamma^4 + ... + (d_1 + d_2 + ...d_{n-1})\gamma^{2^{n-1}} + \beta =$$
$$= d_0\gamma + d_1\gamma^2 + ... + d_{n-1}\gamma^{2^{n-1}} + \beta = \beta + \beta = 0.$$

Теорема доказана.

Математическая суть ряда методов коррекции ошибок помехоустойчивыми кодами сводится к решению уравнений в полях Галуа.

Пример 4.11.1. Исправить ошибки в сообщении $\overline{x}$ из примера 4.8.3.

Решение. Данный код исправляет двойные ошибки. Предположим, что у сообщения $\overline{x}$ ошибочными являются i-я и j-я позиции. Это означает, что синдром $\overline{s}$ является суммой i-го и j-го столбцов матрицы H. В первой строке матрицы H на i-м месте расположен элемент $\alpha^{i-1} = x,$ на j-м месте – элемент $\alpha^{j-1} = y.$ Для нахождения неизвестных x и y имеем систему двух уравнений $\begin{cases} x + y = \alpha^{11}, \\ x^3 + y^3 = \alpha. \end{cases}$

Данная система сводится к квадратному уравнению. Действительно, $x^3 + y^3 = (x + y)(x^2 + xy + y^2) = \alpha^{11}(\alpha^{22} + xy) = \alpha.$ Тогда $xy = \alpha^{22} + \alpha / \alpha^{11} = \alpha^7 + \alpha^5 = \alpha^{13}.$ Замена $y = x + \alpha^{11}$ приводит к уравнению $x^2 + \alpha^{11}x + \alpha^{13} = 0.$ После замены $x = \alpha^{11}t$ приходим к каноническому виду $t^2 + t + \alpha^5 = 0.$ Нетрудно проверить, что след $Tr(\alpha^5) = 0$ и, следовательно, уравнение имеет решения в поле $F(16).$ Непосредственным подбором можно убедиться, что корнями являются $t_1 = \alpha, t_2 = \alpha + 1 = \alpha^4.$ Тогда $x = \alpha^{11}\alpha = \alpha^{12};$ $y = \alpha^{12} + \alpha^{11} = 1.$ Таким образом, ошибочными в принятом сообщении являются 1-я и 13-я позиции и правильным является сообщение $\overline{c}_0 = (011011110110001).$

Замечание. Полученная формула корней квадратного уравнения для полей Галуа характеристики 2 явно не вызывает восторга ввиду своей очевидной громоздкости. Разнообразные попытки обойтись без данной формулы, предпринятые в том числе и автором доказанной теоремы, привели к так называемой процедуре Ченя – последовательной подстановке элементов поля Галуа в решаемое квадратное уравнение. Ясно, что ситуация с уравнениями высших порядков не лучше. Многочисленные приложения конечных полей требуют решения проблемы поиска простых и быстрых методов решения уравнений в полях Галуа.

Литература

1. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. – М.: Мир, 1987. – 416 с.
2. Аршинов Н.Н., Садовский Л.Е. Коды и математика. – М.: Наука, 1983. – 124 с.
3. Бейкер А. Введение в теорию чисел. – Мн.: Выш. ш., 1995. – 127 с.
4. Биркгоф Г., Барти Т. Современная прикладная алгебра. – М.: Мир, 1976. – 400 с.
5. Боро В., Цагир Д., Рольфс Ю. и др. Живые числа. Пять экскурсий. – М.: Мир, 1985. – 128 с.
6. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – М.: МЦНМО, 2003. – 326 с.
7. Виноградов И.М. Основы теории чисел. – М.: Наука, 1976. – 168 с.
8. Каргополов М.И., Мерзляков Ю.И. Основы теории групп. – М.: Наука, 1972. – 240 с.
9. Конопелько В.К., Липницкий В.А. и др. Прикладная теория кодирования. Т. 1 – 2. – Мн.: БГУИР, 2004. – 688 с.
10. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. – М.: Постмаркет, 2001. – 324 с.
11. Ленг С. Алгебра. – М.: Мир, 1968. – 564 с.
12. Лиддл Р., Ниддеррайтер Г. Конечные поля. Т. 1 – 2. – М.: Мир, 1988. – 882 с.
13. Мак-Вильямс Ф.Дж., Слоэн Н.ДЖ.А. Теория кодов, исправляющих ошибки. – М.: Связь, 1979. – 744 с.
14. Мальцев А.И. Алгебраические системы. – М.: Наука, 1970. – 392 с.
15. Муттер В.М. Основы помехоустойчивой телепередачи информации. – Л.: Энергоатомиздат, 1990. – 286 с.
16. Ноден П., Китте К. Алгебраическая алгоритмика. – М.: Мир, 1999. – 720 с.
17. Прасолов В.В. Многочлены. – М.:МЦНМО, 2000. – 336 с.
18. Самсонов Б.Б., Плохов Е.М., Филоненков А.И., Кречет Т.В. Теория информации и кодирование. – Р-н/Д.: Феникс, 2002. – 288 с.
19. Серр Ж.-П. Курс арифметики. – М.: Мир, 1972. – 184 с.
20. Соловьев Ю.П., Садовничий В.А., Шавгулидзе Е.Т., Белокуров В.В. Эллиптические кривые и современные алгоритмы теории чисел. – М.-Ижевск: Институт компьютерных исследований, 2003. – 192 с.
21. Сушкевич А.К. Теория чисел. Элементарный курс. – Харьков: ХГУ, 1954. – 204 с.
22. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии. – М.: МЦНМО, 2002. – 104 с.
23. Харин Ю.С., Берник В.И., Матвеев Г.В. Математические основы криптологии. – Мн.: БГУ, 1999. – 320 с.
24. Холл М. Теория групп. – М.: ИЛ, 1962. – 468 с.

Св. план 2005, поз. 66

Учебное издание

Липницкий Валерий Антонович

СОВРЕМЕННАЯ ПРИКЛАДНАЯ АЛГЕБРА. МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ПОМЕХ И НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Учебное пособие
по курсу «Высшая математика»
для студентов специальностей «Системы, сети и устройства телекоммуникаций» и «Информатика»
всех форм обучения

Редактор Н.В. Гриневич
Корректор Е.Н. Батурчик

Подписано в печать 30.05.2005. Формат 60x84 1/16. Бумага офсетная.
Гарнитура «Таймс». Печать ризографическая. Усл. печ. л. 5,35.
Уч.-изд. л. 4,4. Тираж 350 экз. Заказ 16.

Издатель и полиграфическое исполнение: Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
Лицензия на осуществление издательской деятельности №02330/0056964 от 01.04.2004.
Лицензия на осуществление полиграфической деятельности №02330/0131518 от 30.04.2004.
220013, Минск, П. Бровки, 6