МИНОБРНАУКИ РОССИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра геометрии

Теоремы характеризации конечного поля

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 421 группы

направления ***02.03.01 – Математика и компьютерные науки***

механико-математического факультета

Ненашева Ивана Станиславовича

Научный руководитель

доцент, к.ф.-м.н.,	05.09.2019	В.Е.НОВИКОВ
должность, уч. степень, уч. звание	подпись, дата	инициалы, фамилия

Зав. кафедрой

д.ф-м.н. профессор	05.09.2019	В.В.РОЗЕН
уч. степень, уч. звание	подпись, дата	инициалы, фамилия

Саратов 2019

ВВЕДЕНИЕ

Начала теории конечных полей восходят к XVII и XVIII веку. Над этой темой работали такие учёные, как Пьер Ферма, Леонард Эйлер, Жозеф Луи Лагранж и Адриен Мари Лежандр, которых можно считать основателями теории конечных полей простого порядка. Однако больший интерес представляет общая теория конечных полей, берущая своё начало с работ Гаусса и Галуа. До некоторого времени эта теория находила применение только в алгебре и теории чисел, однако впоследствии были найдены новые точки соприкосновения с геометрией, комбинаторикой и теорией кодирования.

В 1830 году восемнадцатилетний Эварист Галуа опубликовал работу, которая положила основу общей теории конечных полей. В этой работе Галуа вводит воображаемый корень сравнения $F(x) \equiv 0 \pmod{p}$, где $F(x)$ — произвольный многочлен степени ν, неприводимый по модулю p. После этого рассматривается общее выражение $A = a_0 + a_1 i + a_2 i^2 + ... + a_{\nu-1} i^{\nu-1}$, где $a_0, a_1, ..., a_{\nu-1}$ — некие целые числа по модулю p. Если присваивать этим числам всевозможные значения, выражение A будет принимать p^ν значений. Далее Галуа показывает, что эти значения образуют поле и мультипликативная группа этого поля является циклической. Таким образом, эта работа является первым камнем в фундаменте общей теории конечных полей. В отличие от его предшественников, рассматривающих только поля $\mathbb{F}_p$, Галуа рассматривает уже поля $\mathbb{F}_{p^n}$, которые начали называть полями Галуа в его честь.

На самом деле, первая работа в этом направлении была написана Гауссом примерно в 1797 году, однако при его жизни это исследование так и не было издано. Вероятно, данное исследование было проигнорировано редактором его сочинений, поэтому на свет эта работа появилась только в посмертном издании в 1863 году.

В 1893 году математик Элиаким Мур доказал теорему о классификации конечных полей, утверждающую, что любое конечное поле является полем Галуа, то есть любое поле из p^n элементов изоморфно полю классов вычетов многочленов с коэффициентами из F_p по модулю неприводимого многочлена степени n. К этому же году относится первая попытка дать аксиоматический подход к теории конечных полей, осуществленная Генрихом Вебером, который пытался объединить в своей работе понятия, возникшие в различных разделах математики, в том числе и понятие конечного поля. Далее в 1905 году Джозеф Веддербёрнruen доказывает малую теорему Веддербёрна о том, что любое конечное тело коммутативно, то есть является полем. Современное аксиоматическое определение поля (с конечными полями в качестве частного случая) принадлежит Эрнсту Штайницу и изложено в его работе 1910 года.

В первой части данной работы рассматриваются основные алгебраические понятия, а именно алгебраические структуры (группы, кольца и поля), многочлены, а также расширение поля. Во второй рассматриваются основные теоремы характеризации конечного поля, рассматривается вопрос о множестве корней неприводимого многочлена, исследуются функции следа и нормы, исследуется поле разложение многочлена x^2-1 над произвольным полем, благодаря чему вводится обобщенное понятие корня из единицы, хорошо известное для комплексных чисел.

Теория конечных полей стала весьма актуальной в связи с разнообразными приложениями. Конечные поля получили широчайшее применение в криптографии, теории кодирования, математической теории переключательных схем.

1 Группы, кольца, поля, многочлены

Определение 1.1. *Группой* $(G, *)$ называется некоторое множество G с бинарной операцией $*$ на нем, для которых выполняются следующие три условия:

1. Операция $*$ *ассоциативна*, т.е. для любых $a, b, c \in G$

$$a * (b * c) = (a * b) * c.$$

2. В G существует единичный элемент (или единица) e, такой, что для любого $a \in G$

$$a * e = e * a = a.$$

3. Для каждого $a \in G$ существует обратный элемент $a^{-1} \in G$, такой, что

$$a * a^{-1} = a^{-1} * a = e.$$

Если группа удовлетворяет следующему условию:

4. Для любых $a, b \in G$

$$a * b = b * a,$$

то она называется *абелевой* (или *коммутативной*)

Определение 1.2. Мультипликативная группа G называется *циклической*, если в ней имеется такой элемент a, что каждый элемент $b \in G$ является степенью элемента a, т.е. существует целое k, такой, что $b = a^k$. Этот элемент a называется *образующим* группы G. Для циклической группы G применяют обозначение $G =< a >$.

Определение 2.1. *Кольцом* $(R, +, \cdot)$ называется множество R с двумя бинарными операциями, обозначаемыми символами $+$ и $\cdot$, такими, что

1. R – абелева группа относительно операции $+$.
2. Операция $\cdot$ ассоциативна, т.е. для всех $a, b, c \in R$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

4. Выполняются законы дистрибутивности, т.е. для всех $a, b, c \in R$

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{и} \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

Определение 2.9.

1. Кольцо *называется кольцом с единицей*, если оно имеет мультипликативную единицу, т.е. если существует такой элемент $e \in R$, что $ae = ea = a$ для любого $a \in R$.
2. Кольцо называется *коммутативным*, если операция $\cdot$ коммутативна.
3. Кольцо называется *целостным кольцом* (или *областью целостности*), если оно является коммутативным кольцом с единицей $e \neq 0$, в котором равенство $ab = 0$ влечет за собой $a = 0$ или $b = 0$.
4. Кольцо R называется *телом*, если $R \neq 0$ и ненулевые элементы в R образуют группу относительно операции $\cdot$.
5. Коммутативное тело называется *полем.*

Определение 2.10. *Поле* есть множество F, на котором заданы две операции, называемые сложением и умножением и которое содержит два выделенных элемента 0 и e, причем $0 \neq e$. Поле F – абелева группа по сложению, единичным элементом которой является 0, а элементы из F, отличные от 0, образуют абелеву группу по умножению, единичным элементом которой является e. Две операции, сложение и умножение, связаны законом дистрибутивности $a(b+c) = ab+ac$. Второй закон дистрибутивности $(b+c)a = ba+ca$ выполняется автоматически в силу коммутативности умножения. Элемент 0 называется нулевым элементом (или просто нулем), а e – единичным элементом (или просто единицей) поля F. В дальнейшем для единицы, как правило, будем использовать символ 1.

Определение 3.1. Пусть R – произвольное кольцо. Многочленом (или полиномом) над R называется выражение вида

$$f(x) = \sum_{i=1}^{n} a_i x^i = a_0 + a_1 x + ... + a_n x^n,$$

где n – неотрицательное целое число, коэффициенты a_i, $0 \le i \le n$, – элементы кольца R, а x – некоторый символ, не принадлежащий кольцу R, называемый переменной (или неизвестной) над R.

Определение 4.1. Пусть F – поле. Подмножество K поля F, которое само является полем относительно операций поля F, называется его *подполем*. В этом случае поле F называется *расширением поля* K. Если $K \neq F$, будем K называть *собственным подполем* поля F.

2 Теоремы характеризации конечных полей

В этой главе излагаются основные свойства конечных полей и описываются методы построения конечных полей.

Наиболее известным примером конечного поля является поле классов вычетов по простому модулю, т.е факторкольцо $Z/(p)$, где p – простое число. Многие свойства этого поля сохраняются и для произвольных конечных полей.

Порядком каждого конечного поля является некоторая степень простого числа и, наоборот, для каждой степени простого числа $q = p^n$, $n \in N$, существует конечное поле, состоящее из q элементов. Оказывается, что все конечные поля с одним и тем же числом элементов изоморфны друг другу и потому могут быть отождествлены.

Теорема 5.1. *Пусть F – конечное поле. Тогда оно состоит из p^n элементов, где простое p является характеристикой из поля F, а натуральное число n является степенью поля F над его простым подполем.*

Теорема 5.2. (Существование и единственность конечных полей) *Для каждого простого числа p и каждого натурального числа n существует конечное поле из p^n элементов. Любое конечное поле из $q = p^n$ элементов изоморфно полю разложения многочлена $x^q - x$ над полем F_p.*

Теорема 5.3. (Критерий подполя) *Пусть F_q – конечное поле из $q = p^n$ элементов (p – простое число). Тогда каждое подполе поля F_q имеет порядок p^m, где m является положительным делителем числа n. Обратно, если m – положительный делитель числа n, то существует ровно одно подполе поля F_q из p^m элементов.*

Теорема 5.4. *Мультипликативная группа F_q^* ненулевых элементов произвольного конечного поля F_q циклична.*

Определение 5.1. Образующий элемент циклической группы F_q^* называется *примитивным элементом* поля F_q.

Наличием в любом конечном поле примитивных элементов можно воспользоваться для доказательства того факта, что каждое конечное поле является простым алгебраическим расширением своего простого подполя.

Теорема 5.5. *Пусть F_q – конечное поле и F_r – его конечное расширение. Тогда F_r является простым алгебраическим расширением поля F_q, причем образующим элементом этого простого расширения может служить любой примитивный элемент поля F_r.*

Следствие. *Для каждого конечного поля F_q и каждого натурального числа n в кольце $F_q[x]$ существует неприводимый многочлен степени n.*

ЗАКЛЮЧЕНИЕ

В данной работе был изучен вопрос характеризации конечного поля. Были рассмотрены основные свойства конечных полей и способы их построения.