МИНИСТЕРСТВО ВЫСШЕГО И СРЕДНЕГО СПЕЦИАЛЬНОГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ УЗБЕКИСТАН

САМАРКАНДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ АЛИШЕРА НАВОИ

Механико-математический факультет

5130100-математическое направление

АМРИДДИНОВА ЗИЛОЛА

«ЛОКАЛЬНЫЕ ПОЛЯ И КОНЕЧНЫЕ РАСШИРЕНИЯ»

(выпускная квалификационная работа
для получения академической степени бакалавра)

Представлено к защите:

Декан факультета _____доц.Х.Х.Рузимурадов

Зав.кафедры _____ проф.А.С.Солеев

Научный руководитель_____ст.пр.Л.С.Соколовская

САМАРКАНД – 2015

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Постановка задачи. Тема выпускной квалификационной работы посвящена одному из классических разделов алгебры локальным полям и их расширениям. На основе теории конструкции конечных и полных полей изучаются расширения Галуа и рассматриваются приложения теории локальных полей и конечных расширений к решению некоторых задач, которые встречаются в различных областях математики.

Актуальность темы. В классической алгебре особое значение имеют теория локальных полей классов – это теория алгебраических, в основном абелевых расширений локальных полей. Многие математики изучали различные виды локальных полей классов. Каждый из них внес свой вклад в теорию полей классов. Это А.Вейль, З.И.Боревич и М.Р.Шафаревич, Вандер Варден, К.Ивасава, Т.Януш, Д.Фадеев.

В настоящее время изучение данной теории приводит к новым открытием и новым понятиям, которые невозможны без знания классических положений.

Теоретических и практический интерес к изучению локальных полей и их расширений связаны со многими другими проблемами теории чисел и алгебры и до сих пор, в настоящее время с успехом могут быть использованы для решения вновь возникающих задач физики, математики.

Цели и задачи. Основной задачей данной квалификационной работы – изучить теорию, тесно связанную с локальной теорией полей классов, понять конструкцию такого поля, изучить свойства и построение, связи и взаимоотношения и применить данные знания к решению некоторых задач.

Научное значения. Теория построения локальных полей и их расширений – важнейшее звено классической и современной теории чисел, имеющее большое научное значения для возникновения новых теорий и новых объектов в алгебре.

Научно – исследовательские методы. Методы исследования изученного материала и их связей на базе применения этой теории к решению многочисленных задач алгебры и теории чисел. Используются методы анализа и сравнения полученных результатов для обобщения теории.

Практическое значение. Методы исследования изученного материала и их связей на базе применения этой теории к решению многочисленных задач – это результат, который в дальнейшем можно использовать как методологию при решении и ранее неиспользованных положений и задач.

Содержание работы. Работа состоит из введения, двух глав и 9 параграфов, заключения и списка использованных источников, который включает 7 наименований, включая и интернет.

Во введении обосновывается тема, дается обзор существующих результатов, формулируются цели и задачи, обсуждается актуальность темы и её научное и практическое значение.

Глава I является вспомогательной и содержит 2 параграфа, в которых излагаются сведения об алгебраических структурах и основные свойства конструкции полей.

Глава II посвящена конечным и локальным полям, их связям и особенностям.

В § II.1 обсуждаются конечные поля и их свойства.

§ II.2 содержит сведения о метрических пространствах и возникновении полного поля.

В §§ II.3 и II.4 излагается теория расширения Галуа полных полей и возникновения локальных полей и его свойства.

§ II.5, § II.6 посвящен конечным расширениям и их особенностям.

§ II.7 содержит решение некоторых задач, связанных с теорией локальных полей классов.

В заключении подводится итог выполнения выпускной квалификационной работе и перечисляются другие возможные формы развития в этой области.

Глава I. Основные понятия и определения.

§ I.1. Алгебраические системы и их изоморфизм

Если в прошлых веках и в начале XX века алгебра изучала весьма ограниченное число алгебраических структур, то сейчас можно дать очень общее определение алгебры – а именно: наука о свойствах множеств, на которых определена та или иная система операций и отношений. В развитие такого взгляда на алгебру внес большой вклад А.И.Мальцев. В частности, он ввел понятие алгебраической системы, что и является темой данного раздела. Благодаря работам А.И.Мальцева стало ясно, что алгебра и математическая логика – два тесно связанные между собой дисциплины [1,7].

Определение 1. n −арным (n −местным) отношением на множестве A называется подмножество n −ой декартовой степени A^n множества A.

Определение 2. n − арной (n − местной) алгебраической операцией (или просто операцией), опеределенной на множестве A называется n −местная функция $f : A^n \to A$.

Число n для n −арной операции f (n −арного отношения r) называется арностью операции f (отношения r) и обозначается $n(f)(n(r))$. Арности отношений – это числа, большие нуля. Арности операций – это числа большие или равные нулю. Операции арности 0 представляют собой функции с областью определения, состоящей из одного элемента (n −ки длины 0) и отождествляются со значением функции.

Для унарных операций мы будем использовать префиксную и постфиксную нотацию, а для бинарных – как правило инфиксную.

Свойства операций и отношений

Если множество A конечно, алгебраическую операцию на этом множестве можно определить в виде таблицы. Если операция бинарная, то такое определение особенно удобно.

Пример 1 (таблица операции).

Составим таблицу операции $(-\ mod\ 5)$ на множестве

$$\{0, 1, 2, 3, 4\}$$

$(+mod\ 5)$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Кроме того, что таблица даёт определение операции, она наглядно выражает некоторые свойства операции. В частности, коммутативность операции соответствует симметричности таблицы относительно главной диагонали.

Определение 3. Алгебраической системой $< A;\ W_F;\ W_r >$ называется объект, состоящий из трёх множеств: непустого множества A, множества алгебраических операций W_F, определённых на A, и множества отношений W_R, определенный на A. Множество A называется носителем алгебраической системы. Если алгебраическая система не содержит операций, она называется моделью, если не содержит отношений, то – алгеброй.

Символы алгебраических операций и отношений (каждый из которых имеет определенную арность) составляют сигнатуру алгебраической системы.

Мы будем иметь дело алгебраическими системами. Содержащими конечное число операций и отношений. Алгебраические системы мы будем записывать в виде:

$$< A;\ f_1, \dots, f_k;\ r_1, \dots r_l >, \quad \text{где} \ \ \{f_1, \dots, f_k\} = W_F\{r_1, \dots r_l\}$$

Определение 4. Типом алгебраической системы $< A;\ f_1, \dots, f_k;\ r_1, \dots r_l >$ называется пара наборов $(n(f_1), \dots, n(f_k))$ и $(n(r_1), \dots, n(r_l))$, состоящих из арностей операций и отношений. Тип будем записывать в виде $< n(f_1), \dots, n(f_k);\ n(r_1), \dots, n(r_l) >$.

Пример 2 (алгебраическая система).

$< N;\ +, \cdot, <>$ является алгебраической системой типа $< 2, 2, \cdot 2 >$, так как операции +, · определены для любых двух натуральных чисел и результат снова является натуральным числом. $< N;\ +, -, \cdot, <>$ не является алгебраической системой, так как результат операции -, применённой к натуральным числам – не всегда натуральное число.

Стандартный алгебраический подход к рассмотрению алгебраических систем – отвлечение от свойств отдельных элементов носителя. Не связанных с операциями и отношениями системы, как и от способов определения (вычисления) операций и отношений, и рассмотрение только их свойств в рамках алгебраической системы. Для обозначения совпадения свойств носителей, операций и отношений в рамках самих алгебраических систем используется понятие изоморфизма.

Определение 5. Пусть $A =< A;\ f_1, \dots, f_k;\ r_1, \dots r_l >$ и $B =< B;\ g_1, \dots, g_k;\ p_1, \dots p_l > -$ алгебраические системы одного типа $< m_1, \dots, m_k;\ n_1, \dots n_l >$. Отображение $j: A \to B$ называется гомоморфзимом алгебраической системы A в B, если выполняются следующие условия:

1. $j\big(f_i(x_1, \dots, x_{mi})\big) = g_i\big(j(x_1), \dots, (x_{mi})\big)$,
2. $(x_1, \dots, x_{mi}) O r_j Ю \big(j(x_1), \dots, (x_{mi})\big) O p_j$.

для любых $x_1, x_2, \dots OA$, для любых $i: 1\ J\ i\ J\ k$, для любых $j: 1\ J\ j\ J\ l$

Пример 3 (гомоморфизм).

Любое отображение любой модели $< A; p >$ типа $< 2 >$ на модель $< A: V >$ (где $V -$ пустое бинарное отношение) является гомоморфизмом, так как первое условие выполняется ввиду отсутствия операций, а второе – из-за того, что посылка импликации всегда ложна.

Определение 6. Если гомоморфизм является биекцией и обратное отображение тоже – гомоморфизм, то такой гомоморфизм называется изоморфизмом. Алгебраические системы, для которых существует изоморфизм, называются изоморфными.

Иначе говоря, изоморфизм алгебраических систем $A =< A;\ f_1, \dots, f_k;\ r_1, \dots r_l >$ и $B =< B;\ g_1, \dots, g_k;\ p_1, \dots p_l >$ одного типа $< m_l, \dots, m_k;\ n_1, \dots, n_l > -$ это взаимно-однозначное отображение j множества A на B, такое что выполняются условия:

1. $j\big(f_i(x_1, \dots, x_{mi})\big) = g_i\big(j(x_1), \dots, (x_{mi})\big)$,
2. $(x_1, \dots, x_{mi}) Or_j \text{Ы} \big(j(x_1), \dots, (x_{mi})\big) Op_j$.

для любых $x_1, x_2, \dots OA$, для любых $i: 1\ J\ i\ J\ k$, для любых $j: 1\ J\ j\ J\ l$.

для алгебр условие 2 автоматически выполняется, поэтому для алгебра изоморфизмы – это гомоморфизмы, являющиеся биекцией.

Пример 4 (изоморфизм алгебр).

Покажем, что алгебры $< R;\ + >$ и $< R_+; \cdot > -$ изоморфны. Определим отображение $j: R \text{®} R_+$ как $j(x) = e^x$. Это отображение – биекция и $j(x + y) = e^{(x+y)} = e^x \cdot e^y = j(x) \cdot j(y)$.

Пример 5 (изоморфизм моделей).

Покажем, что модели $< R\ ; J >$ и $< R\ ; i >$ изоморфны. Определим отображение $j(x) = -x$. Это отображение – биекция и $j(x) i\ j(y) \text{Ы} - x\ i - y\ \text{Ы}\ x\ J\ y$.

Определение 7. Изоморфизм алгебраической системы на себя называется автоморфизмом. Автоморфизм, являющийся тождественным отображением называется тривиальным.

§ I.2. Основные свойства и конструкция поля

Абстрактное определение поля F ; под расширением K поля F понимается произвольное поле K , содержащее F в качестве подполя; расширение K называется алгебраическим, если любой элемент $\alpha \in K$ является корнем некоторого многочлена с коэффициентами в F: $a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n = 0$, где $a_1 \in F$. Например, множество чисел вида $a + b\sqrt{2}$ с $a, b \in Q$ представляет собой алгебраические расширение поля Q.

a) Пусть $F -$ некоторое поле. Наименьшее целое положительное число n, для которого 1, будучи сложена сама с собой n раз, дает в результате 0, называется характеристикой поля F и обозначается через $char\ (F)$. Если $1 + 1 + \ldots + 1$ всегда $\neq 0$, то по определению $char\ (F) = 0$. (Логичнее было бы полагать $char\ (F) = \infty$, однако принято считать характеристику поля в этом случае равной 0.) Поля Q, Q_p, R и C имеют характеристику 0, тогда как множество классов вычетов кольца Z по простому модулю p является полем характеристики p. (Вскоре нам встретятся другие примеры полей характеристики p.).
b) Определение векторного пространства V над полем F; понятие базиса V над F: свойство конечномерности векторного простаранства V; если V конечномерно, то его размерность равна числу элементов любого базиса.
c) Любое расширение K поля F можно рассматривать как векторное пространство над F ; если это пространство конечномерно, то соответствующее расширение будет алгебраическим; размерность этого векторного пространства называется степенью расширение и обозначается $[K:F]$. Если $\alpha \in K$ обладает тем свойством, что каждый элемент поля K представим в виде рационального выражения от α над F, то говорят, что расширение K получено присоединением элемента α

к полю F, и записывают это в виде $K = F(\alpha)$. Пусть $K' -$ конечное расширение поля K. Тогда легко установить конечность K' как расширения поля F и установить конечность K' как расширения поля F и соотношение $[K':F] = [K':K] \cdot [K:F]$.

d) Пусть $\alpha -$ элемент алгебраического расширения K поля F. Тогда существует единственный неприводимый многочлен со старшим коэффициентом 1 (неприводимость означает, что его нельзя разложить в произведение в F), такой, что

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ \ldots + a_1\alpha + a_0 = 0, \qquad a_i \in F.$$

Этот многочлен называется минимальным многочленом элемента α, а число $n -$ степенью данного элемента α. Расширение $F(\alpha)$ имеет степень n над F (действительно, в качестве базиса векторного пространства $F(\alpha)$ над F можно взять набор элементов $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$).

e) Если поле F имеет характеристику 0 (например, Q или Q_p) или является конечным (подробное изложение теории конечных полей следует за данным обзором), то можно доказать, что каждое конечное расширение K поля F имеет вид $K = F(\alpha)$ для некоторого $\alpha \in K$. Такой элемент α называется примитивным. (На самом деле это верно, если поле F совершенное, т.е. либо $char\,(F) = 0$, либо $char\,(F) = p$ и каждый элемент поля F обладает корнем степени p в F.) Знание примитивного элемента α расширения K упрощает изучение этого K, так как в этом случае каждый элемент из K представим в виде многочлена от α степени $< n$, т.е. $K = \left\{\sum_{i=0}^{n-1} a_i\alpha^i | a_i \in F\right\}$.

f) Рассмотрим некоторый неприводимый многочлен f степени n с коэффициентами в F. Можно построить расширение $K \supset F$ степени n, в котором f имеет корень $\alpha \in K$. Последовательно присоединяя корни всех многочленов с коэффициентами в F, мы получаем алгебраическое

замыкание (обозначаемое $F^{alg\,c1}$ или F) поля F, т.е., по определению, наименьшее алгебраически замкнутое поле, содержащее F (напомним, что поле K называется алгебраически замкнутым, если всякий многочлен с коэффициентами в K имеет корень в K). Всякое алгебраическое расширение поля F содержится в некотором его алгебраическим замыкании (т.е. его можно расширить до алгебраического замыкания поля F). Любые два алгебраических замыкания поля F изоморфны. Поэтому мы обычно пишем «алгебраическое замыкание» вместо «любое алгебраическое замыкание». Как правило, алгебраическое замыкание поля F является объединением бесконечного множества конечных алгебраических расширений поля F. Так, например, алгебраическое замыкание поля Q состоит из всех комплексных чисел, являющихся корнями многочленов с рациональными коэффициентами. Однако алгебраическое замыкание поля вещественных чисел R равно $C = R(\sqrt{-1})$, т.е. это конечное расширение степени 2 поля R. Но этот пример – скорее исключение, чем правило.

g) Пусть $K = F(\alpha), K' -$ другое расширение поля F, а $\sigma: K \to K' -$ изоморфное вложение поля K в K' (где $\sigma -$ некоторый $F -$ гомоморфизм, т.е. это отображение сохраняет все операции поля и $\sigma(a) = a$ для любого $a \in F$). Тогда элемент α и его образ $\sigma(\alpha)$ в K' обладают одним и тем же минимальным многочленом. Обратно, пусть $K = F(\alpha), K' -$ другое расширение поля F и $\alpha' \in K' -$ корень минимального многочлена для α. Тогда существует единственный изоморфизм σ поля K на подполе $F(\alpha') \subset K'$, для которого $\sigma(a) = a$ при любом $a \in F$ и $\sigma(a) = a'$.

h) Все корни минимального многочлена над F элемента $\alpha \in \bar{F}$, лежащие в поле $\bar{F} = F^{alg\,c1}$, называются элементами, сопряженными с α. Существует взаимно однозначное соответствии между изоморфными

вложениями $F(\alpha)$ в $\bar{F}$ и элементами α', сопряженными с α. Если $char(F) = 0$ или $F -$ конечное поле (или $F -$ совершенное поле), то каждый неприводимый многочлен с коэффициентами в F не имеет кратных корней. В этом случае число элементов, сопряженных с α, равно $[F(\alpha): F]$.

i) Расширение $K = F(\alpha)$ поля F называется расширением Галуа, если все элементы, сопряженные с α, лежат в K. В этом случае все сопряженные любого элемента $x = \sum_{i=0}^{n-1} a_i \alpha^i \in K$ также лежат в K, поскольку такие сопряженные имеют вид $\sum_{i=0}^{n-1} a_i \alpha'^i$, где $\alpha' -$ элемент, сопряженный с α. Приведем несколько примеров расширений Галуа поля $Q: Q(\sqrt{2})$ (так как $\alpha = \sqrt{2}$ обладает единственным сопряженным, равным другому корню $\alpha' = -\sqrt{2}$ уравнения $x^2 - 2 = 0$, и $-\sqrt{2} \in Q(\sqrt{2})$); $Q(i); Q(\sqrt{d})$ для любого $d \in Q; Q(\xi_m)$, где $\xi_m = e^{2\pi i/m} -$ примитивный корень из 1 степени m, лежащий в C (так как все сопряженные с $\xi_m -$ это другие примитивные корни степени m. а они имеют вид ξ_m^i, где i взаимно просто с m). Поле $Q(\sqrt[4]{2})$ дает пример расширения поля Q, которое не есть расширение Галуа. Действительно, сопряженные с $\sqrt[4]{2} -$ это 4 корня уравнения $x^4 - 2 = 0$, а именно: $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$. Но $i\sqrt[4]{2} \notin Q(\sqrt[4]{2})$ (так как $Q(\sqrt[4]{2})$ содержится в поле вещественных чисел).

j) Пусть $K -$ некоторое расширение Галуа поля F. Тогда образ каждого изоморфизма из пункта (h) совпадает с K, т.е. все эти изоморфизмы являются Fизоморфизмами поля K в себя, или $F -$автоморфзмами поля K. Эти автоморфизмы образуют группу, которая называется группой Галуа поля K над F. Каждый автоморфизм σ из этой группы определяет множество элементов $x \in K$, для которых $\sigma(x) = x$. Оно называется полем $\sigma -$ инвариантов (легко проверить, что это действительно подполе в K, содержащее F). Рассмотрим следующий пример: поле $K = Q(\sqrt{2} + \sqrt{3}) -$расширение Галуа поля Q степени 4;

возьмем автоморфизм σ, переводящий $\sqrt{2}+\sqrt{3}$ в $\sqrt{2}-\sqrt{3}$; тогда поле $\sigma-$инвариантов совпадает с $Q(\sqrt{2})$. Нетрудно установить, что если $K-$расширение Галуа поля F, а $K' \neq K-$некоторое промежуточное поле между K и $F: F \subset K' \subset Kd$, то существует нетривиальный автоморфизм поля K,оставляющий неподвижными все элементы из K'. Более того, существует взаимно однозначное соответствие между подгруппами S группы Галуа поля K над F и промежуточными полями $F \subset K' \subset K$, такое, что

$$S \leftrightarrow K'_S = \{x \in K | \sigma x = x \ \text{ для любого } \ \sigma \in S\}.$$

Перейдем теперь к изучению конечных полей. Простейший пример такого поля есть поле классов вычетов целых чисел по простому модулю p. Элементами этого поля являются классы эквивалентности целых чисел по отношению эквивалентности $x \sim y$, определяемому как $x \equiv y(mod\ p)$. Существует ровно p таких классов эквивалентности, а именно классы элементов 0, 1, 2, 3, …, $p-2, p-1$. На множестве этих классов легко ввести операции сложения и умножения, а затем проверить, что при этом получится поле (в частности, каждый ненулевой класс эквивалентности обратим по умножению; иначе говоря, если $x-$целое, не делящееся на p, то существует целое y, для которого $xy \equiv 1(mod\ p)$). Это поле обозначается F_p, а иногда Z/pZ (факторкольцо кольца целых чисел по идеалу целых чисел, делящихся на p). С таким же успехом можно построить это поле, исходя из множества целых $p-$адических чисел Z_p и отношения эквивалентности $x \sim y\left(x, y \in Z_p\right)$, определяемого как $x \equiv y(mod\ p)$ (т.е. эквивалентные x и y имеют один и тот же первый знак в $p-$адическом разложении). Поэтому поле F_p можно записывать также в виде Z_p/pZ_p (факторкольцо кольца целых $p-$адических чисел по идеалу $p-$адических целых, делящихся на p). Факторкольцо Z_p/pZ_p называется полем вычетов кольца Z_p. Причина нашего интереса к общим конечным полям заключается в том, что ниже, при исследовании

алгебраических расширений поля Q_p, мы столкнемся с их полями вычетов, которые строятся аналогично полю вычетов для $Z_p \subset Q_p$, однако оказываются уже совсем не такими простыми, как F_p. Они представляют собой алгебраические расширения поля F_p. Поэтому сейчас нам необходимо поучить некоторое представление о том, как же выглядят конечные поля вообще [2,6].

Пусть $F -$ конечное поле. Тогда характеристика $F \neq 0$, так как все элементы 0, 1, 1+1, 1+1+1, … из F не могут быть различными. Пусть $n = char(F)$. Заметим, что число n должно быть простым. Действительно, если $n = n_0 n_1$ для n_0 и $n_1 < n$, то $n_0 \neq 0$ и после умножения на n_0^{-1} мы получаем противоречие: $n_1 = n_0^{-1} n = 0$. Обозначим это простое число (F) через p.

Очевидно, любое поле F характеристики p содержит в качестве подполя описанное выше поле из p элементов (оно состоит из элементов вида 1+1+ … +1). Это подполе называется простым подполем в F.

Заметим теперь, что для каждого поля F характеристики p определено отображение $x \to x^p$, сохраняющие операции сложения и умножения:

$$xy \to (xy)^p = x^p y^p,$$

$$x + y \to (x + y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} = x^p + y^p$$

потому что целое число $\binom{p}{i} = p!/i!\ \ (p-i)!$ делится на p при $1 \leq i \leq p-1$, а поэтому соответствующий элемент в F равен 0.

Глава II. Конечные и локальные поля.

§ II.1. Конечные поля.

Пусть $F -$ конечное поле из q элементов. Существует гомоморфизм

$$Z \to F_1$$

переводящий $1 \to 1$, ядро которого не может быть 0 и является главным идеалом, порожденным простым числом p, так как Z/pZ вкладывается в F, а $F -$ не имеет делителей 0. Таким образом, F имеет характеристику p и содержит поле, изоморфное Z/pZ, которое не имеет других автоморфизмов, кроме тождественного [5].

Любой автоморфизм должен отображать $1 \to 1$ и следовательно составляет каждый элемент на месте, т.к. 1 аддитивно порождает Z/pZ.

Отождествим Z/pZ с его образом в F тогда $F -$ есть некоторое пространство, конечномерное, т.к. $F -$конечно. пусть его размерность будет n и $\omega_1, \omega_2, \dots, \omega_n -$ базис для F над Z/pZ. Всякий элемент из F имеет единственное представление в виде

$$\alpha_1\omega_1 + \alpha_2\omega_2 + \dots + \alpha_n\omega_n, \quad \text{где} \quad a_i \in Z/Z_p$$

Откуда следует $q = p^n$. А мультипликативная группа $F^* \in F$ имеет порядок $q - 1$, тогда любой элемент $\alpha \in F^*$ удовлетворяет условию $X^{q-1} = 1$.

Откуда следует что всякий элемент из F удовлетворяет уравнению

$$f(x) = x^q - x = 0\,.$$

Это означает, что многочлен $f(x)$ имеет q различных корней в F, а именно все элементы из F. Следовательно, f разлагается в $\neq$ на множители степени 1, а именно.

$$x^q - x = \prod_{a \in F} (x - \alpha)$$

В частности, $F -$ есть поле разложения для f. Но поле разложения однозначно определено с точностью до изоморфизма. Следовательно, если конечные поле порядка p^n существует, то оно однозначно определено с точностью до изоморфизма как поле разложения

$$x^{p^n} - x \quad \text{над} \quad Z/pZ$$

В результате рассуждений получена теорема. Для всякого простого числа p и всякого целого числа $n > 1$ существует поле порядка p^n, означаемое символом F_{p^n}, однозначно определенные как подполе в алгебраическом замыкании $\bar{F}_p$. Это поле разложения многочлена.

$x^{p^n} - x$ и его элементы – корни этого многочлена.

Всякое конечное поле изоморфно одному и только одному из обўих полей F_{p^n}.

Если обозначить $p^n = q$ и $F_q = F_{p^n}$, получаем **следствие:** Пусть F_q конечное поле $m -$ целое число ≥ 1. В данном алгебраическом замыкании $\bar{F}_q$ существует одном только одно расширение поля F_q степени m, и этим расширением является поле F_{p^m}.

Из этого следствия следует следущие заключения:

1. Мультипликативная группа конечного поля – циклическая.

Доказательство. Пусть $q = p^n$ и $F_q -$ конечное поле из q элементов. Рассмотрим отображение Фробеншса

$$\varphi : F_q \to F_q$$

такое, что $\varphi(x) = x^p$. Очевидно, что $\varphi -$ гомоморфизм и его ядро равно 0, т.к. $F_q -$ поле. Следовательно, φ инъективно.

Так как $F_q -$ конечно, то $\varphi -$ сюръективно и что, $\varphi -$ изоморфизм, который оставляет $F_p -$ неподвижным.

2. Группа автоморфизмов поля F_q является циклической группой порядка n с образующей φ.

Доказательство. Пусть $G -$ группа, порожденная φ, т.к. $\varphi^n(x) = x^{p^n} = x \quad \forall\ x \in F_q$, то $n -$ показатель для φ.

Пусть $d -$период φ, так что $d \geq 1$. Имеем $\varphi^d(x) = x^{p^d}, \forall\ x \in F_q \Rightarrow$ что всякий элемент $x \in F_q$ является корнем уравнения

$$x^{p^d} - x = 0$$

Это уравнение имеет самое большое p^d корней. Следовательно $d \geq n \Rightarrow d = n$.

Остается доказать, что G совпадает с группой всех автоморфизмов поля F_q а F_q не может иметь никаких других автоморфизмов, кроме тех, что содержатся в G.

Пусть $Z_p = Z/pZ -$ конечные поле $K \supset F -$ произвольное конечное расширение конечного поля F.

Если $|F| = q$ и $[K:F] = n$, то $|K| = q^n$, т.е. после выбора базиса векторного пространства K/F оно отождествляется с пространством F^n строк $(\alpha_1, \alpha_2, \dots, \alpha_n)$ длины n. Все координаты α_i независимо друг от друга принимают q значений из $F \Rightarrow |K| = |F^n| = q^n$.

§ II.2. Метрические пространства и полные поля

Вещественные числа – это пополнение поля рациональных чисел.

Пусть X −непустое множество. Функция d, определенная на множестве всех упорядоченных пар (x, y) элементов $\in X$ и принимающая неотрицательные значения $d(x, y)$, называется расстоянием или метрикой в X, если она обладает следующими свойствами:

1. $d(x, y) = 0$ тогда и только тогда, когда $x = y$
2. $d(x, y) = d(y, x)$.
3. $d(x, y) \leq d(x, z) + d(z, y) + z \in X$.

Множество X вместе с заданной в нем метрикой d называется метрическим пространством [1].

Если вместо X рассматривать поля, то т.к. поле F есть множество с двумя бинарными операциями $+$ и $\cdot$, такими, что функция коммутативной группой относительно +, а $F - \{0\}$ −относительно операции $\cdot$, и выполнен закон дистрибутивности $a(b + c) = ab + ac$; примера … полей иметь в виду поле рациональных чисел и поле вещественных чисел.

Нормой на поле F называется отображение, обозначаемое $\| \|$, поля F в множество неотрицательных вещественных чисел такое, что

1. $\|x\| = 0$ тогда и только тогда, когда $x = 0$.
2. $\|x \cdot y\| = \|x\| \cdot \|y\|$.
3. $\|x + y\| \leq \|x\| + \|y\|$.

Когда метрика $d,,$ соответствует норме $\| \|$, то это надо понимать, что метрика d определяется соотношением $d(x, y) = \|x - y\|$.

Основной пример нормы на поле рациональных чисел Q дает абсолютная величина $|x|$. Индуцированная ею метрика $d(x, y) = |x - y|$ совпадает с обычным расстоянием на числовой прямой.

Пусть $P \leftarrow \{2,3,5,7,11,13,\dots\}-$ некоторое простое число. Для произвольного ненулевого целого числа P в разложении a на простые сомножители, т.е. наибольшему целому неотрицательному числу m, для которого $a \equiv 0(mod\ p^m)$.

Например $ord_5 35 = 1, ord_5 250 = 3, ord_2 96 = 5, ord_2 97 = 0$.

Если $a = 0$ то $ord_p 0 = \infty$.

Функция $ord_p(a_1 a_2) = ord_p(a_1) + ord_p(a_2)$.

Для произвольного рационального $x = a/b$ положим $ord_p x = ord_p d - ord_p b$. Но тогда на Q определим следующее отображение

$$|x|_p = \begin{cases} \frac{1}{p^{ord_p x}}, & \text{если } x \neq 0 \\ 0, & \text{если } x = 0 \end{cases}$$

Функция $|\ |_p$ является нормой на поле Q. Норма называется неархимедовой, если всегда выполнено $\|x + y\| \leq \max(\|x\|, \|y\|)$.

Пусть $k-$поле и $v-$его нормирование. Существует расширение k' поля k, снабженное нормированием μ, которые является продолжением v и пусть выполнены два условия:

k' является полным относительно μ, а поле k является подмножеством в k'. В этом случае говорят, что поле $k' -$ пополнение поля k относительно нормирования v.

Поле k, полное относительно регулярного нормирования v, мы будем в дальнейшем для краткости называть просто полным полем (опуская явное указание на v), а нормирование $v-$полным регулярным. Если же нужно будет указать и нормирование v, то будет использоваться символ (k, v). В связи с нормированием v были введены понятия кольца $\mathfrak{o}$, идеала $\mathfrak{p}$, поля вычетов $\mathfrak{k} = \mathfrak{o}/\mathfrak{p}$ и группы единиц U, которые в случае полного регулярного

нормирования будут соотноситься с самим полем k, т.е. мы будем говорить о кольце, максимальном идеале, поле вычетов и группе единиц данного поля k; если $\pi -$ униформизирующая полного регулярного нормирования v, то будем говорить, что $\pi -$униформизирующая соответствующего поля k.

Если $v -$ произвольное регулярное нормирование поля k и $(k', v') -$пополнение k относительно v, о котором говорилось в предыдущем параграфе, то $v'\left(k'^{\times}\right) = v(k^{\times}) = Z$, т.е. v' является полным регулярным нормированием, а $(k', v') -$ полным поем. Существует много естественных примеров полных полей.

Пример 1. Пусть $p -$простое число, $Q -$поле рациональных чисел и $v -$обычное $p -$адическое нормирование на Q. Тогда пополнение поля Q относительно $v -$это поле $p -$адических чисел Q_p. Так как нормирование v регулярно, поле Q_p при любом p является полным. Кольцом нормирования поля Q_p является кольцо целых $p -$ адических чисел Z_p, максимальным идеалом служит pZ_p, полем вычетов $- Z_p/pZ_p$, являющееся конечным полем F_p.

Пример 2. Пусть $F -$ произвольное поле. Составим всевозможные формальные степенные ряды с коэффициентами из F, в которых число отрицательных степеней не более чем конечно,

$$\sum_{-\infty \ll n} a_n X^n, \;\; a_n \in F;$$

Совокупность $F\left((X)\right)$ всех таких рядов является, как известно, полем и, очевидно, расширением поля F. Для каждого такого степенного ряда, отличного от нуля, можно фиксировать младший ненулевой коэффициент a_{n_0} и положить

$$v\left(\sum_{-\infty \ll n} a_n X^n\right) = n_0.$$

Естественно считать, что $v(0) = +\infty$. В этом случае функция v оказывается полным регулярным нормированием поля $F((X))$. Следовательно, $(F((X)), v) -$ полное поле. Его кольцом является $F\big[[X]\big] -$ множество всех рядов без отрицательных степеней переменной X ; его максимальным идеалом служит $(X) = XF\big[[X]\big]$ и, следовательно, $F\big[[X]\big]/XF\big[[X]\big] = F$ является его полем вычетов. Поле рациональных функций $F(X)$, очевидно, содержится в $F((X))$, кольцом и максимальным идеалом ограничения нормирования $v|F(X)$ будут соответственно кольцо многочленов $F[X]$ и простой идеал $XF[F]$ (аналогично случаю p −адического нормирования поля Q); следовательно $v|F(X)$ определяет на $F(X)$ регулярное нормирование. Пополнением поля $F(X)$ относительно $v|F(X)$ является, очевидно, $(F((X)), v)$ [4].

Пусть (k, v) −произвольное полное поле, $\mathfrak{k} = \mathfrak{o}/\mathfrak{p} -$ его поле вычетов и $A -$ полная система представителей в кольце $\mathfrak{o}$ элементов поля $\mathfrak{k}$; иными словами, A −это подмножество в $\mathfrak{o}$, составленное из элементов, выбранных по одному из каждого класса вычетов в $\mathfrak{o}/\mathfrak{p}$. В качестве представителя нулевого элемента поля $\mathfrak{k} = \mathfrak{o}/\mathfrak{p}$, т.е. в качестве представителя идеала $\mathfrak{p}$, выберем нулевой элемент 0 поля k. Если $\pi -$ униформизирующая поля k, то в силу полноты нормирования v ряд

$$\sum_{-\infty \ll n} a_n \pi^n, \;\; a_n \in A,$$

является сходящимся в k относительно $\mathfrak{p} -$ адической топологии к некоторому элементу x из k. Если $a_{n_0} -$ первый ненулевой коэффициент в этом ряду, то $a_{n_0} \in 0$ и $a_{n_0} \notin \mathfrak{p}$; следовательно, $v\big(a_{n_0}\big) = 0$, и потому, как легко понять, $v(x) = n_0$.

Теорема II.2.1. Пусть A, π имеют прежний смысл и $x -$ произвольный элемент полного поля k. Тогда x представляется, и притом единственным образом, в виде сходящегося ряда

$$x = \sum_{-\infty \ll n} a_n \pi^n, \quad a_n \in A.$$

В частности,

$$\mathfrak{o} = \left\{ \sum_{n=0}^{\infty} a_n \pi^n \mid a_n \in A \right\}, \qquad \mathfrak{p} = \left\{ \sum_{n=0}^{\infty} a_n \pi^n \mid a_n \in A \right\}.$$

Доказательство. Если $x \neq 0$, то $v(x) = n_0$ при некотором n_0 и $v(\pi^{-n_0} x) = 0$. Поэтому достаточно доказать теорему в случае $v(x) = 0$. При таком предположении существует $a_0 \in A$, удовлетворяющий условию $x \equiv a_0 mod\, \mathfrak{p}$, обязательно $a_0 \neq 0$. Но $\mathfrak{p} = \mathfrak{o}\pi$; поэтому $x = a_0 + x'\pi,\ x' \in \mathfrak{o}$. Аналогично рассуждая, получаем, что $x' \equiv a_1 mod\, \mathfrak{p}$, где $a_1 \in A$, так что $x \equiv a_0 + a_1\pi\ mod\, \mathfrak{p}^2$. Продолжая в том же духе, замечаем, что $\mathfrak{p}^2 = \mathfrak{o}\pi^2$ и $x = a_0 + a_1\pi + x''\pi^2$, где $x'' \in \mathfrak{o}$, откуда $x \equiv a_0 + a_1\pi + a_2\pi^2\ mod\, \mathfrak{p}^3$. Таким образом, в системе A выделяется множество элементов $a_0, a_1, a_2, ...$, которые обеспечивают равенство

$$x = \sum_{n=0}^{\infty} a_n \pi^n$$

Единственность коэффициентов a_n в полученном представлении очевидна из-за описанного их выбора. (Это заново доказывается в приведенном ниже следствии.) Отсюда ясно, как и в общем случае, когда $v(x) = n_0$, получить с помощью $\mathfrak{o}$ и $\mathfrak{p}$ соответствующее равенство.

Если для каждого целого n выбрать в поле k по одному элементу π_n такому, что $v(\pi_n) = n$, то для любого x из k будет иметь место разложение

$$x = \sum_{-\infty \ll n} a_n \pi^n, \quad a_n \in A,$$

существование и единственность которого доказываются аналогично теореме II.2.1, в которой, очевидно, рассматривается случай $\pi_n = \pi^n$.

Далее мы будем обсуждать расширения конечной степени полных полей.

Теорема II.2.2. Пусть $(k, v)-$ полное поле и $k'-$ произвольное расширение конечной степени поля k. Тогда на k' существует, и притом единственное, регулярное нормирование v', удовлетворяющее условию $v'|k \sim v$. Нормирование v' является полным, так что (k', v') представляет собой полное поле.

Доказательство. Существует, и притом единственное, продолжение μ нормирования v на поле k', и если $n = [k' : k]$, то

$$n\mu(k'^{\times}) \subseteq v(k^{\times}) = Z,$$

$$e = e(\mu/v) = [n\mu(k'^{\times}) : v(k^{\times})] < +\infty .$$

Поэтому можно положить $v' = e\mu$ и тогда

$$v'^{(k'^{\times})} = Z, \;\; v'|k = ev \sim v.$$

Единственность нормирования v' следует из единственности продолжения μ нормирования v.

§ II.3. Расширения Галуа полных полей

Продолжим рассмотрение полного поля (k, v);пусть $k' -$ расширение конечной степени поля k. В этом параграфе k'/k будет считаться расширением Галуа и его группа будет обозначаться через $G = Gal(k'/k)$. Если $\sigma -$ произвольный элемент из G, то можно естественным образом распространить действие σ на поле вычетов $\mathfrak{k}' = \mathfrak{o}'/\mathfrak{p}'$ и на факторкольца $\mathfrak{o}'/\mathfrak{p}'^{i+1}$, $i \geq 0$ получая во всех случаях автоморфизмы. Фиксируем множество G_i всех элементов σ из G, тождественных на факторкольце $\mathfrak{o}'/\mathfrak{p}'^{i+1}$.

$$G_i = \{\sigma | \sigma \in G, \sigma(x') \equiv x' mod \mathfrak{p}'^{i+1} \quad \forall x' \in \mathfrak{o}'\}.$$

Очевидно, что G_i являются инвариантными подгруппами группы G и

$$\ldots \subseteq G_{i+1} \subseteq G_i \subseteq \ldots \subseteq G_1 \subseteq G_0 \subseteq G.$$

Теорема II.3.1. Пусть $k'/k -$ вполне разветвленное расширение Галуа. Тогда $G = G_0$ и $G_1 = 1$ для достаточно больших i. Кроме того, факторгруппа G_0/G_1 изоморфна подгруппе мультипликативной группы $\mathfrak{k}^\times$ поля вычетов $\mathfrak{k}$ поля k, a факторгруппы G_i/G_{i+1} при $i \geq 1$ изоморфны подгруппе аддитивной группы $\mathfrak{k}^+$ поля вычетов $\mathfrak{k}$. Группа G является, таким образом, разрешимой.

Доказательство. Расширение k'/k вполне разветвлено; поэтому, как отмечалось в конце предыдущего параграфа, $\mathfrak{o}' = \mathfrak{o}[[\pi']]$, где $\pi' -$ униформизирующая поля k'. Следовательно,

$$G_i = \{\sigma | \sigma \in G, \sigma(\pi') \equiv \pi' mod \mathfrak{p}'^{i+1}\}.$$

Элементы π' и $\sigma(\pi')$ принадлежат $\mathfrak{p}'$; отсюда $G = G_0$. Далее, $k' = k(\pi')$, и если $\sigma \neq 1$, то $\sigma(\pi') = \pi'$. Поэтому $i \geq v'(\sigma(\pi') - \pi')$ при $\sigma \notin G_i$. Таким образом, $G_i = 1$ для достаточно больших i. Как следует из сказанного выше, для любого σ из G_0 существует такой элемент $x \in \mathfrak{o}, x \notin \mathfrak{p}$, что

$\sigma(\pi') \equiv x\pi' mod \mathfrak{p}'^2$; аналогично для σ из $G_i, i \geq 1$ существует такой элемент y из $\mathfrak{o}$, что $\sigma(\pi') \equiv \pi' + y\pi'^{i+1} mod \mathfrak{p}'^{i+1}$. Определим теперь отображения

$$G_0/G_1 \to \mathfrak{k}^{\times} \quad \text{и} \quad G_i/G_{i+1} \to \mathfrak{k}^{+}$$

так: $\sigma \to x \, mod \, \mathfrak{p}$ и $\sigma \to y \, mod \, \mathfrak{p}$. Легко проверить, что получились вложения. Следовательно, группы G_i/G_{i+1}, $i \geq 0$, являются абелевыми. Поскольку $G_i = 1$ для достаточно больших i, группа G разрешима.

Обычно расширение k'/k не является вполне разветвленным; можно доказать, что тогда группа автоморфизмов $Aut\,(\mathfrak{k}'/\mathfrak{k})$ поля вычетов $\mathfrak{k}'$ над полем $\mathfrak{k}$ изоморфна G/G_0,

$$G'/G_0 \simeq Aut\,(\mathfrak{k}'/\mathfrak{k})$$

и, кроме того, G_0 разрешимая группа.

Рассмотрим частный случай. Пусть $p -$ произвольное простое число и k'/k вполне разветвленное циклическое расширение степени p. В этом случае $G = Gal(k'/k)$ является циклической группой порядка p, и, следовательно, в силу доказанной выше теоремы существует целое число $s \geq 1$, такое, что

$$G = G_0 = \ \ldots \ = G_{s-1}, \qquad G_s = 1$$

Если $\sigma \in G, \sigma \neq 1$, то $\sigma \in G_{s-1}, \sigma \in G_s$ и, согласно доказательству той же теоремы и определению группы G_i, справедливо равенство

$$v'\left(\pi' - \sigma'(\pi')\right) = s.$$

В дальнейшем будет играть важную роль следующая теорема о группе $U_s = 1 + \mathfrak{p}^s$ и группе единиц U'

Теорема II.3.2. Пусть $N_{k'/k} -$ норменное отображение рассматриваемого расширения k'/k. Тогда

$$U_s \subseteq N_{k\prime/k}(U').$$

Доказательство. Пусть $\pi' -$ униформизирующая поля k'; так как расширение k'/k вполне разветвлено, справедливо равенство $k' = k(\pi')$. В этом случае π' является корнем некоторого неприводимого в $k[X]$ многочлена

$$f(X) = X^p + c_1X^{p-1} + \ \dots + c_p, \qquad c_i \in k.$$

Коэффициенты c_i представляют собой известные симметричные выражения от элементов $\sigma(\pi'), \sigma \in G$. Но $\sigma(\pi') \in \mathfrak{p}'$; поэтому, очевидно, $v(c_i) \geq 1$. Так как в данном случае $f(k'/k) = 1$, то в силу следствия из теоремы 3 $v(c_p) = v\left(\pm N_{k\prime/k}(\pi')\right) = v'^{(\pi')} = 1$. Значит, $f(X)$ −многочлен Эйзенштейна. Но тогда при любом элементе u из группы U_s многочлен

$$g(X) = X^p + c_1X^{p-1} + \ \dots + c_{p-1}X + uc_p$$

тоже будет многочленом Эйзенштейна, так как $v(uc_p) = v(c_p) = 1$. Таким образом, $g(X)$ также неприводим в кольце $k[X]$. Присоединим к полю k' корень α многочлена $g(X)$, получив некоторые поле F, и пусть $k'' = k(\alpha)$. Следовательно,

$$F = k'(\alpha) = k'k'', \qquad k'' = k(\alpha), \qquad g(\alpha) = 0.$$

Предположим, что $k' \neq k''$. Так как $p = [k'\colon k] -$ простое число, в этом случае $k' \cap k'' = k$, откуда следует, что F/k'' является циклическим расширением степени p с группой Галуа $Gal(F/k'') = Gal(k'/k) = G$. Если $\tilde{v} -$ регулярное нормирование полного поля F, то, для любого $\sigma \in G$

$$\tilde{v}(\alpha - \sigma(\pi')) = \tilde{v}(\sigma(\alpha - \pi')) = \tilde{v}(\alpha - \pi').$$

Поэтому, полагая $e = e(F/k')$, так что $\tilde{v}|k' = ev'$, можно записать

$$ev'(\pi - \sigma(\pi')) = \tilde{v}(\pi' - \alpha + \alpha - \sigma(\pi')) \geq \tilde{v}(\alpha - \pi').$$

Если $\sigma \neq 1$, то $v' = e\big(\pi - \sigma(\pi')\big) = s$ и $\tilde{v}(\alpha - \pi') \leq es$. Следовательно, для

$$f(X) = \prod_{\sigma \in G}\big(X - \sigma(\pi')\big)$$

получаем

$$\tilde{v}(f(\alpha)) = \sum_{\sigma \in G} \tilde{v}\big(\alpha - \sigma(\pi')\big) = p\tilde{v}(\alpha - \pi') \leq pes.$$

Однако $k'/k -$ вполне разветвленное расширение и $e(k'/k) = p$, $\tilde{v}|k' = ev'|k = epv$. Так как $v\big(c_p\big) = 1$ и $u \in U_s = 1 + \mathfrak{p}^s$,

$$\tilde{v}\big(f(\alpha)\big) = \tilde{v}\big(f(\alpha) - g(\alpha)\big) = \tilde{v}\big(c_p - uc_p\big) =$$

$$= epv\left(c_p(1-u)\right) \geq ep(1+s).$$

Это противоречит предыдущему неравенству. Следовательно, $k' = k'', F = k'$ и $\alpha \in k'$. Так как $g(X)$ является неприводимым в $k(X)$ многочленом, из $g(\alpha) = 0$ следует, что $N_{k'/k}(\alpha) = (-1)^p uc_p$, и, согласно следствию из теоремы 3, снова получаем, что $v'(\alpha) = v\big(uc_p\big) = 1$. С другой стороны, $N_{k'/k}(\pi') = (-1)^p c_p$ и $v'^{(\pi')} = 1$; поэтому если $\xi = \alpha/\pi'$, то

$$u = N_{k'/k}(\xi), \;\; \xi \in U'.$$

§ II.4. Локальные поля и его свойства.

Поле k с конечным числом вычетов $\bar{f}$ называется локальным. В этом случае характеристика поля $\bar{f}$ является некоторым простым числом p.

Пусть k в дальнейшем обозначает локальное поле, $v-$ его полное регулярное нормирование, $\mathfrak{k} = \mathfrak{o}/\mathfrak{p}$ –его поле вычетов и $q-$ число элементов поля $\mathfrak{k}$. Поле k будет предполагаться $p-$ полем, т.е. q будет степенью некоторого простого числа p. В этом случае $p\mathfrak{o} \subseteq \mathfrak{p}$ и, следовательно, $v(p \cdot 1) > 0$, так что характеристика самого поля k оказывается равной 0 или p.

Теорема II.4.1. Локальное поле k содержит q различных корней многочлена $X^q - X$. Множество A этих корней является полной системой представителей поля вычетов $\mathfrak{k} = \mathfrak{o}/\mathfrak{p}$ в кольце $\mathfrak{o}$.

Доказательство. Поле $\mathfrak{k}$ является конечным и состоит из q элементов; поэтому многочлен $X^q - X$ имеет q различных корней в $\mathfrak{k}$. Следовательно, согласно этому многочлен $X^q - X$ имеет q различных корней и в кольце $\mathfrak{o}$, причем эти корни принадлежат различным классам вычетов из $\mathfrak{k} = \mathfrak{o}/\mathfrak{p}$. Таким образом, очевидно, множество A является полной системой представителей поля вычетов $\mathfrak{k} = \mathfrak{o}/\mathfrak{p}$ в кольце $\mathfrak{o}$. Нулевой элемент 0 поля k при этом оказывается в A.

Следствие. Пусть $V-$ множество всех корней степени $q-1$ из 1, содержащихся в k; тогда $V-$ циклическая мультипликативная группа и при естественном эпифморфизме $\mathfrak{o} \to \mathfrak{k} = \mathfrak{o}/\mathfrak{p}$ осуществляется изоморфизм мультипликативных групп:

$$V \rightarrow \mathfrak{k}^{\times}.$$

Доказательство. Если из множества A, фигурировавшего в лемме 1, удалить 0, то получится множество V, откуда следует, что $V \twoheadrightarrow \mathfrak{k}^{\times}$, так как группа $\mathfrak{k}^{\times}$ является циклической порядка $q-1$.

Пусть $k'-$ произвольное конечное алгебраическое поля k ; на k' существует единственное регулярное нормирование v', такое, что $v'|k \sim v$ и k' является полным относительно v'. Если $\mathfrak{k}' = \mathfrak{o}'/\mathfrak{p}' -$ поле вычетов поля k', то степень $f(k'/k) = [\mathfrak{k}' : \mathfrak{k}] -$ конечное число и, следовательно, $\mathfrak{k}'$ так же, как и $\mathfrak{k}$, - конечное поле. Значит, конечное алгебраическое расширение локального поля всегда является локальным полем. Так как поле вычетов $\mathfrak{k}$ конечно, его конечное расширение $\mathfrak{k}'/\mathfrak{k}$ представляет собой расширение Галуа. Поскольку $k-$локальное $p-$поле, то очевидно, что и k' локальное $p-$поле. Таким образом, все конечные алгебраические расширения описанных выше локальных p −полей Q_p и $F_p((X))$ являются локальными p −полями; верно и обратное.

Теорема II.4.2. Всякое локальное $p-$поле k (или просто локальное поле) изоморфно конечному алгебраическому расширению поля Q_p или поля $F_p((X))$. Если характеристика поля k равна p, то в нем содержится подполе F, изоморфное полю вычетов $\mathfrak{k}$, и k изоморфно полю формальных степенных рядов $F((X))$ над F.

Доказательство. Если характеристика поля k равна 0, то оно содержит поле рациональных чисел Q . В этом случае $p \in \mathfrak{p}$ и $e = v(p) \geq 1$. Следовательно, ограничение $v|Q$ является нормированием на Q , эквивалентным $p-$ адическому нормированию. Так как $v-$ полное нормирование, топологическое замыкание $\bar{Q}$ поля Q в k является пополнением поля Q относительно нормирования $v|Q$, т.е. $\bar{Q} = Q_p$. С другой стороны, поле вычетов $\mathfrak{k}$ поля k является конечным полем характеристики p и, значит, конечным расширением поля вычетов F_p поля Q_p. Пусть степень

этого расширения равна $f = [\mathfrak{k}: F_p]$. Тогда из доказательства теоремы 3 § 1.3 легко получить, что $[k: Q_p] = ef < +\infty$. Таким образом, поле k изоморфно конечному расширению поля Q_p.

Если же характеристика поля k равна p, то в силу леммы 1 множество

$$A = \{x | x \in k, x^q = x\}$$

является, очевидно, подполем в k. Следовательно, если его обозначить через F, то можно сказать, что естественный гомоморфизм $\mathfrak{o} \to \mathfrak{k} = \mathfrak{o}/\mathfrak{p}$ индуцирует изоморфизм конечных полей $F \rightarrow \mathfrak{k}^{\times}$. Если π −униформизирующая поля k, то в силу теоремы 1 из § 1.3 сопоставление $X \to \pi$ определяет следующий изоморфизм над F:

$$F\big((X)\big) \rightarrow k\,.$$

Так как характеристика поля F равна p и расширение F/F_p конечно, поле $F\big((X)\big)$ является конечным расширением поля $F_p\big((X)\big)$. Теорема доказана.

Замечание. Обычно если k − полное поле характеристики p, то поле вычетов $\mathfrak{k}$ предполагается всего лишь совершенным; в этом случае аналогично изложенному выше доказывается тот же результат: $k \simeq F\big((X)\big), F \simeq \mathfrak{k}$. Однако поле k является конечным расширением поля $F_p\big((X)\big)$, если F является конечным расширением поля F_p; в общем же случае k и $F\big((X)\big)$ не являются конечными расширениями поля $F_p\big((X)\big)$.

Теорема II.4.3. Локальное поле k является недискретным вполне несвязным локально компактным полем. Кольцо нормирования $\mathfrak{o}$ поля k и степени максимального идеала $\mathfrak{p}^n$, $n \geq 1$, являются открытыми компактными аддитивными подгруппами в k; в частности, $\mathfrak{o}$ − максимальное компактное подкольцо в k.

Доказательство. Так как v –регулярное нормирование, означает, что k – недискретное вполне несвязное топологическое поле и все степени $\mathfrak{p}^n$, $n \geq 0$, являются открытыми аддитивными подгруппами в k. С другой стороны, так как поле вычетов $\mathfrak{k}$ поля k конечно, соответствующая ему полная система различных представителей A являются конечным и, следовательно, компактным множеством в $\mathfrak{o}$. Это означает, что кольцо $\mathfrak{o}$ компактно; поэтому поле k локально компактно. Все степени $\mathfrak{p}^n$, $n \geq 0$, в таком случае – открытые, а потому и замкнутые, подгруппы в $\mathfrak{o}$; следовательно, все они компактны. Далее, если R – какое-нибудь компактное подкольцо в k, то множество значений нормирования $\{v(x)|x \in R\}$ ограничено снизу. Следовательно, если $x \in R$ любой элемент, то $x^n \in R$ для всякого $n \geq 1$ и $v(x^n) = nv(x)$, в силу чего $v(x) \geq 0$ и $x \in \mathfrak{o}$. Отсюда следует, что $R \subseteq \mathfrak{o}$ и что $\mathfrak{o}$ – максимальное компактное подкольцо в k.

Замечание. Кольцо $\mathfrak{o}$ является не только компактным. В смысле метрики p, определенной на $\mathfrak{o}$ с помощью нормирования v, кольцо $\mathfrak{o}$ является вполне ограниченным полным пространством – на это прямо указывает конец проведенного выше доказательства.

Теорема II.4.4. Мультипликативная группа $k^\times$ локального поля k является недискретной вполне несвязной локально компактной абелевой группой в индуцированной полем k топологии. Группа единиц U поля k, а также все ее подгруппы $U_n = 1 + \mathfrak{p}^n$, $n \geq 1$, являются открытыми компактными подгруппам в $k^\times$, причем U – максимальная компактная подгруппа в $k^\times$. Так как в поле k содержатся все корни из 1 степени $q - 1$, то они составляют мультипликативную группу V (лемма 1, следствие) и

$$U = V \times U_1, \qquad [U: U_n] = (q-1)q^{n-1}, \qquad n \geq 1.$$

Доказательство. В силу сказанного в § 1.1 эпиморфизм $\mathfrak{o} \to \mathfrak{k} = \mathfrak{o}/\mathfrak{p}$ индуцирует изоморфизм $U/U_1 \rightarrow \mathfrak{k}^\times$. С другой стороны, в силу следствия из теоремы II.4.1 $V \rightarrow \mathfrak{k}^\times$; поэтому $U = V \times U_1$. Справедливы изоморфизмы

$U_n/U_{n+1} \simeq \mathfrak{k}^+, n \geq 1$. Следовательно, $[U: U_n] = (q-1)q^{n-1}$. Утверждение теоремы о том, что группы $U_n = 1 + \mathfrak{p}^n, n \geq 1$, являются открытыми компактными подгруппами в $k^\times$, очевидно. Так как $[U: U_1] = q - 1$, группа U по аналогичным причинам также является открытой компактной подгруппой в $k^\times$. Тот факт, что это максимальная компактная подгруппа в $k^\times$, доказывается аналогично утверждению о том, что $\mathfrak{o} -$ максимальное компактное подкольцо в k. Наконец, то, что $k^\times -$ недискретная вполне несвязная локально компактная группа, очевидно.

Примем теперь во внимание, что $U_1 -$ компактная группа, числа $[U_1: U_n] = q^{n-1}$ являются степенями числа p и единичный элемент 1 есть теоретико-множественное пересечение всех групп $U_n, n \geq 1$; в этих условиях U_1 может рассматриваться как проективный предел конечных $p -$ групп U_1/U_n, $n \geq 1$. Таким образом, группа U_1 является про $-p -$ группой. Аналогично аддитивная группа кольца $p -$ является проективным пределом конечных $p -$ групп $\mathfrak{o}/\mathfrak{p}^n, n \geq 1$, т.е. $\mathfrak{o} -$ это тоже про $-p -$ группа. отсюда следует, что если натуральное число m не делится на p, то отображения $u \mapsto u^m$ и $x \mapsto mx$ определяют соответственно автоморфизмы групп U_1 и $\mathfrak{o}$, т.е.

$$U_1^m = U_1, \qquad m\mathfrak{o} = \mathfrak{o}.$$

Перечислим общие свойства локальных полей:

1. Если характеристика локального поля k равна p, то группа U_1/U_1^p является бесконечной.
2. Если $k -$ локальное поле характеристики 0, то для любого натурального числа $m \geq 1$ группы k^{xm}, u^m, u_1^m являются открытыми подгруппами в k^x, а факторгруппы $k^x/k^{xm}, u/u^m, u_1/u_1^m -$ конечными группами 3. Если же характеристика поля k равна p, то аналогичные результаты справедливы для всех m, не делящихся на p.

§ II.5. Конечные расширения.

Пусть k' – произвольное расширение конечной степени локального поля k. Как отмечалось в начале предыдущего параграфа, поле k' также является локальным. Мы рассмотрим сейчас случай неразветвленного расширения k'/k [3,4].

Теорема II.5.1. Для всякого натурального $n1$ существует, и притом единственное (с точностью до изоморфизма над k), расширение k' степени n поля k, неразветвленное над k. Расширение k' представляет собой поле разложения многочлена $X^{q^l} - X$ над k и k'/k является циклическим расширением $n-$й степени. Если $\mathfrak{k}'-$ поле вычетов поля k', то каждый элемент σ группы Галуа $Gal(k'/k)$ индуцирует автоморфизм σ' расширения $\mathfrak{k}'/\mathfrak{k}$ и соответствие $\sigma \longmapsto \sigma'$ определяет естественный изоморфизм

$$Gal(k'/k) \rightarrow Gal(\mathfrak{k}'/\mathfrak{k}).$$

Доказательство. Докажем сначала существование поля k'. Так как $\mathfrak{k}$ является конечным полем, для всякого натурального $n \geq 1$ существует (и притом единственное) расширение $\mathfrak{k}^*$ степени n поля $\mathfrak{k}$, такое, что $\mathfrak{k}^*/\mathfrak{k}$ сепарабельно. Следовательно, кольцо $\mathfrak{k}[X]$ содержит некоторый неприводимый многочлен $g(X)$ степени n. Пусть $g(X)$ совпадает по $mod\ \mathfrak{p}$ с некоторым многочленом $f(X)$ степени n из $\mathfrak{o}[X]$ и $k'-$ поле, полученное присоединением к k некоторого корня α многочлена $f(X)$, т.е. $k' = k(\alpha)$ и $f(\alpha) = 0$. Очевидно, что $[k':k] \leq n$. Можно считать, что старшие коэффициенты многочленов $f(X)$ и $g(X)$ равны 1, в силу чего α оказывается элементом, целым над кольцом $\mathfrak{o}$; по этой причине α принадлежит кольцу $\mathfrak{o}'$. Следовательно, если $\omega-$ класс вычетов элемента α в поле $\mathfrak{k}' = \mathfrak{o}'/\mathfrak{p}'$, то $g(\omega) = 0,\ \omega \in \mathfrak{k}'$. Так как $g(X)-$ неприводимый многочлен степени n в $\mathfrak{k}[X]$ получаются соотношения

$$n = [\mathfrak{k}(\omega):\mathfrak{k}] \leq [\mathfrak{k}':\mathfrak{k}] = f(k'/k) \leq [k':k] \leq n.$$

Таким образом, $[k':k] = n = f(k'/k)$ и k' является неразветвленным расширением степени n поля k.

Пусть теперь k' – произвольное неразветвленное расширение степени n поля k. Так как $[\mathfrak{k}':\mathfrak{k}] = f(k'/k) = n$, поле $\mathfrak{k}'$ оказывается конечным полем из q^n элементов. Следовательно, в силу леммы 1 множество $A' = \left\{x' | x' \in k', x'^{q^n} = x'\right\}$ является полной системой представителей поля $\mathfrak{k}' = \mathfrak{o}'/\mathfrak{p}'$, содержащейся в $\mathfrak{o}'$. Если $k'' = k(A')$ и $\mathfrak{k}''$ – поле вычетов поля k'', то

$$k \subseteq k'' \subseteq k' \text{ и } \mathfrak{k} \subseteq \mathfrak{k}'' \subseteq \mathfrak{k}';$$

поскольку $A' \in k''$, справедливо равенство $\mathfrak{k}'' = \mathfrak{k}'$. Откуда следует, что

$$n = [\mathfrak{k}':\mathfrak{k}] = [\mathfrak{k}'':\mathfrak{k}] = f(k''/k) \leq [k'':k] \leq [k':k] = n.$$

Поэтому $k' = k'' = k$. Значит, k' – поле разложения над k многочлена $X^{q^n} - X$. Одновременно мы доказали и единственность поля k'. Так как многочлен $X^{q^n} - X$ имеет в k' q^n различных корней, расширение k'/k является сепарабельным и, следовательно, расширением Галуа. С другой стороны, так как $\mathfrak{k}$ – конечное поле, $\mathfrak{k}'/\mathfrak{k}$ – циклическое расширение степени n; и каждый элемент σ из $Gal(k'/k)$ определяет некоторый автоморфизм σ' расширения $\mathfrak{k}'/\mathfrak{k}$ и соответствие $\sigma \longmapsto \sigma'$ является гомоморфизмом групп $Gal(k'/k) \to Gal(\mathfrak{k}'/\mathfrak{k})$. Так как σ отображает множество A' корней многочлена $X^{q^n} - X$ на себя, а множество A' является полной системой представителей поля $\mathfrak{k}' = \mathfrak{o}'/\mathfrak{p}'$, равенство $\sigma' = 1$ означает, что $k' = k(A')$ остается на месте, т.е. $\sigma = 1$. Следовательно, гомоморфизм $Gal(k'/k) \to Gal(\mathfrak{k}'/\mathfrak{k})$ является инъективным. Кроме того, порядок обеих групп Галуа равен $n = [k':k] = [\mathfrak{k}':\mathfrak{k}]$ и, значит, $Gal(k'/k) \Rightarrow Gal(\mathfrak{k}'/\mathfrak{k})$. Но так как $Gal(\mathfrak{k}'/\mathfrak{k})$ – циклическая группа, $Gal(k'/k)$ также циклическая группа порядка n, откуда вытекает, что k'/k – циклическое расширение степени n.

Определение. Поскольку поле $\mathfrak{k}$ конечно и состоит из q элементов, группа Галуа $Gal(\mathfrak{k}'/\mathfrak{k})$ порождается автоморфизмом $\omega \longmapsto \omega^q, \omega \in \mathfrak{k}'$. Следовательно, в силу теореме II.5.1 этот автоморфизм соответствует некоторому элементу φ из $Gal(k'/k)$, такому, что

$$\varphi(x') \equiv x'^q mod\ \mathfrak{p}'$$

для всех $x' \in \mathfrak{o}'$. Элемент $\varphi -$ образующая группы $Gal(k'/k)$, которая этими соотношениями определяется однозначно. Автоморфизм φ называется автоморфизмом Фробениуса (или подстановкой Фробениуса).

Теорема II.5.2. Поле k' содержит поле разложения k_0 многочлена $X^{qf} - X$ над полем k. Поле k_0 является максимальным неразветвленным расширением поля k, содержащимся в k', и $[k_0 : k] = f$. Кроме того, расширение k'/k_0 является вполне разветвленным и $[k' : k_0] = e$.

Доказательство. Если $\mathfrak{k}' -$ поле вычетов локального поля k', то $[\mathfrak{k}' : \mathfrak{k}] = f$ и $\mathfrak{k}'$ является конечным полем из q^f элементов. Согласно лемме 1, в этом случае поле разложения k_0 многочлена $X^{qf} - X$ над k содержится в k'. Расширение k_0/k не разветвлено и имеет степень f. Если $k'' -$ произвольное неразветвленное расширение поля k, содержащееся в k', и $f_1 = f(k''/k) = [k'' : k]$, то по той же теореме k'' будет полем разложения над k многочлена $X^{qf_1} - X$. Однако, так как $f(k'/k) = f(k'/k'')f(k''/k)$, число f_1 является делителем числа f и, следовательно, $X^{qf} - X$ делится на $X^{qf_1} - X$. Поэтому $k'' \subseteq k_0$ и $k_0 -$ максимальное неразветвленное расширение поля kсодержащееся в k'. Так как расширение k_0/k неразветвленное, справедливы равенства $f(k_0/k) = [k_0 : k] = f = f(k'/k)$. Значит, $f(k'/k_0)$ и $k'/k_0 -$ вполне разветвленное расширение. Так как

$$[k' : k_0] = [k' : k] \cdot [k_0 : k]^{-1} = ef/f = e.$$

Описанное в этой теореме поле k_0 называется полем инерции расширения k'/k.

Теорема II.5.3. Если k'/k – расширение Галуа, то группа $Gal(k'/k_0)$ совпадает с инвариантной подгруппой G_0 группы $G = Gal\,(k'/k)$. Пусть

$$Gal(k'/k_0) = G_0, \qquad Gal(k_0/k) = G/G_0$$

Доказательство. Каждый элемент σ группы $Gal\,(k'/k)$ определяет автоморфизм σ' расширения $\mathfrak{k}'/\mathfrak{k}$, и отображение $\sigma \longmapsto \sigma'$ является групповым гомоморфизмом $Gal\,(k'/k) \to Gal\,(\mathfrak{k}'/\mathfrak{k})$. По определению группа G_0 является ядром этого гомоморфизма. С другой стороны, если $\mathfrak{k}_0$ – поле вычетов поля k_0, то определяется групповой изоморфизм $Gal\,(k_0/k) \twoheadrightarrow Gal\,(\mathfrak{k}_0/\mathfrak{k})$ и диаграмма

$$\begin{array}{ccc} Gal\,(k'/k) & \to & Gal\,(\mathfrak{k}'/\mathfrak{k}) \\ \downarrow & & \downarrow \\ Gal\,(k_0/k) & \twoheadrightarrow & Gal\,(\mathfrak{k}_0/\mathfrak{k}) \end{array}$$

Окзывается коммутативной. Однако вертикальные отображения здесь определяются соответствиями $\sigma \longmapsto \sigma|k_0$ и $\sigma' \longmapsto \sigma'|\mathfrak{k}_0$ и представляют собой гомоморфизмы. Кроме того, $f(k'/k) = f = [k_0 : k] = f(k_0/k)$, так что $\mathfrak{k}' = \mathfrak{k}_0$. Следовательно, G_0 является ядром отображения $Gal\,(k'/k) \to Gal\,(k_0/k)$ и совпадает с группой $Gal(k'/k_0)$.

Инвариантная подгруппа G_0 группы $G = Gal\,(k'/k)$, соответствующая полю инерции k_0, называется группой инерции расширения Галуа k'/k.

Теорема II.5.4. Для всякого конечного расширения Галуа k' локального поля k группа $Gal\,(k'/k)$ разрешима, т.е. расширение k'/k разрешимо.

Доказательство. Группа G/G_0 является циклической. Далее, в силу теоремы II.5.2 расширение k'/k_0 вполне разветвлено, так что группа $G_0 = Gal\,(k'/k_0)$ разрешима. Следовательно, разрешима и группа $G = Gal(k'/k)$.

Пусть $k-$ локальное поле, $k'-$ его расширение конечной степени, $N_{k'/k}-$ норменное отображение из k' в k и $U, U'-$ группы единиц в k и k' соответственно. Очевидно, $N_{k'/k}\,(k'^{\times})$ является подгруппой мультипликативной группы $k^{\times}$; из формулы вытекает равенство

$$N_{k'/k}(U') = N_{k'/k}\,(k'^{\times}) \cap U$$

Кроме того, группа U' компактна, и, в силу непрерывности норменного отображения $N_{k'/k}(U')$ является компактной подгруппой в U. Группы $N_{k'/k}\,(k'^{\times})$ и $N_{k'/k}(U')$ называются соответственно норменной группой и группой норменных единиц расширения k'/k.

Теорема II.5.5. Если k'/k неразветвленное расширение, то $N_{k'/k}(U') = U$.

Доказательство. С помощью униформизирующей π поля k можно определить следующие изоморфизмы:

$$U/U_1 \nrightarrow \mathfrak{k}^{\times}, \qquad U_n/U_{n+1} \nrightarrow \mathfrak{k}^{+}, \qquad n \geq 1$$

Если через T' и N' обозначить соответственно отображение следа и норменное отображение расширения конечных полей $\mathfrak{k}'/\mathfrak{k}$, то, применяя изоморфизм $Gal(k'/k) \nrightarrow Gal(\mathfrak{k}'/\mathfrak{k})$ из теоремы 4, можно построить следующие коммутативные диаграммы:

$$\begin{array}{ccc} U'/U_1' \nrightarrow \mathfrak{k}'^{\times} & & U_n'/U_{n+1}' \nrightarrow \mathfrak{k}'^{+} \\ \downarrow N \quad \downarrow N' & & \downarrow N \quad \downarrow T' \\ U/U_1 \nrightarrow \mathfrak{k}^{\times} & & U_n/U_{n+1} \nrightarrow \mathfrak{k}^{+} \end{array}$$

Так как в случае расширения конечных полей $\mathfrak{k}'/\mathfrak{k}$ отображения T', N' сюръективны, вертикальные отображения $N = N_{k'/k}$ этих диаграммах также сюръективны. Следовательно, каждый смежный класс из $U_n/U_{n+1} \geq 0$,

представляется элементом из $N_{k'/k}(U'_n)$. теперь нетрудно получить равенство $N_{k'/k}(U') = U$.

Теорема II.5.6. Если $k'-$ чисто несепарабельное расширение локального поля k степени $n = [k':k]$, то k'/k является вполне разветвленным и

$$N_{k'/k}(k') = k'^n = k.$$

Доказательство. Если характеристика поля k равна 0, то $k' = k,\ n = 1$ и утверждение леммы очевидно. Поэтому пусть характеристика поля k равна p и, следовательно, n является степенью числа p. Ранее было установлено, что в такой ситуации $k'-$ тоже локальное поле, которое в силу теоремы 1 содержит подполе F , изоморфное его полю вычетов $\mathfrak{k}'$, и при этом $k' = F((X))$. Учитывая, что $k'/k-$ чисто несепарабельное расширение, заметим, что $N_{k'/k}(x') = x'^n$ для произвольного x' и k' . Следовательно, $k'^n \subseteq k$. Кроме того, поле F, являясь конечным полем характеристики p, удовлетворяет соотношению $F^n = F$, в котором, как указывалось выше, m есть степень числа p. Значит,

$$k'^n = F((X^n))$$

Поле $F((X^n))$ лежит в $k' = F((X))$ и, так как $\left[F\left((X)\right): F\left((X^n)\right)\right] = n$, справедливы соотношения $[k':k] = n, k'^n \subseteq k$. Таким образом, $k = k'^n$. Далее, так как $\mathfrak{k}' \backsimeq F \subseteq k$ поле вычетов $\mathfrak{k}$ поля k совпадает с $\mathfrak{k}'$. Значит, $f = [\mathfrak{k}':\mathfrak{k}] = 1$ т.е. расширение k'/k является вполне разветвленным.

Теорема II.5.7. Если $k-$ локальное поле и k' любое его расширение конечной степени, то норменная группа $N_{k'/k}(k'^{\times})$ и группа норменных единиц $N_{k'/k}(U')$ расширения k'/k являются открытыми и, следовательно, замкнутыми подгруппами в $k^{\times}$, причем

$$\left[k^{\times}: N_{k'/k}(k'^{\times})\right] < +\infty, \qquad \left[U: N_{k'/k}(U')\right] < +\infty.$$

Доказательство. Обозначим для простоты $\left[U: N_{k'/k}(U')\right]$ через $i(k'/k)$ и докажем, что это конечное число. Пусть $k'/k -$ циклическое расширение простой степени. Тогда оно – либо неразветвленное, либо вполне разветвленное расширение. Это означает, что $i(k'/k) < +\infty$. Далее, так как характеристика поля k равна p и $k'/k -$ чисто несепарабельное расширение степени p, справедливо равенство $i(k'/k) = \left[U: N_{k'/k}(U') \cap U\right] = 1$. Пусть теперь $k'/k -$ произвольное конечное расширение и $k'' -$ промежуточное поле в k'/k; пусть $U'' -$ его единиц, так что

$$N_{k'/k''}(U') \subseteq U'', \qquad N_{k'/k}(U') \subseteq N_{k''k}(U'') \subseteq U,$$

$$\left[N_{k''k}(U''): N_{k'/k}(U')\right] \leq \left[U'': N_{k'/k''}(U')\right]$$

и, следовательно,

$$i(k'/k) \leq i(k'/k'')i(k''/k), \qquad i(k''/k) \leq i(k'/k).$$

Поэтому если $i(k'/k'') < +\infty$ и $i(k''/k) < +\infty$, то $i(k'/k) < +\infty$, и, наоборот, если $i(k'/k) < +\infty$, то $i(k''/k) < +\infty$. Поэтому, используя теорему 6 и рассуждая точно так же, как при доказательстве теоремы, легко установить, что если $k'/k -$ расширение конечной степени, то $i(k'/k) < +\infty$.

Группа $N_{k'/k}(U')$ является компактной; следовательно, группа U замкнута и, поскольку $i(k'/k'') < +\infty$, одновременно и открыта. Так как группа U открыта в $k^\times$, открытой в $k^\times$ будет и группа $N_{k'/k}(U')$. В свою очередь группа $N_{k'/k}(k^\times)$, содержащая $N_{k'/k}(U')$, очевидно, открыта в $k^\times$. Наконец, если $\pi -$ униформизирующая в k и $n = [k': k]$, то $\pi^n = N_{k'/k}(\pi) -$ элемент из $N_{k'/k}(k'^\times)$ и, поскольку $k^\times = \langle\pi\rangle \times U$ и $i(k'/k) < +\infty$, справедливо соотношение $\left[k^\times: N_{k'/k}(k'^\times)\right] < +\infty$.

Мы рассмотрим сейчас один пример, связанный с группой норменных единиц, очень важный для дальнейшего изложения. Пусть (k, v) – локальное $p-$ поле характеристики p. Поле k содержит конечное подполе F, изоморфное полю вычетов $\mathfrak{k} = \mathfrak{o}/\mathfrak{p}$, причем $k = F((X))$, $\mathfrak{o} = F[[X]]$, $\mathfrak{p} = (X) = XF[[X]]$. Если пользоваться прежними обозначениями, то $U_n = 1 + \mathfrak{p}^n,\ n \geq 1,\ F = F^p$ и $U = V \times U_1 = F^\times \times U_1$, так что

$$U^p = F^\times \times U_1^p = F^\times \times (1 + X^p F[[X^p]]).$$

Значит, для $m = \left[\frac{n}{p}\right]$ получаем

$$[U: U^p U_{n+1}] = [U_1: U_1^p U_{n+1}] = q^{n-m}, \qquad n \geq 1.$$

Здесь q – число элементов в $\mathfrak{k}$ и, следовательно, в F. Для произвольного элемента x из k положим

$$\wp(x) = x^p - x;$$

тогда $\wp: k^+ \to k^+$ будет эндоморфизмом аддитивной группы k^+ поля k и его ядром служит аддитивная группа F_p^+ простого поля F_p, содержащегося в k. Для произвольного $n \geq 0$ положим

$$A_n = X^{-n} F[[X]] = \{x | x \in k, v(x) \geq -n\}, \qquad B_n = A_n \cap \wp(k^+).$$

Так как $\wp(F) \subseteq F$ и $F_p \subseteq F$, справедливо равенство $[F, \wp(F)] = p$. Далее, если $x \in \mathfrak{p}$, то ряд

$$y = \sum_{i=0}^{\infty} (-x)^{p^i}$$

будет сходящимся в $\mathfrak{p}$ и, поскольку $\wp(y) = x$, то $\mathfrak{p} = \wp(\mathfrak{p}) \subseteq \wp(k^+)$. С другой стороны, если $v(x) < 0$, то $v(\wp(x)) = pv(x) < 0$, в силу чего $B_0 = \mathfrak{o} \cap \wp(k^+) = \wp(\mathfrak{o}) = \wp(F) + \mathfrak{p}$ и, так как $A_0 = \mathfrak{o}$, получаем

$$[A_0: B_0] = [F: \wp(F)] = p.$$

Далее, если $v(x) < 0$ и $p|v(x)$, то, применяя равенство $F^p \equiv F$, можно найти такой элемент y из k, что

$$y \equiv x \; mod \; \wp(k^+), \qquad v(x) < v(y).$$

Следовательно, каждый смежный класс из A_n/B_n при $n \geq 1$ содержит элемент вида

$$\sum_{\substack{i=-n \\ p\nmid i}}^{-1} a_i X^i + a_0\,, \qquad a_i \in F,$$

при этом все a_i при $i \neq 0$ являются элементами из F, а $a_0 -$ элемент из системы представителей для $F/\wp(F)$. Тем самым получается полная система представителей для A_n/B_n. Отсюда

$$[A_n : B_n] = pq^{n-m}, \qquad m = \left[\frac{n}{p}\right].$$

Для результатов об этом групповом индексе нам потребуется материал следующей главы.

Пусть $\Omega -$ алгебраическое замыкание поля k и $k_x -$ содержащееся в Ω поле разложения многочлена $Y^p - Y - x$ построенного по произвольному элементу x из k. Если $\alpha -$ корень многочлена $Y^p - Y - x$, то полный набор корней этого многочлена будет таким: $\alpha, \alpha + 1, \dots, \alpha + p - 1$; поэтому

$$k_x = k(\alpha), \;\text{ где }\; \alpha^p - \alpha = x, \qquad \alpha \in \Omega.$$

Следовательно, для расширения k_x/k оказываются справедливыми следующие результаты теоремы Артина – Шрейера:

1) Если $x \in \wp(k^+)$, то $k_x = k$. Если же $x \notin \wp(k^+)$, то k_x/k является циклическим расширением степени p и группа $Gal(k_x/k)$ порождается автоморфизмом σ, таким, что $\sigma(\alpha) = \alpha + 1$. Более того, все

циклические расширения поля k степени p (содержащиеся в Ω) получаются таким образом.

2) Пусть $x, y \in k$; для выполнения равенства $k_x = k_y$ необходимо и достаточно , чтобы x и y принадлежали одному и тому же смежному классу из $k^+/\wp(k^+)$.

Если $x \in A_0 + \wp(k^+)$, то существует элемент $a \in F$, такой, что $x \equiv a \bmod \wp(k^+)$ и, таким образом, $k_x = k_a = k(\alpha_0)$, где $\alpha_0^p - \alpha_0 = a$. Очевидно, если $a \in \wp(F)$, то $\alpha_0 \in F$ и $k_x = k_a = k$. Если же $a \notin \wp(F)$, то в силу теоремы Артина – Шрейера, примененной к F, расширение $F(\alpha_0)/F$ является циклическим степени p; следовательно, поле

$$k_x = k_a = F(\alpha_0)\big((X)\big)$$

Не разветвлено над $k = F\big((X)\big)$. Если $x \notin A_0 + \wp(k^+)$, то в силу 1) и 2) поле k_x не совпадает с неразветвленным расширением $k_a = F(\alpha_0)\big((X)\big)$ поля k, являющимся циклическим и имеющим степень p, так как в силу теоремы 4 в Ω существует только одно неразветвленное расширение поля k степени p. Таким образом, $k_x/k -$ разветвленное расширение; поскольку его степень равна p, оно является вполне разветвленным.

Теорема II.5.8. Пусть $x -$ произвольный элемент аддитивной группы $A_n,\ n \geq 0$, о котором говорилось выше, и $k' = k_x = k(\alpha),\ \alpha^p - \alpha = x$. Тогда

$$U_{n+1} \subseteq N_{k'/k}(U'),$$

где $U' -$ группа единиц поля k'.

Доказательство. Пусть сначала $x \in A_0 + \wp(k^+)$ т.е. $x \in A_0 + B_n$ и, как отмечалось выше, $k' = k_x = k$ а k'/k неразветвленное расширение степени p. Тогда в силу леммы 4 $N_{k'/k}(U') = U$ и утверждение доказано. Пусть, далее, $x \notin A_0 + \wp(k^+)$, т.е. $x \notin A_0 + B_n$, и, значит, k'/k является циклическим вполне разветвленным расширением степени p. Предположим,

что элемент x таков, что в $k' = k_x$ содержатся независимые от него смежные классы из A_n/B_n и с помощью системы представителей для A_n/B_n получаются равенства

$$v(x) = -i, \qquad 1 \leq i \leq n, \qquad p \nmid i.$$

Пусть $v' -$ регулярное нормирование поля $k', \pi' -$ его униформизирующая и $\sigma -$ образующая группы $Gal(k_x/k)$; тогда $v'(\sigma(\pi') - \pi') = s$, т.е. $\sigma(\pi') - \pi' + \beta\pi'^s$, $\beta \in k'$, $v'(\beta) = 0$ и в силу теоремы 5 $U_s \subseteq N_{k'/k}(U')$. Если $s = 1$, то справедливость леммы очевидна, так как $U_{n+1} \subseteq U_s$. Поэтому предположим, что она верна и для $s \geq 2$. Тогда в силу сказанного выше

$$\sigma\left(\pi'^{-i}\right) \equiv \pi'^{-i}(1 - i\beta\pi'^{s-1}) mod\ \pi'^{-i+s},$$

$$\sigma\left(\pi'^{-i+j}\right) \equiv \pi'^{-i+j} mod\ \pi'^{-i+s}, j \geq 1.$$

Поскольку $\alpha^p - \alpha = x$ и $v'(x) = pv(x) = -ip$, обязательно $v'(\alpha) = -i$. С другой стороны, k'/k является вполне разветвленным расширением и поле вычетов $\mathfrak{k}'$ поля k' совпадает с полем вычетов $\mathfrak{k}$ поля k; следовательно, F представляет собой полную систему представителей. Поэтому благодаря теореме 1 для элемента α из k' можно получить разложение вида

$$\alpha = \alpha_{-i}\pi'^{-i} + \alpha_{-i+1}\pi'^{-i+1} + \ \ldots, \alpha_{-i+j} \in F, \qquad \alpha_{-i} \neq 0.$$

Объединяя это с предыдущими формулами, получаем

$$\sigma(\alpha) \equiv \alpha - i\alpha_{-i}\beta\pi'^{-i+s-1} mod\ \pi'^{-i+s},$$

где $p \nmid i, \alpha_{-i} \in F, \alpha_{-i} \neq 0$ и $v'(\beta) = 0$; поэтому

$$v'(\sigma(\alpha) - \alpha) = -i + s - 1.$$

Но так как $\sigma(\alpha) = \alpha + 1$, левая часть последнего равенства равна 0; следовательно, $s = i + 1$. Тогда для $i \leq n$ получаем $U_{n+1} \subseteq U_s \subseteq N_{k'/k}(U')$, что и завершает доказательство леммы.

§ II.6. Алгебраические расширение и его норменная группа

Основными объектами рассмотрения являются локальное поле k и его алгебраические (в основном абелевы) расширения. Причины такого отбора материала станут вскоре ясны. Для удобства мы будем предполагать, что все рассмотрения проводятся в раз и навсегда фиксированном алгебраическом замыкании Ω поля k. Так как $\Omega/k-$ алгебраическое расширение, в соответствии с леммой 2 полное регулярное нормирование v поля kпродолжается единственным образом до нормирования μ поля Ω. Если $\bar{\Omega}-$ пополнение поля Ω относительно μ, то естественное продолжение нормирования μ на $\bar{\Omega}$ мы будем обозначать через $\bar{\mu}$. Если $F-$ произвольное алгебраическое расширение поля k, то с точностью до изоморфизма над k мы будем считать, что $F-$ промежуточное поле в расширении Ω/k. Так как поле $\bar{\Omega}$ является топологическим относительно топологии нормирования $\bar{\mu}$, оно содержит замыкание $\bar{F}$ поля F, которое, как легко понять, является пополнением поля F относительно ограничения нормирования $\mu|F$. В дальнейшем F/k будет обозначать алгебраическое расширение, для которого, таким образом,

$$k \subseteq F \subseteq \Omega, \qquad k \subseteq F \subseteq \bar{F} \subseteq \bar{\Omega};$$

кроме того, введем обозначения

$$v_F = \mu|F, \qquad v_{\bar{F}} = \bar{\mu}|\bar{F}.$$

Заметим, что v_F- это единственное продолжение нормирования v на алгебраическое расширение F поля k и $v_{\bar{F}}$ является естественным продолжением на $\bar{F}$ нормирования v_F.

Пусть $\sigma-$ автоморфизм над k поля F; он является топологическим и $v_F \circ \sigma = v_F$. Следовательно, в силу непрерывности автоморфизм σ однозначно продолжается до топологического автоморфизма $\bar{\sigma}$ поля $\bar{F}$ и

$v_{\bar{F}} \circ \bar{\sigma} = v_{\bar{F}}$. Так как $e(v_{\bar{F}}/v_F) = 1$ и v_F и $v_{\bar{F}}$ имеют одно и то же поле вычетов, автоморфизмы σ и $\bar{\sigma}$ задают один и тот же автоморфизм поля вычетов.

Рассмотрим случай, когда $F -$ расширение Галуа поля k. Его группа Галуа $Gal(F/k)$ компактна и вполне несвязна в топологии Крулля. Если $F' -$ промежуточное расширение в F/k . группа Галуа $Gal(F/F')$ является замкнутой подгруппой в $Gal(F/k)$. Поскольку F/k расширение Галуа, его можно представить как объединение конечных расширений Галуа k_i поля k, выбранных из семейства всех таких расширений $\{k_i\}_{i\in I}$. Если $k_i,\ k_j$ выбраны из этого семейства и $k_i \subseteq k_j$, то будем писать $i \leq j$; в этом случае отображение ограничения $\sigma \longmapsto \sigma|k_i$ на конечных группах определяет эпиморфизм групп Галуа

$$Gal\left(k_j/k\right) \to Gal\ (k_i/k).$$

Так как F является объединением полей $k_i,\ i \in I$, для любых двух индексов $i_1, i_2 \in I$ существует такой индекс $i_3 \in I$, что $i_1 \leq i_3$ и $i_2 \leq i_3$. Следовательно, соответствующее семейство эпиморфизмов, заиндексированных парами $i \leq j$, позволяет определить проективный предел конечных групп $Gal\ (k_i/k) -$ группу $\lim\limits_{\leftarrow} Gal\ (k_i/k)$, причем отображения ограничения $Gal\ (F/k) \to Gal\ (k_i/k)$ индицируют естественный изоморфизм

$$Gal\ (F/k) \rightarrow\!\!\!\!\!\rightarrow \lim_{\leftarrow} Gal\ (k_i/k)$$

Указанный здесь в правой части объект называется проконечной группой; эта группа компактна и вполне несвязна, а построенной изоморфизм является топологическим, если на группе $Gal\ (F/k)$ подразумевать топологию Крулля, в которой она компактна. В дальнейшем для простоты мы будем отождествлять эти две группы с помощью описанного изоморфизма, т.е. считать, что

$$Gal\ (F/k) = \varprojlim Gal\ (k_i/k).$$

Заметим, кроме того, что если $k \subseteq F' \subseteq F \subseteq \Omega$ и $F/F' -$ расширение Галуа, то и группа $Gal(F/F')$ является, аналогичным образом, проконечной.

До сих пор группа единиц локального поля или его пополнения обозначалась символами типа U, U', U_k ; в дальнейшем для всякого промежуточного поля F расширения Ω/k мы будем обозначать через $U(F)$ его группу единиц (а нормирование – через v_F). Аналогично для пополнения $\bar{F}$ поля F соответствующая группа единиц будет обозначаться через $U(\bar{F})$ (а нормирование – через $v_{\bar{F}}$) .

Пусть $F -$ произвольное расширение поля k; определим норменную группу $N(F/k)$ и группу норменных единиц $NU(F/k)$ соответственно следующими равенствами:

$$N(F/k) = \bigcap_{k\prime} N_{k'/k}\,(k'^{\times}), \qquad NU(F/k) = \bigcap_{k\prime} N_{k'/k}\,(U(k')),$$

Где k' пробегает все такие поля, что

$$k \subseteq k' \subseteq F, \qquad [k'\colon k] < +\infty,$$

И $N_{k'/k}$ обозначает обычное норменное отображение применительно к расширению конечной степени k'/k . Очевидно, что $N(F/k)$ и $NU(F/k)$ являются подгруппами в $k^{\times}$ и $U(k)$ соответственно, и если $F/k -$ расширение конечной степени, следует, что эти группы совпадают с определенными там норменной группой и группой норменных единиц соответственно. Если воспользоваться теоремой 7, то станет ясно, что $N(F/k)$ и $NU(F/k)$ являются замкнутыми подгруппами в $k^{\times}$. Далее, если $k \subseteq F' \subseteq F$. то

$$N(F/k) \subseteq N(F'/k) \text{ и } NU(F/k) \subseteq NU(F'/k).$$

Для любого конечного расширения k'/k справедливо равенство $NU(k'/k) = N(k'/k) \cap U(k)$; в случае произвольного расширения F оно остается справедливым, что следует непосредственно из определения, т.е.

$$NU(F/k) = N(F/k) \cap U(k).$$

Лемма II.6.1. Для любого натурального числа $n \geq 1$ имеет место равенство

$$NU(F/k)^n = \bigcap_{k'} N_{k'/k}\,(U(k'))^n\,.$$

Доказательство. Очевидно, что группа из левой части этого равенства принадлежит группе, стоящей в правой части. Рассмотрим произвольный элемент u из теоретико-множественного пересечения, которое представляет собой правая часть. Для всякого расширения k', фигурирующего в правой части, справедливы соотношения $k \subseteq k' \subseteq F,\ [k':k] < +\infty$, а вгруппе $N_{k'/k}(U(k'))$ обязательно существует элемент v. такой, что $v^n = u$. Пусть $S(k') -$ множество всех таких элементов v. В силу редположения множество $S(k')$ непусто. Кроме того, очевидно, что оно является замкнутым подмножеством компактной группы $U(k)$. далее, если $k \subseteq k_1', k_2' \subseteq F, [k_1':k] < +\infty,\ [k_2':k] < +\infty$, то $k \subseteq k_1'k_2' \subseteq F$ и $[k_1'k_2':k] < +\infty$ и при этом $S(k_1'k_2') \subseteq S(k_1') \cap S(k_2')$; в силу компактности группы $U(k)$ это означает, что пересечение множеств $S(k')$ по всевозможным k' является непустым. Если $w -$ элемент из этого пересечения, то $w \in NU(F/k)$ и $u = w^n \in NU(F/k)^n$. Тем самым лемма доказана.

Лемма II.6.2. Если $k \subseteq k' \subseteq F \subseteq \Omega,$ и $[k':k] < +\infty$, то

$$N_{k'/k}\big(NU(F/k')\big) = NU(F/k).$$

Доказательство. Так как $k'/k -$ конечное расширение, поле $k' -$ это локальное поле, строение которого аналогично строению исходного поля k.

В частности, аналогичным образом определяется группа норменных единиц $NU(F/k')$ алгебраического расширения F/k'. А именно пусть k'' пробегает всевозможные расширения конечной степени поля k', промежуточные в расширении F/k'; тогда

$$NU(F/k') = \bigcap_{k''} N_{k''/k'}\,(U(k''))$$

и, кроме того,

$$NU(F/k) = \bigcap_{k''} N_{k''/k}\,(U(k'')),$$

Откуда легко получается, что левая часть равенства, указанного в формулировке леммы, принадлежит правой части. Далее, если рассмотреть произвольный элемент u из правой части $NU(F/k)$, то для всякого k'' будет выполняться равенство $N_{k'/k}(v) = u$ при некотором $v \in N_{k''/k'}(U(k''))$. Если $S(k'') -$ множество всех таких элементов v из $N_{k''/k'}(U(k''))$, то как следует из рассуждений, аналогичных проведенным при доказательстве предыдущей леммы, множество $S(k'')$ является непустым замкнутым подмножеством в $U(k')$ и $S(k_1''k_2'') \subseteq S(k_1'') \cap S(k_2'')$. Следовательно, в силу компактности группы $U(k')$ пересечение множеств $S(k'')$ по всем k'' непусто. Любой элемент w из этого пересечения содержится в $NU(F/k')$ и $u = N_{k'/k}\big(NU(F/k')\big)$. Лемма доказана.

Пусть k, Ω и $\bar{\Omega}$ имеют прежний смысл. Если $k' -$ расширение конечной степени поля k, то $v_{k'} - \mu|k'$ является однозначно определенным продолжением на k' полного регулярного нормирования v поля k

$$e(k'/k) = e(v_{k'}/v) = [v_{k'}(k'^{\times}) : v(k^{\times})].$$

Следовательно, для того чтобы расширение k'/k было неразветвленным, необходимо и достаточно, чтобы $v_{k'}(k'^{\times}) = v(k^{\times}) = Z$,

т.е. чтобы v_k, было регулярным нормированием. Отсюда получается естественным образом следующее определение: произвольное (не обязательно конечное) алгебраическое расширение F поля k, $k \subseteq F \subseteq \Omega$, называется неразветвленным, если нормирование $v_F = \mu|F$ регулярно. Если $F/k -$ неразветвленное расширение и $F' \subseteq F$, то и $F'/k -$ неразветвленное расширение.

Пусть $q -$ число элементов в конечном поле $\mathfrak{k}$, являющемся полем вычетов локального поля k. Для всякого натурального числа $n \geq 1$ существует, и притом единственное, промежуточное расширение k_n, удовлетворяющее условиям

$$k \subseteq k_n \subseteq \Omega, \qquad [k_n : k] = n, \qquad k_n/k \text{ неразветвленное.}$$

Поле k_n служит полем разложения для многочлена $X^{q^n} - X$ над k, и расширение k_n/k является циклическим степени n; если $\mathfrak{k}_n -$ поле вычетов поля k_n, то естественное отображение $\sigma \longmapsto \sigma'$ определяет изоморфизм

$$Gal\,(k_n/k) \rightarrow Gal(\mathfrak{k}_n/\mathfrak{k}).$$

Если $n|m$, многочлен $X^{q^n} - X$ делит многочлен $X^{q^m} - X$ и $k_n \subseteq k_m$. Следовательно, объединение K всех полей k_n, $n \geq 1$, является промежуточным полем в расширении Ω/k. Заметим, что $v_K|k_n = \mu|k_n = v_{k_n} -$ регулярное нормирование на k_n; поэтому $v_K = \mu|K$ является объединением регулярных нормирований, в силу чего $K/k -$ неразветвленное расширение. С другой стороны, если $F/k -$ произвольное неразветвленное расширение и $\alpha \in F$, то $k\,(\alpha)/k$ будет неразветвленным расширением и, когда $[k(\alpha) : k] = n$, имеем для $k(\alpha) = k_n$. Следовательно, $\alpha \in k_n \subseteq K$, откуда $F \subseteq K$. По этой причине поле K называют максимальным неразветвленным расширением поля k (из числа содержащихся в Ω). В дальнейшем это K будет обозначаться символом k_{ur},

$$k_{ur} = K = \bigcup_{n \geq 1} k_n.$$

Так как всякое расширение k_n/k является абелевым, k_{ur}/k тоже абелево. Заметим, кроме того, что поле K получается из поля k присоединением всех корней всех многочленов $X^{q^n} - X$, $n \geq 1$. Иначе говоря, поле K получается из k присоединением всех корней из 1 степени $q^n - 1$ при всевозможных $n \geq 1$. Поскольку $k -$ локальное $p -$ поле, то q является степенью числа p; следовательно, если $V_\infty -$ множество всех корней из 1 в поле Ω, степень которых есть p^l для какого-либо целого числа $l > 0$, то

$$K = k_{ur} = k(V_\infty).$$

Теорема II.6.3. Поле вычетов $\mathfrak{k}_K$ поля $K = k_{ur}$ является алгебраическим замыканием поля вычетов $\mathfrak{k}$ поля k. Всякий автоморфизм σ из $Gal(K/k)$ определяет естественным образом автоморфизм σ' поля $\mathfrak{k}_K$ над $\mathfrak{k}$, и соответствие $\sigma \longmapsto \sigma'$ является топологическим изоморфизмом групп

$$Gal(K/k) \rightarrow Gal(\mathfrak{k}_K/\mathfrak{k}).$$

Доказательство. Так как при $n|m$ имеет место включение $k_n \subseteq k_m$, справедливы включения $\mathfrak{k}_n \subseteq \mathfrak{k}_m \subseteq \mathfrak{k}_K$. Следовательно, если принять во внимание, что $K -$ это объединение полей k_n, $n \geq 1$, а кольцо нормирования поля $K -$ объединение колец нормирования полей k_n, $n \geq 1$, то станет ясно, что $\mathfrak{k}_K$ это объединение подполей $\mathfrak{k}_n, n \geq 1$. С другой стороны, конечное поле $\mathfrak{k}$ имеет для любого натурального числа $n \geq 1$ единственное расширение степени n; поскольку $[\mathfrak{k}_n : \mathfrak{k}] = [k_n : k] = n$, сказанное выше означает, что $\mathfrak{k}_k$ является алгебраическим замыканием поля $\mathfrak{k}$. Далее, при $n|m$ обязательно $k_n \subseteq k_m$ и ограничение $\sigma \longmapsto \sigma|k_n$ определяет гомоморфизм $Gal(k_m/k) \rightarrow Gal(k_n/k)$; так как K является объединением полей $k_n \geq 1$, в соответствии с предыдущим параграфом получаем

$$Gal(K/k) = \varprojlim Gal(k_n/k).$$

Аналогично

$$Gal(\mathfrak{k}_K/\mathfrak{k}) = \lim_{\leftarrow} Gal(\mathfrak{k}_n/\mathfrak{k}).$$

Отображение $\sigma \longmapsto \sigma'$ из формулировки данной теоремы является для всех $n \geq 1$ изоморфизм групп $Gal(k_n/k) \rightarrow Gal(\mathfrak{k}_n/\mathfrak{k})$; поэтому, сравнивая два полученных равенства, получаем

$$Gal(K/k) \rightarrow Gal(\mathfrak{k}_K/\mathfrak{k})$$

что и требовалось.

Так как K/k неразветвленное расширение и $v_K -$ регулярное нормирование, пополнение $(\overline{K}, v_{\overline{K}})$ поля (K, v_K) является полным полем. При этом поле вычетов $\mathfrak{k}_{\overline{K}}$ поля совпадает с полем вычетов $\overline{K}$ поля. В силу предыдущей теоремы $\mathfrak{k}_k$ алгебраически замкнуто; поэтому $(\overline{K}, v_{\overline{K}})$ является замкнуто-полным. Таким образом, проведенные построения можно рассматривать как естественный способ построить по заданному локальному полю k замкнуто-полное поле $\overline{K}$. Например, если $\overline{F} -$ алгебраическое замыкание конечного поля F, то замкнуто-полное поле $\overline{K}$, соответствующее локальному полю $k = F\big((X)\big)$, будет полем формальных степенных рядов $\overline{F}\big((X)\big)$.

Так как поле $\mathfrak{k}$ состоит из q элементов, а $\mathfrak{k}_k$ является его алгебраическим замыканием, отображение

$$\omega \longmapsto \omega^q, \qquad \omega \in \mathfrak{k}_k,$$

- автоморфизм поля $\mathfrak{k}_k$. этот автоморфизм из группы $Gal(K/k) \rightarrow Gal(\mathfrak{k}_K/\mathfrak{k})$, который в группе $Gal(K/k)$ обозначается через φ, называется автоморфизмом Фробениуса расширения K/k (или подстановкой Фробениуса). Если $\mathfrak{o}_K -$ кольцо нормирования поля K и $\mathfrak{p}_K -$ его максимальный идеал, то для всякого α из $\mathfrak{o}_K$ справедливо соотношение

$$\varphi(\alpha) \equiv \alpha^q mod\ \mathfrak{p}_K,$$

в котором заключено отличительное свойство элемента φ, выделяющее его в группе $Gal(K/k)$. Очевидно, что для любого $n \geq 1$ отображение φ определяет автоморфизм Фробениуса φ_n расширения k_n/k. Так как циклическая группа n-го порядка $Gal(k_n/k)$ порождается элементом φ_n, имеет место изоморфизм

$$Z/nZ \to Gal(k_n/k),$$

$$a\ mod\ n \longmapsto \varphi_n^a.$$

Если $n|m$, то $\varphi_m|k_n = \varphi|k_n = \varphi_n$ и коммутативна следующая диаграмма:

$$\begin{array}{ccc} Z/mZ & \to & Gal(k_m/k) \\ \downarrow & & \downarrow \\ Z/nZ & \to & Gal(k_n/k) \end{array}$$

Здесь левое вертикальное отображение задается естественным образом: $a\ mod\ m \longmapsto a\ mod\ n$. Следовательно, для всевозможных $n|m$ имеется система таких гомоморфизмов, что определен проективный предел

$$\tilde{Z} = \varprojlim Z/nZ,$$

а также в силу коммутативности указанной диаграммы проективный предел $Gal(K/k) = \lim_{\leftarrow} Gal(k_n/k)$, являющийся проконечной группой (т.е. компактной вполне несвязной группой), причем имеет место топологический изоморфизм

$$\tilde{Z} \Rightarrow Gal(K/k). \qquad (1)$$

Естественные гомоморфизмы $Z \to Z/nZ$, $n \geq 1$, задают вложение $Z \to \tilde{Z}$ благодаря чему Z становится плотной подгруппой в $\tilde{Z}$; легко проверить, что при этом натуральное число $1 \in Z$, переходя в $\tilde{Z}$, становится тем элементом,

который с помощью (1) переводится в автоморфизм Фробениуса φ расширения K/k, т.е. $1 \longmapsto \varphi$. Следовательно, с помощью (1) определяется изоморфизм

$$Z \rightarrow \langle \varphi \rangle,$$

$$n \longmapsto \varphi^n$$

Очевидно, что φ порождает в $Gal(K/k)$ подгруппу, являющуюся плотной, так как Z является плотной подгруппой в $\tilde{Z}$. Топологический изоморфизм (1) отображает единичный элемент 1 из Z в автоморфизм Фробениуса φ, откуда следует его единственность.

Если $p-$ простое число и $Z_p^+ -$ аддитивная группа кольца целых $p-$ адических чисел, то группа $\tilde{Z}$ оказывается изоморфной прямому произведению по всем p компактных групп Z_p^+.

Согласно предыдущей теореме, поле $\mathfrak{k}_K$ является объединением полей $\mathfrak{k}_n$ для всех $n \geq 1$; поэтому, если для каждого k_n, $n \geq 1$, то естественный гомоморфизм $\mathfrak{o}_K \to \mathfrak{k}_K = \mathfrak{o}_K/\mathfrak{p}_K$ задаст изоморфизм мультипликативных групп $V_\infty \rightarrow \mathfrak{k}_K^\times$. Согласно данному раннее определению, множество V_∞ содержится в Ω и состоит из всевозможных корней из 1 степени $q^n - 1$ (или, иначе говоря, степени $p^n - 1$). Следовательно, $\varphi(V_\infty) = V_\infty$, так как автоморфизм Фробениуса φ для каждого η из V_∞ дает сравнение $\varphi(\eta) \equiv \eta^q mod\ \mathfrak{p}_K$, а потому и равенство $\varphi(\eta) = \eta^q,\ \eta \in V_\infty$.

Докажем теперь несколько результатов о пополнении $\overline{K}$ поля $K = k_{ur}$, т.е. о замыкании поля K в поле $\tilde{\Omega}$. автоморфизм Фробениуса φ расширения K/k однозначно продолжается до автоморфизма $\bar{\varphi}$ поля $\overline{K}$, причем на поле вычетов $\mathfrak{k}_K = \mathfrak{k}_{\overline{K}}$ оба автоморфизма φ и $\bar{\varphi}$ индуцируют один и тот же автоморфизм $\omega \longmapsto \omega^q$. Для простоты в дальнейшем, если это не будет вызывать недоразумений, мы будем $\bar{\varphi}$ обозначать тоже через φ. Пусть, как обычно, $\mathfrak{k} = \mathfrak{o}/\mathfrak{p}$ и $\mathfrak{k}_{\overline{K}} = \mathfrak{o}_{\overline{K}}/\mathfrak{p}_{\overline{K}}$. Очевидно, с помощью автоморфизма $\varphi(= \bar{\varphi})$

можно определить следующие автоморфизмы аддитивной группы кольца нормирования $\mathfrak{o}_{\overline{K}}$ и мультипликативной группы единиц $U(\overline{K})$:

$$\varphi - 1 \colon \mathfrak{o}_{\overline{K}} \to \mathfrak{o}_{\overline{K}},$$

$$\alpha \longmapsto (\varphi - 1)\alpha = \varphi(\alpha) - \alpha,$$

$$\varphi - 1 \colon U(\overline{K}) \to U(\overline{K}),$$

$$\xi \longmapsto \xi^{\varphi - 1} = \varphi(\xi)/\xi.$$

Относительно этих автоморфизмов имеет место следующая теорема.

Теорема II.6.4. Если $\mathfrak{o} \to \mathfrak{o}_{\overline{K}}$ и $U(k) \to U(\overline{K})$ – естественные вложения, то последовательности

$$0 \to \mathfrak{o} \to \mathfrak{o}_{\overline{K}} \xrightarrow{\varphi - 1} \mathfrak{o}_{\overline{K}} \to 0,$$

$$1 \to U(k) \to U(\overline{K}) \xrightarrow{\varphi - 1} U(\overline{K}) \to 1$$

точны.

Доказательство. Для обеих последовательностей рассуждения однотипны. Поэтому рассмотрим лишь вторую из них. Заметим, что, так как поле $\mathfrak{k}_{\overline{K}} = \mathfrak{k}_K$ алгебраически замкнуто, отображение $\omega \longmapsto \omega^q - \omega$ группы $\mathfrak{k}_{\overline{K}}^+$ и отображение $\omega \longmapsto \omega^{q-1}$ группы $\mathfrak{k}_{\overline{K}}^\times$ являются сюръективными; следовательно,

$$(\varphi - 1)\mathfrak{o}_{\overline{K}} + \mathfrak{p}_{\overline{K}} = \mathfrak{o}_{\overline{K}}, \quad U(\overline{K})^{\varphi - 1}(1 + \mathfrak{p}_{\overline{K}}) = U(\overline{K}). \qquad (2)$$

Так как K/k – неразветвленное расширение, униформизирующая π поля k является униформизирующей и в K, а потому и в $\overline{K}$.

Если $\xi \in U(k)$, то, очевидно, $\xi^{\varphi - 1} = 1$. Пусть, обратно, ξ – элемент из $U(\overline{K})$, для которого $\xi^{\varphi - 1} = 1$, т.е. $\varphi(\xi) = \xi$. Так как $\mathfrak{k}_{\overline{K}} = \mathfrak{k}_K$, введенное выше множество V_∞ с присоединенным к нему нулевым элементом 0 составляет полную систему представителей для $\mathfrak{k}_{\overline{K}}$ в $\mathfrak{o}_{\overline{K}}$; эту систему мы будем

обозначать через A. Следовательно, элемент ξ единственным образом представляется в виде ряда

$$\xi = \sum_{n=0}^{\infty} a_n \pi^n, \quad a_n \in A.$$

Так как $\pi -$ униформизирующая поля k, имеет место равенство $\varphi(\pi) = \pi$. Далее для всякого элемента a из V_∞ и, следовательно, из A, согласно предыдущему, справедливы соотношения $\varphi(a) = a^q \in A$. Следовательно,

$$\xi = \varphi(\xi) = \sum_{n=0}^{\infty} \varphi(a_n)\, \varphi(\pi)^n = \sum_{n=0}^{\infty} a_n^q \pi^n, \qquad a_n^q \in A.$$

Но в силу единственности разложения $a_n^q = a_n,\ n \geq 0$. Поэтому все элементы $a_n,\ n \geq 0$. принадлежат основному полю k. Однако локальное поле k является полным, так что ряд $\xi = \sum_{n=0}^{\infty} a_n \pi^n$ сходится в k; значит, элемент ξ принадлежит $U(k) = k^\times \cap U(\overline{K})$. Тем самым доказана точность последовательности

$$1 \to U(K) \to U(\overline{K}) \xrightarrow{\varphi - 1} U(\overline{K}).$$

Пусть, далее, $\xi -$ произвольный элемент из $U(\overline{K})$. Докажем, что существует последовательности $\{\eta_n\}_{n \geq 0}$ элементов из $U(\overline{K})$, такая, что

$$\xi \equiv \eta_n^{\varphi - 1} mod\ \mathfrak{p}_{\overline{K}}^{n+1}, \qquad \eta_n \equiv \eta_{n+1} mod\ \mathfrak{p}_{\overline{K}}^{n+1}, \qquad n \geq 0.$$

Из (2) ясно. Что η_0 существует. Предположим, что существуют требуемые $\eta_0, \eta_1, \ldots, \eta_n\ (n \geq 0)$. Тогда $\xi \eta_n^{\varphi - 1} = 1 + \alpha \pi^{n+1}$. где $\alpha -$ элемент из $\mathfrak{o}_{\overline{K}}$; в силу (2) существует $\beta \in \mathfrak{o}_{\overline{K}}$, такой, что $\alpha \equiv (\varphi - 1)\beta\ mod\ \mathfrak{p}_{\overline{K}}$. После этого непосредственно проверяется, что элемент $\eta_{n+1} = \eta_n(1 - \beta \pi^{n+1})$ является таким элементом из $U(\overline{K})$, что

$$\xi \equiv \eta_{n+1}^{\varphi-1} mod\ \mathfrak{p}_{\overline{K}}^{n+2}, \qquad \eta_n \equiv \eta_{n+1} mod\ \mathfrak{p}_{\overline{K}}^{n+1}\ .$$

Следовательно, существование последовательности $\{\eta_n\}_{n\geq 0}$ доказано. Так как $\overline{K}-$ полное поле, последовательность $\{\eta_n\}_{n\geq 0}$ сходится в $\overline{K}$, и пусть $\eta = \lim_{n\to\infty}\eta_n$. Очевидно, что η являются тем элементом из $U(\overline{K})$, для которого $\xi = \eta^{\varphi-1}$.

Таким образом, отображение $U(\overline{K}) \xrightarrow{\varphi-1} U(\overline{K})$ сюръективно и теорема полностью доказана.

Лемма II.6.3. Если $K = k_{ur}$, то

$$N(K/k) = NU(K/k) = U(k).$$

Доказательство. Для всякого $n \geq 1$ имеет место равенство $N_{k_n/k}\big(U(k_n)\big) = U(k)$. Так как K является объединением всех k_n, $n \geq 1$, непосредственно из определения следует, что $NU(K/k) = U(k)$. Далее, униформизирующая π поля k одновременно является униформизирующей и в каждом k_n, в силу чего $k_n^{\times} = \langle\pi\rangle \times U(k_n)$. Поэтому

$$N_{k_n/k}(k_n^{\times}) = \langle\pi\rangle \times U(k).$$

Но поскольку $\langle\pi\rangle \simeq Z$, отсюда получается и равенство $NU(K/k) = U(k)$.

Лемма II.6.4. Пусть $F-$ алгебраические расширение поля k, т.е. $k \subseteq F \subseteq \Omega$. Для того чтобы норменная группа $N(F/k)$ содержала униформизирующую π поля k, необходимо и достаточно, чтобы

$$F \cap K = k, \text{ где } K = k_{ur}\ .$$

Доказательство. Пусть $F \cap K = k$, т.е. при $n \geq 2$ выполняется включение $k_n \subseteq F \cap K$. Тогда $N(F/k) \subseteq N(k_n/k) = \langle\pi^n\rangle \times U(k), n \geq 2$, откуда следует, что $N(F/k)$ не содержит униформизирующую поля k. Пусть, далее, $F \cap K = k$ и $k' -$ произвольное расширение конечной степени поля k,

содержащееся в F. Пусть $\Pi_{k'} -$ множество всех униформизирующих поля k'. Если $k' -$ любая униформизирующая поля k', то $\Pi_{k'} = \pi' U(k')$. Следовательно, множество $\Pi_{k'}$ является компактным в k'. Так как $k' \cap K = k$, расширение k'/k вполне разветвлено, в силу чего $N_{k'/k}(\pi') -$ униформизирующая поля k. Поэтому $N_{k'/k}(\pi') \in \Pi_k$. Отсюда

$$S(k') = N_{k'/k}(\Pi_{k'}) = N_{k'/k}(\pi')NU(k'/k)$$

и $S(k')$ является непустым компактным подмножеством в Π_k. Аналогично тому, как это было сделано при доказательстве леммы 1 в предыдущем параграфе, можно показать, что $S(k'_1k'_2) \subseteq S(k'_1) \cap S(k'_2)$; в силу компактности множества Π_k это означает, что пересечение всех $S(k')$ (по всем (k') является непустым. Если $\pi -$ элемент из этого пересечения, то он будет униформизирующей поля k, принадлежащей группе $N(F/k)$. Следовательно, лемма доказана.

§ II.7. Приложения теории локальных полей и конечных расширений к решению некоторых задач.

Пусть $F -$ поле, если $F -$ подполе поля E, то $E -$ расширение поля F, а E можно рассматривать как векторное пространство над F.

Элемент $\alpha \in E$ называется алгебраическим над F, если в F существует элементы $a_0, \dots, a_n$ $(n \geq 1)$ не все равны 0 и такие, что

$$a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$$

Расширение E поля F называется алгебраическим, если всякий элемент из E алгебраичен над $F_n[E:F] -$ размерность E и это обозначает степень E над F.

Эти данные применимы для решения следующих задач по алгебре.

Задача 1. Пусть $k -$ поле и $F \subset E$ расширение k и $[E:k] = [E:F][F:k]$. Доказать, что если $\{x_i\}\ i \in J -$ базис поля F над k и $\{u_j\}_{j\in J} -$ базис поля E над F, то $\{x_i y_j\}_{(i,j)\in J\times\gamma}$ будет базисам поля E над k.

Решение. Пусть $z \in E$. Существует элементы $\alpha_j \in F$, почти все равные нулю и такие, что

$$Z = \sum_{j\in J} \alpha_j J_k$$

Для каждого $j \in J$ существует элементы b_{ki}, из которых почти все равны 0, такие, что

$$\alpha_j = \sum_{i\in J} b_{ji}x_i\ ,$$

и следовательно

$$Z = \sum_j \sum_i b_{ji} x_i y_j$$

А это означает, что $\{x_i y_j\}$ – является семейством образующих для E над k. осталось показать, что оно линейно независимо. Пусть $\{c_{ij}\}$ семейство элементов над k, почти все из которых равны 0, такое, что

$$\sum_j \sum_i c_{ij} x_i y_j = 0$$

Тогда для каждого j так как все элементы

$$\sum_i c_{ij} x_i = 0$$

y_j линейно независимы над F. Наконец $c_{ij} = 0$ для каждого i, так как $\{x_i\}$ – базис поля F над k.

Задача 2. Пусть k – локальное поле характеристики $P, k = F((x))$. Доказать, что поле k' – произвольное расширение поля k конечной степени и

$$e = e(k'/k), \qquad f = f(k'/k)$$

Решение. Если поле F является полем вычетов и служит подполе в k. Так как F – конечное поле из q элементов, а его расширение F' степени n является полем разложения над F многочлена $Y^{q^n} - Y$. Отсюда следует, что поле $k' = F'((x))$ представляет собой по теореме II.5.2 расширение степени n поля k.

Причем, если $\forall x' \in k'$, где x' – элемент поля k', то есть некоторый степенной ряд, который получается из x' заменой каждого коэффициента z на a^q.

Таким образом $k' -$ произвольное расширение поля k конечной степени и $e = e(k'/k),\ f = f(k'/k)$, где $[k'\colon k] = e, [k_0\colon k] = e$.

Задача 3. Найти число элементов любого конечного поля.

Решение. Поле $\sum$ называется конечным, если оно состоит из конечного числа элементов. Все конечные поля имеют простую характеристику, и если характеристика некоторого конечного поля $\sum$ равна p, то это поле содержит простое подполе, не имеющие собственных подполей, которое изоморфно полю $Z_p -$ поле вычетов в кольце целых рациональных чисел Z по простому модулю p. Можно считать, что $Z_p \subset Z$. Расширение $\sum/Z_p -$ конечно. Если его степень равна m и если $\omega_1, \omega_2, \dots, \omega_m -$ базис $\sum$ над Z_p , то каждый элемент $\xi \in \sum -$ однозначно представлен в виде:

$$\xi = c_1\omega_1 + c_2\omega_2 + \ \dots + c_m\omega_m, \qquad \text{где}$$

c_i независимо друг от друга пробегает все p элементов из Z_p. Так как число всех таких линейных комбинаций равно p^m. Отсюда следует, что число элементов любого конечного поля равно степени его характеристики.

Задача 4. Доказать, что конечная подгруппа G мультипликативной группы K^* произвольного поля K всегда циклична.

Доказательство. Мультипликативная группа $\sum^*$ конечного поля $\sum$ является конечной абелевой группой. Если в абелевой группе существуют элементы порядков m и n , то в G существует также элемент, порядок которого равен общему наименьшему кратному к чисел m и n.

Пусть элементы x и $y \in G$ имеют порядки m и n соответственно. Если $(m, n) = 1$, то произведение $x\,y$ имеет порядок $k = m \cdot n$. В общем случае имеем каноническое разложение чисел m и n в произведения степеней простых чисел, найдем:

$$m = m_0 \cdot m_1\ ; \quad n = n_0 \cdot n_1\ ,$$

таких, что $(m_0, m_1) = 1$ и $k = m_0 \cdot m_1$ элементы x^{m_1} и y^{n_1} имеют порядки m_0 и n_0, а их произведение $x^{m_1}y^{n_1}$ имеет порядок $k = m_0 n_0$.

Пусть G конечная подгруппа порядка g мультипликативной группы поля K. Если m есть наибольший из порядков элементов группы G, то, $m \leq g$. С другой стороны из только что доказанного следует, что порядок любого элемента из G является делителем m, т.е. все элементы группы G являются корнями многочлена $t^m - 1$. Но в любом поле многочлен степени m не может иметь более m корней, поэтому $g \leq m$. Откуда следует $g = m$, а это означает, что группа $G -$ циклична.

ЗАКЛЮЧЕНИЕ

Многие математики современности и в настоящее время продолжают исследования по алгебраическим расширениям полей и их пополнениям по данному локальному полю, в частности используют топологический изоморфизм группы единиц такого поля на группу Галуа. Известно, что теория развивается только тогда, когда появляется необходимость решить очень нужную проблему или небольшую задачу.

Изучив необходимые факты, связанные с теорией локальных полей классов в данной квалификационной работе решены следующие задачи:

1. Если $k-$ поле, $F \in E$ расширение k и $[E:k] = [E:F] \cdot [F:k]$, то базис поля F над k будет базисом поля F над k.
2. Пусть $k-$ локальное поле характеристики p и k' произвольное расширение поля $k-$ будет конечной степени.
3. Найдено формула числа элементов любого конечного поля, степени его характеристики.
4. Доказано, что конечная подгруппа G мультипликативной группы k^* произвольного поля $k-$ всегда циклична.

Потребности развития смежных разделов математики и других наук приводят к тому, что некоторые математические законы получают уже видоизмененные формы, а это уже дальнейшее развитие теории.

Список использованной литературы

1. З.И.Боревич, М.Р.Шафаревич. Теория чисел. – Google.ru. 2012 г.
2. А.Вейль. Основы теории чисел. – М; Мир, 1972, 148 стр.
3. Вандер Варден. Алгебра. –М, Мир, 1969, 447 стр.
4. К.Айерленд, М.Роузен. Классическое введение в современную теорию чисел. –М, Мир, 1987, стр 403.
5. К.Ивасава. Локальная теория полей классов. М, Мир, 1983. 204 стр.
6. Г.Д.Януш. Алгебраические числовые поля. Google.ru. 2013 г.
7. Д.Фадеев. Лекции по алгебре. –М, Наука, 1984, 483 стр.