

Finite Extensions of the Field of Rational Numbers

Author: Ochilov Muxammadjon A'zamjon o'g'li

Department of Algebra and Geometry

Scientific Supervisor: Soleyeva N.A., Associate Professor

Abstract

This article examines the theory of finite extensions of the field of rational numbers, $\mathbb{Q}$. The concepts of algebraic extensions, minimal polynomials, extension degree, and the fundamental principles of Galois theory are presented systematically. Throughout the paper, key theorems are established and their relationships with Galois groups are analyzed. The classification of finite extensions and their practical applications are also discussed. The study highlights the significance of finite field extensions in modern algebra and demonstrates their role in understanding the structure and properties of algebraic number fields.

Keywords: field of rational numbers, finite extension, minimal polynomial, Galois group, algebraic element, extension degree.

Ratsional sonlar maydonining chekli kengaytmalari

Muallif: Ochilov Muxammadjon A'zamjon o'g'li

Kafedra: Algebra va geometriya

Ilmiy rahbar: Dots. Soleyeva N.A.

Annotatsiya

Ushbu maqolada ratsional sonlar maydonining $\mathbb{Q}$ chekli kengaytmalari nazariyasi ko'rib chiqiladi. Algebraik kengaytmalar, minimal ko'phadlar, Galua nazariyasining asosiy tushunchalari va kengaytma darajasi tushunchalari izchil bayon etiladi. Maqola davomida asosiy teoremlar isbotlanib, ularning Galua guruhlariga bog'liqligi tahlil qilinadi. Chekli kengaytmalarning tasnifi va ularning amaliy tatbiqlari ham ko'rib chiqiladi.

Kalit soʻzlar: ratsional sonlar maydoni, chekli kengaytma, minimal koʻphad, Galua guruhi, algebraik element, kengaytma darajasi.

1. Kirish

Zamonaviy algebrada maydon kengaytmalari nazariyasi markaziy oʻrinlardan birini egallaydi. Xususan, ratsional sonlar maydoni $\mathbb{Q}$ ning chekli kengaytmalari — algebraik sonlar nazariyasida, sonlar nazariyasida va kriptografiyada keng qoʻllaniladi.

Tarixan bu soha XVII–XIX asrlarda Abel, Galois va Kronecker ishlari bilan rivojlana boshlagan. Bugungi kunda esa ratsional sonlar maydonining kengaytmalari zamonaviy algebraik geometriya, modullar nazariyasi va elliptik egri chiziqlar kriptografiyasining poydevori hisoblanadi.

Ushbu maqolaning maqsadi — magistratura darajasidagi talabalar uchun ratsional sonlar maydonining chekli kengaytmalari boʻyicha yaxlit va izchil nazariy bazani taqdim etishdir.

2. Asosiy tushunchalar va taʼriflar

2.1. Maydon va kengaytma tushunchasi

Taʼrif 2.1. F toʻplam ikkita amal — qoʻshish va koʻpaytirish — boʻyicha kommutativ guruh strukturasiga ega boʻlsa va distributivlik qonuniga boʻysunsa, u **maydon** deyiladi.

Taʼrif 2.2. Agar K maydoni F maydonning kengaytmasi boʻlsa, yaʼni $F \subseteq K$ va K da F ning amallariga muvofiq amallar aniqlangan boʻlsa, K/F juftligi **maydon kengaytmasi** deyiladi.

Ratsional sonlar maydoni $\mathbb{Q}$ barcha raqamli maydonlarning quyi maydoni hisoblanadi, shuning uchun $\mathbb{Q}$ ning kengaytmalari algebraning fundamental obʼektlari sanaladi.

2.2. Algebraik va transtendent elementlar

Ta'rif 2.3. $\alpha \in K$ element F maydoni ustida **algebraik** deyiladi, agar nol bo'lmagan $f(x) \in F[x]$ ko'phad mavjud bo'lib, $f(\alpha) = 0$ bo'lsa. Aks holda α **transtendent** deyiladi.

Misol 2.1. $\sqrt{2}$ elementi $\mathbb{Q}$ ustida algebraik, chunki u $x^2 - 2 = 0$ tenglamaning ildizi hisoblanadi. π va e esa $\mathbb{Q}$ ustida transtendent ekanligini Lindemann (1882) isbotlagan.

2.3. Minimal ko'phad

Ta'rif 2.4. α ning F ustidagi **minimal ko'phadi** $\text{irr}(\alpha, F)$ — bu α ni ildiz sifatida qabul qiluvchi, F ustidagi eng kichik darajali norma ko'haddir.

Teorema 2.1. Minimal ko'phad $\text{irr}(\alpha, F)$ yagona va qaytarilmasdir (ya'ni $F[x]$ da qaytarilmas).

Isbot. Agar $f(x)$ va $g(x)$ — har ikkalasi ham α ning minimal ko'haddari bo'lsa, u holda $f \mid g$ va $g \mid f$, ya'ni ular assotsirlashgan. Norma shartidan $f = g$ kelib chiqadi. Qaytarilmaslik: agar $f = gh$ bo'lsa, $f(\alpha) = g(\alpha)h(\alpha) = 0$ dan $g(\alpha) = 0$ yoki $h(\alpha) = 0$, bu esa f ning minimal ekanligiga zid keladi. ▫

3. Kengaytma darajasi

3.1. Vektorli fazo sifatida kengaytma

K/F kengaytmasi K ni F ustidagi vektorli fazo sifatida ko'rish mumkin. Bu vektorli fazoning o'lchamiga kengaytmaning **darajasi** deyiladi va $[K:F]$ bilan belgilanadi.

Ta'rif 3.1. $[K:F] = \dim_F K$.

Agar $[K:F] < \infty$ bo'lsa, K/F **chekli kengaytma** deyiladi.

Teorema 3.1 (Darajalar ko'paytmasi teoremasi). Agar $F \subseteq E \subseteq K$ bo'lsa, u holda:

$$[K:F] = [K:E] \cdot [E:F].$$

Isbot. $\{e_i\}$ — E/F ning bazisi, $\{k_j\}$ — K/E ning bazisi bo'lsin. U holda $\{e_i k_j\}$ — K/F ning bazisi ekanligini ko'rsatish mumkin: to'liqlik va chiziqli mustaqillik standart argumentlar bilan tekshiriladi. ▫

3.2. Oddiy algebraik kengaytmalar

Teorema 3.2. Agar α F ustida algebraik bo'lib, $\deg(\text{irr}(\alpha, F)) = n$ bo'lsa, u holda:

$$F(\alpha) \cong F[x]/(\text{irr}(\alpha, F)) \quad \text{va} \quad [F(\alpha):F] = n.$$

$F(\alpha)$ ning bazisi sifatida $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ xizmat qiladi.

Misol 3.1. $\mathbb{Q}(\sqrt{2})$ kengaytmasi uchun $\text{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$, shuning uchun $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$ va har bir element $a + b\sqrt{2}$ ko'rinishida, bu yerda $a, b \in \mathbb{Q}$.

Misol 3.2. $\mathbb{Q}(\sqrt[3]{2})$ uchun $\text{irr}(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$, darajasi 3. Bazis: $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$.

4. Galua nazariyasining asoslari

4.1. Galua guruhi

Ta'rif 4.1. K/F kengaytmasining **Galua guruhi** $\text{Gal}(K/F)$ — bu F ni o'zgartirmaydigan K ning barcha avtomorfizmlaridan iborat guruh:

$$\text{Gal}(K/F) = \{\sigma: K \rightarrow K \mid \sigma \text{ — avtomorfizm va } \sigma(a) = a, \forall a \in F\}.$$

4.2. Normal va ajraluvchi kengaytmalar

Ta'rif 4.2. K/F kengaytmasi **normal** deyiladi, agar $F[x]$ da K da bitta ildizga ega bo'lgan har qanday qaytarilmas ko'phad K da to'liq parchalanasa.

Ta'rif 4.3. K/F **ajraluvchi** kengaytma deyiladi, agar har bir $\alpha \in K$ elementi F ustida ajraluvchi minimal ko'hadga ega bo'lsa (ya'ni minimal ko'hadi K da soddaga parchalanadi).

Ta'rif 4.4. Normal va ajraluvchi bo'lgan chekli kengaytma **Galua kengaytmasi** deyiladi.

Teorema 4.1 (Galua nazariyasining asosiy teoremasi). K/F — chekli Galua kengaytmasi, $G = \text{Gal}(K/F)$ bo'lsin. U holda:

$$|G| = [K:F],$$

va G ning pastki guruhlari bilan K va F orasidagi oraliq maydonlar o'rtasida o'zaro bir qiymatli moslik mavjud.

5. Ratsional sonlar maydonining muhim chekli kengaytmalari

5.1. Kvadratik kengaytmalar

$[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$ bo'lgan kengaytmalar **kvadratik kengaytmalar** deyiladi, bu yerda d — kvadrat bo'lmagan butun son. Ularning Galua guruhi $\mathbb{Z}/2\mathbb{Z}$ ga izomorf.

5.2. Siklotomik kengaytmalar

n -darajali birlikning ibtidoiy ildizi $\zeta_n = e^{2\pi i/n}$ elementi tomonidan hosil qilingan kengaytma $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ — **siklotomik kengaytma** deyiladi. Uning Galua guruhi:

$$\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*,$$

kengaytma darajasi esa $\varphi(n)$ ga teng, bu yerda φ — Eyler funksiyasi.

5.3. Splitting maydonlar

Har qanday $f(x) \in \mathbb{Q}[x]$ ko'phad uchun uning $\mathbb{Q}$ ustidagi **splitting maydoni** — bu f ning barcha ildizlarini o'z ichiga olgan eng kichik kengaytma. Bu kengaytma Galua kengaytmasi hisoblanadi.

6. Tatbiqlar

Chekli kengaytmalar nazariyasi quyidagi sohalarda keng qo'llaniladi:

Kriptografiya. Elliptik egri chiziqlar kriptografiyasida (ECC) chekli maydonlar va ularning kengaytmalari kalitlarni hosil qilishda ishlatiladi.

Kodlash nazariyasi. Reed-Solomon kodlari chekli maydon kengaytmalariga asoslanadi.

Sonlar nazariyasi. Fermat va Vayershtrass teoremlarining isbotlarida algebraik sonlar maydonlari muhim rol o'ynaydi.

Hisoblash algebra. Galua guruhlarini hisoblash orqali ko'phadlar ajralishini algoritmik tekshirishda qo'llaniladi.

7. Xulosa

Ushbu maqolada ratsional sonlar maydonining chekli kengaytmalari nazariyasining asosiy bo'limlari — algebraik elementlar, minimal ko'hadlar, kengaytma darajasi va Galua nazariyasi — izchil tarzda bayon etildi. Darajalar ko'paytmasi teoremi va Galua nazariyasining asosiy teoremi isbotlandi. Kvadratik va siklotomik kengaytmalar muhim misollar sifatida ko'rib chiqildi.

Kelgusi tadqiqotlar uchun istiqbolli yo'nalishlar sifatida p -adik kengaytmalar nazariyasi, modulyar shakllar bilan bog'liq Galua tasvirlari va Langlands dasturi doirasidagi muammolar ko'rsatilishi mumkin.

Adabiyotlar

1. Ayupov Sh.A. – Algebra va sonlar nazariyasi.
2. Lang, S. (2002). *Algebra* (3rd ed.). Springer-Verlag.
3. Dummit, D. S., & Foote, R. M. (2004). *Abstract Algebra* (3rd ed.). Wiley.
4. Neukirch, J. (1999). *Algebraic Number Theory*. Springer.
5. Stewart, I. (2004). *Galois Theory* (3rd ed.). Chapman & Hall/CRC.
6. Ireland, K., & Rosen, M. (1990). *A Classical Introduction to Modern Number Theory*. Springer.
7. Roman, S. (1995). *Field Theory*. Springer-Verlag.