KŪNŲ TEORIJA

2000 metų rudens paskaitos

1. Kūnų plėtiniai

2. Galua grupės

3. Polinomų Galua grupės

4. Mažos eilės grupių klasifikacija

5. Fundamentalioji teorema

6. Separabilusis ir normalusis plėtinys

7. Klasikiniai brėžimo skriestuvu ir liniuote uždaviniai

8. Išspendžiamos grupės

9. Radikalinis plėtinys ir polinomo išsprendžiamumas radikalais

10. Abelio teorema

Kiekvienas polinomas, kurio laipsnis neviršija 4, yra išsprendžiamas radikalais virš nulinės charakteristikos kūno. Gerai mums žinomos kvadratinės lygties sprendimas pirmą kartą buvo paminėtas jau 3 a.p.Kr. Diofanto "Aritmetikoje". 16-ame amžiuje italų matematikai Dž. Kardanas (G.Cardano,1501-1576) ir L.Feraris (L.Ferrari,1522-1565) išreiškė 3 -iojo ir 4 -ojo laipsnio polinomų šaknis radikalais. Po šio rezultato 300 metų buvo bandoma 5-ojo laipsnio polinomo sprendinius išreikšti radikalais. Tik 1826 metais N.Abelis įrodė, kad to padaryti negalima. Praeitame skyriuje mes matėme kodėl, dar daugiau, gavome būtinas ir pakankamas sąlygas polinomo išsprendžiamumui radikalais(Teorema 9.4). Šiame skyriuje mes įrodysime N.Abelio rezultatą: *bendro pavidalo polinomas, kurio laipsnis* > 4 *radikalais neišsprendžiamas.*

Iš Teoremos 9.4 žinome, kad jeigu polinomo $f \in K[x]$ Galua grupė yra neišsprendžiama, tai lygtis $f(x) = 0$ yra neišsprendžiama radikalais. Mes rasime

polinomus, kurių Galua grupė yra neišsprendžiama grupė S_p, čia $p \geq 5-$ pirminis skaičius. Pradėsime lema apie pačią grupę S_p.

Lema 10.1 *Tegu $p-$ yra pirminis skaičius. Jeigu S_p pogrupyje H yra transpozicija ir ilgio p ciklas, tai $H = S_p$.*

Įrodymas. Tegu transpozicija $(12) \in H$ (priešingu atveju, pakeiskime numeraciją). Tegu ilgio p ciklas $\sigma' \in H$. Aišku, kad šį ciklą galime pradėti vienetu: $\sigma' = (1i_2...i_p)$. Pakėlus ciklą tam tikru laipsniu s ir pasinaudojų tuo, kad p yra pirminis, galite pasiekti, kad $(\sigma')^s = (12a_3...a_p) = \sigma$, o pakeitę numeraciją, pasieksite tai, kad $\sigma = (123...p)$. H yra pogrupis, todėl $\tau = (23...p) = (12)(123...p) \in H$. Turime, kad $\tau^k(12)\tau^{k-1} = (1, k+1) \in H$ su visais $1 \leq k \leq p-1$. Gavome, kad $(12), (13), ..., (1,p) \in H$. Tada su visais $k_1, k_2 \neq 1$, $(1,k_1)(1,k_2)(1,k_1) = (k_1, k_2) \in H$. Gavome, kad visos transpozicijos yra pogrupyje H. Tada $H = S_p$.
Įrodyta.

Dabar galime pateikti neišsprendžiamų radikalais polinomų pavyzdžių.

Teorema 10.2 *Tegu p yra pirminis skaičius, o $f \in \mathbf{Q}[x]$ yra neredukuojamas virš $\mathbf{Q}$ polinomas, kurio laipsnis p. Jeigu polinomas f turi lygiai $p-2$ realias šaknis, tai polinomo f Galua grupė yra izomorfiška S_p. Taigi, polinomas f yra neišsprendžiamas radikalais.*

Įrodymas.Tegu $F \subseteq \mathbf{C}$ yra polinomo f skaidinio kūnas virš $\mathbf{Q}$, o $G =$Gal$(F/K) -$ polinomo f Galua grupė. Tegu $\alpha \in F$ yra polinomo šaknis. Polinomas f yra neredukuojamas, todėl $[\mathbf{Q}(\alpha) : \mathbf{Q}] = \deg f = p$. Pagal Teoremą 1.8 kūnų grandinei $F \supset \mathbf{Q}(\alpha) \supset \mathbf{Q}$ turime, kad p yra $[F : \mathbf{Q}] = (G : \langle \mathrm{id} \rangle)$ daliklis. Iš Silovo teoremos (Teorema 4.4 (1)) turime, kad grupėje G yra elementas, kurio eilė yra p (faktą: *jeigu pirminis p dalija grupės eilę, tai šioje grupėje yra elementas, turintis eilę p,* – vadina Koši teorema). Iš Teoremos 2.2 žinome, kad grupės G elementai yra polinomo f šaknų keitiniai ir todėl $G \subseteq S_p$. Vienintėliai elementai grupėje S_p, o tuo pačiu ir grupėje G, turintys eilę p, yra ilgio p ciklai. Gavome, kad grupėje G yra ilgio p ciklas.

Iš bendro algebros kurso žinome, kad jeigu $a + ib$ yra polinomo su realiais koeficientais kompleksinė šaknis, tai šio polinomo šaknimi yra ir $a - ib = \overline{a + ib}$. Iš sąlygos turime, kad funkcija $\sigma : \mathbf{C} \to \mathbf{C}$, $\sigma(a + ib) = a - ib$ yra transpozicija, priklausanti grupei G (ji keičia dvi jungtines viena kitai polinomo kompleksines

šaknis, o realiąsias šaknis nekeičia). Gavome, kad polinomo f Galua grupėje G yra ir transpozicija, ir ilgio p ciklas. Iš Lemos 10.1 turime, kad $G = S_p$. Grupė $S_p, p \geq 5$, yra neišsprendžiama, todėl ir polinomas f yra neišsprendžiamas radikalais.

Įrodyta.

Baigdami skyrių, parodysime, kaip sukonstruoti polinomus neišsprendžiamus radikalais.

Pavyzdžiai 10.3 (1)Tegu $p \geq 5$ yra pirminis skaičius, o m- lyginis skaičius ir $n_1 < \cdots < n_{p-2}$ sveikieji skaičiai. Tegu $g(x) = (x^2 + m)(x - n_1) \cdots (x - n_{p-2})$, o $f(x) = g(x) - 2$. Polinomo $f(x) = x^p + a_{p-1}x^{p-1} + \cdots + a_1 x + a_0$ visi koeficientai yra lyginiai, bet $a_0 = -m \cdot n_1 \cdots n_{p-2} - 2$ nesidalija iš $2^2 = 4$. Pagal Eizenšteino kriterijų polinomas f yra neredukuojamas virš $\mathbf{Q}$. Turime, kad polinomas f yra $p-$ ojo laipsnio neredukuojamas polinomas, turintis $p - 2$ realias šaknis, kurio Galua grupė yra S_p ir todėl yra neišsprendžiamas radikalais.

Konkrečiu pavyzdžiu galėtų būti polinomas

$$f = (x^2 + 2)(x - 2)(x - 4)(x - 6) - 2 = x^5 - 12x^4 + 46x^3 - 72x^2 + 88x - 94.$$

(2) Kitas paprastesnis pavyzdys: $f(x) = x^5 - 4x + 2$. Pagal Eizenšteino kriterijų, kai $p = 2$, polinomas f yra neredukuojamas virš $\mathbf{Q}$. Žinodami, kad $f(x) < f(-2)$, kai $x < 2$, $f(-2) = -22$, $f(0) = 2$, $f(1) = -1$ $f(2) = 26$ ir $f(x) > f(2)$, kai $x > 2$, turime, kad funkcijos $y = f(x)$ grafikas kerta Ox ašį lygiai trijuose taškuose, t.y. polinomas turi lygiai tris realias šaknis. Pagal Teoremą 10.3 polinomas f yra neišsprendžiamas radikalais.