II S K Y R I U S
ŽIEDŲ IR KŪNŲ TEORIJOS ELEMENTAI

10. Idealai

10.1. Apibrėžimas. *Komutatyviojo žiedo A idealu vadinamas to žiedo adicinis pogrupis I, kai $I \cdot A \subset I$.*

10.2. Teorema (žiedo idealo požymis). *Žiedo A netuščias poaibis I yra to žiedo idealas tada ir tik tada, kai:*

1) *jei $\alpha, \beta \in I$, tai $\alpha - \beta \in I$;*

2) *jei $\alpha \in I$, $a \in A$, tai $a\alpha \in I$.*

Įrodymas. Būtinumas. 1) Tarkime, $\alpha, \beta \in I$. Tuomet $\alpha - \beta \in I$, nes I – adicinis žiedo A pogrupis.

2) Sąlygos būtinumas išplaukia iš idealo apibrėžimo. $\triangle$

Pakankamumas. Iš 1) sąlygos išplaukia, kad poaibis R yra adicinis žiedo A pogrupis. 2) sąlyga reiškia, kad $I \cdot A \subset I$. $\triangle$

10.3. Pavyzdžiai. 1) Žiedas A yra savo paties idealas, nes A yra adicinė grupė ir $A \cdot A \subset A$. Šis žiedas vadinamas *vienetiniu idealu.*

2) Aibė, sudaryta iš žiedo A nulinio elemento $I = \{0\}$, yra to žiedo idealas. Iš tikrųjų, $0 - 0 = 0 \in I$ ir $a \cdot 0 = 0 \in I$. Šis idealas vadinamas *nuliniu idealu.*

3) Fiksavę žiedo A elementus $\alpha_1, \alpha_2, \ldots, \alpha_n$, sudarykime aibę

$$I = (\alpha_1, \alpha_2, \ldots, \alpha_n) = \Big\{ \sum_{i=1}^{n} a_i \alpha_i \Big| a_i \in A, \;\; i = \overline{1, n} \Big\}.$$

Įrodysime, kad šis žiedo A poaibis yra idealas.

Tarkime,

$$\alpha = \sum_{i=1}^{n} a_i \alpha_i, \quad \beta = \sum_{i=1}^{n} b_i \alpha_i \in I. \quad \Longrightarrow$$

$$\alpha + \beta = \sum_{i=1}^{n} (a_i + b_i) \alpha_i \in I.$$

Tarkime $a \in A$, $\alpha = \sum_{i=1}^{n} a_i\alpha_i \in I$. $\Longrightarrow$

$$a\alpha = a\sum_{i=1}^{n} a_i\alpha_i = \sum_{i=1}^{n}(aa_i)\alpha_i \in I.$$

Šis idealas yra vadinamas elementų $\alpha_1, \alpha_2, \ldots, \alpha_n$ *generuotu idealu*. Kai $n = 1$, toks idealas vadinamas *vyriausiuoju idealu*, generuotu elemento α_1.

10.4. Teorema. *Visi sveikųjų skaičių žiedo Z idealai yra vyriausieji.*

Įrodymas. Tarkime, I yra žiedo Z idealas. Galime laikyti I nenuliniu idealu, kitaip būtų $I = (0)$. Idealui I priklauso bent vienas nenulinis skaičius a. Jei a – neigiamas, tai jau priešingas skaičius $-a$ – teigiamas, taip pat priklausantis I. Iš visų natūraliųjų skaičių, priklausančių idealui I, pasirenkame mažiausiąjį skaičių n ir įrodysime, kad jis ir generuoja patį idealą: $I = (n)$.

Tarkime, $a \in I$. Padalinę a iš n su liekana – $a = qn + r$, $0 \leq r < n$, įrodysime, kad $r = 0$. Tarkime priešingai, $r \neq 0$. Turime lygybę $r = a - qn$. Vadinasi $r \in I$, kadangi $a, n \in I$,. Gauname prieštarą skaičiaus n, kaip mažiausiojo natūraliojo skaičiaus, priklausančio idealui I, pasirinkimui. Vadinasi, $r = 0$. Todėl $a \in (n)$ ir $I \subset (n)$.

Tarkime, $a \in (n)$. Vadinasi, $a = nk$, $k \in Z$. Iš idealo I apibrėžimo gauname $a \in I$. Taigi $(n) \subset I$ ir galutinai gauname lygybę $I = (n)$. $\triangle$

Išskirsime idealo funkciją faktorizuojant.

Tarkime, I yra žiedo A idealas. Apibrėžiame žiede A ekvivalentumo ryšį: sakome, kad elementas a ekvivalentus elementui b ir rašome $a \sim b$, kai $a - b \in I$. Patikrinsime, ar šis sąryšis yra ekvivalentumo sąryšis.

1. $a \sim a$, nes $a - a = 0 \in I$.

2. Tarkime, $a \sim b$. Tuomet $a - b \in I$ ir jam priešingas elementas $-(a - b) = b - a \in I$. Todėl $b \sim a$.

3. Tarkime $a \sim b$, $b \sim c$. Vadinasi $a - b$, $b - c \in I$. Todėl ir šių elementų suma $(a - b) + (b - c) = a - b + b - c = a - c \in I$. Taigi $a \sim c$. $\triangle$

Įsitikinę, kad šis sąryšis yra ekvivalentumo sąryšis, pažymėkime $\overline{a}$ klasę, sudarytą iš visų žiedo A elementų, ekvivalenčių a:

$$\overline{a} = \big\{b \in A \mid b \sim a\big\}.$$

Įrodysime, kad $\overline{a}$ sutampa su sluoksniu $a + I$.

Tarkime, $b \in \overline{a}$. Vadinasi, $b \sim a$. Iš ekvivalentumo apibrėžimo turime $b - a \in I$, todėl $b \in a + I$. Gauname, kad $\overline{a}$ yra poaibis $a + I$: $\overline{a} \subset a + I$.

Tarkime, $b \in a + I$. Iš čia $b - a \in I$ ir $b \sim a$. Todėl $b \in \overline{a}$ ir $a + I \subset \overline{a}$. $\triangle$

Faktoraibėje A/I apibrėžiame sudėties ir daugybos operacijas –

$$(a+I)+(b+I)=a+b+I$$
$$(a+I)\cdot(b+I)=ab+I.$$

Kadangi šios operacijos tarp sluoksnių yra apibrėžtos per atstovus, būtina įrodyti jų apibrėžimo korektiškumą.

Tarkime $a'+I=a+I$, $b'+I=b+I$ ir

$$(a'+I)+(b'+I)=a'+b'+I,$$
$$(a'+I)\cdot(b'+I)=a'b'+I.$$

Turime įrodyti, kad $a'+b'+I=a+b+I$ ir $a'b'+I=ab+I$. Tam pakanka parodyti, kad atitinkamų sluoksnių sankirtos yra netuščios:

$$(a'+b'+I)\cap(a+b+I)\neq\emptyset \quad \text{ir}$$
$$(a'b'+I)\cap(ab+I)\neq\emptyset.$$

Elementas $a+b$ priklauso savo sluoksniui $a+b+I$, o $a'+b'\in a'+b'+I$.

Parodysime, kad sluoksniui $a+b+I$ priklauso elementas $a'+b'$. Iš tikrųjų,

$$(a'+b')-(a+b)=(a'-a)+(b'-b)\in I.$$

Vadinasi, $a'+b'\in a+b+I$ ir

$$(a'+b'+I)\cap(a+b+I)\neq\emptyset.$$

Kadangi šie sluoksniai kertasi netuščiai, jie sutampa.

Analogiškai parodome, kad sluoksnių $a'b'+I$ ir $ab+I$ sankirtai priklauso elementas $a'b'$:

$$a'b'-ab=a'b'-a'b+a'b-ab=a'(b'-b)+(a'-a)b\in I.$$

Todėl ir šie sluoksniai sutampa. Vadinasi, abi algebrinės operacijos yra apibrėžtos korektiškai. Šių operacijų atžvilgiu faktoraibė A/I sudaro žiedą:

1) sudėtis asociatyvi:

$$\big((a+I)+(b+I)\big)+(c+I)=(a+b+I)+c+I=$$
$$=a+b+c+I=a+I+(b+c+I)=(a+I)+\big((b+I)+(c+I)\big);$$

2) egzistuoja nulinis elementas – sluoksnis $0+I=I$:

$$(a+I)+(0+I)=(a+0)+I=a+I;$$

3) sluoksniui $a+I$ egzistuoja priešingas sluoksnis $-(a+I)=-a+I$:

$$(a+I)+(-a+I)=a-a+I=0+I=I;$$

4) sudėtis komutatyvi:

$$(a+I)+(b+I)=a+b+I=b+a+I=(b+I)+(a+I);$$

5) sandauga asociatyvi:

$$\big((a+I)\cdot(b+I)\big)\cdot(c+I)=(ab+I)\cdot(c+I)=abc+I=$$
$$(a+I)(bc+I)+(a+I)\big((b+I)\cdot(c+I)\big);$$

6) sudėtį ir daugybą jungia distributyvumo dėsnis:

$$\big((a+I)+(b+I)\big)\cdot(c+I)=(a+b+I)(c+I)=(a+b)c+I=$$
$$=ac+bc+I=(ac+I)+(bc+I)=(a+I)(c+I)+(b+I)(c+I).\quad\triangle$$

11. Žiedų homomorfizmai

11.1. Apibrėžimas. *Žiedo homomorfizmu žiede A' vadiname atvaizdį $\varphi: A\to A'$, stabilų žiedo A operacijų atžvilgiu, t. y.*

1) $\varphi(a+b)=\varphi(a)+\varphi(b)\qquad\forall a,b\in A;$

2) $\varphi(ab)=\varphi(a)\,\varphi(b)\qquad\forall a,b\in A.$

11.2. Pavyzdžiai. 1. Polinomų žiedo $A[t]$ atvaizdis φ žiede A, apibrėžtas lygybe

$$\varphi\big(f(t)\big)=f(0),$$

yra homomorfizmas. Iš tikrųjų,

$$\varphi\big(f(t)+g(t)\big)=f(0)+g(0)=\varphi\big(f(t)\big)+\varphi\big(g(t)\big),$$
$$\varphi\big(f(t)\cdot g(t)\big)=f(0)\cdot g(0)=\varphi\big(f(t)\big)\cdot\varphi\big(g(t)\big),$$

2. Sveikųjų skaičių žiedo Z atvaizdis φ lyginių skaičių žiede $2Z$, apibrėžtas lygybe,

$$\varphi(a)=2a,$$

nėra homomorfizmas. Iš tikrųjų, nors

$$\varphi(a+b)=2(a+b)=2a+2b=\varphi(a)+\varphi(b),$$

bet, pavyzdžiui,

$$\varphi(3\cdot 5)=\varphi(15)=30\neq\varphi(3)\cdot\varphi(5)=2\cdot 3\cdot 2\cdot 5=60.$$

3. Polinomų žiedo $R[t]$ atvaizdis φ į save, apibrėžtas lygybe

$$\varphi\big(f(t)\big)=f(t+1),$$

yra homomorfizmas. Iš tikrųjų,

$$\varphi\big(f(t)+g(t)\big)=f(t+1)+g(t+1)=\varphi\big(f(t)\big)+\varphi\big(g(t)\big),$$
$$\varphi\big(f(t)\cdot g(t)\big)=f(t+1)\cdot g(t+1)=\varphi\big(f(t)\big)\cdot\varphi\big(g(t)\big).$$

11.3. Apibrėžimas. *Žiedo A homomorfizmo φ žiede A' branduoliu vadinamas žiedo A elementų poaibis*

$$\operatorname{Ker}\varphi=\big\{a\in A\mid\varphi(a)=0'\big\}$$

(čia $0'$ –žiedo A' nulinis elementas).

11.4. Teorema. 1. *Homomorfizmo φ vaizdas $\varphi(A)$ yra žiedo A' požiedis.*

2. *Homomorfizmo φ branduolys* $\operatorname{Ker}\varphi$ *yra žiedo A idealas.*

Įrodymas. 1. Tarkime, $\varphi(a),\varphi(b)\in\varphi(A)$. Tuomet

$$\varphi(a)-\varphi(b)=\varphi(a-b)\in\varphi(A),$$
$$\varphi(a)\cdot\varphi(b)=\varphi(ab)\in\varphi(A).$$

Vadinasi, $\varphi(A)$ yra žiedo A' požiedis. $\triangle$

2. Tarkime, $a,b\in\operatorname{Ker}\varphi$. Tuomet

$$\varphi(a-b)=\varphi(a)-\varphi(b)=0'-0'=0'.$$

Vadinasi, $a-b\in\operatorname{Ker}\varphi$.

Tarkime, $a\in\operatorname{Ker}\varphi$, $b\in A$. Tuomet

$$\varphi(ab)=\varphi(a)\varphi(b)=0'\cdot\varphi(b)=0'.$$

Vadinasi, $ab\in\operatorname{Ker}\varphi$ ir branduolys $\operatorname{Ker}\varphi$ yra žiedo A idealas. $\triangle$

11.5. Teorema (pagrindinė žiedų homomorfizmų teorema). 1. *Tarkime, φ yra žiedo A homomorfizmas žiede A'. Tada faktoržiedis $A/_{\operatorname{Ker}\varphi}$ yra izomorfiškas vaizdui $\varphi(A)$:*

$$A/_{\operatorname{Ker}\varphi}\cong\varphi(A).$$

2. *Tarkime, I yra žiedo A idealas. Tada egzistuoja surjekcinis homomorfizmas $\varphi : A \to A/I$ toks, kad branduolys* $\operatorname{Ker}\varphi$ *sutampa su idealu I.*

Įrodymas. 1. Kadangi $\operatorname{Ker}\varphi$ yra žiedo A idealas, juo galime faktorizuoti ir nagrinėti faktoržiedžio $A/\operatorname{Ker}\varphi$ atvaizdžius žiedo A' požiedyje $\varphi(A)$.

Apibrėžkime atvaizdį $f : A/\operatorname{Ker}\varphi \to \varphi(A)$ lygybe

$$f(a + \operatorname{Ker}\varphi) = \varphi(a).$$

Pirmiausia įrodysime, jog šis atvaizdis yra apibrėžtas korektiškai. Tarkime, a' yra kitas sluoksnio $a + \operatorname{Ker}\varphi$ atstovas – $a' + \operatorname{Ker}\varphi = a + \operatorname{Ker}\varphi$ ir

$$f(a' + \operatorname{Ker}\varphi) = \varphi(a').$$

Turime įrodyti lygybę $\varphi(a) = \varphi(a')$. Iš lygybės $a' + \operatorname{Ker}\varphi = a + \operatorname{Ker}\varphi$ turime, kad $a' - a \in \operatorname{Ker}\varphi$. Vadinasi, $0' = \varphi(a - a') = \varphi(a) - \varphi(a')$. Todėl $\varphi(a) = \varphi(a')$. Taigi atvaizdžio f apibrėžimas nepriklauso nuo atstovų parinkimo, t. y. korektiškas. Įrodysime, kad f yra žiedų izomorfizmas.

1) f – homomorfizmas, nes

$$\begin{aligned} f(a + \operatorname{Ker}\varphi + b + \operatorname{Ker}\varphi) &= f(a + b + \operatorname{Ker}\varphi) = \varphi(a + b) = \varphi(a) + \varphi(b) = \\ &= f(a + \operatorname{Ker}\varphi) + f(b + \operatorname{Ker}\varphi); \end{aligned}$$

$$\begin{aligned} f\big((a + \operatorname{Ker}\varphi)(b + \operatorname{Ker}\varphi)\big) &= f(ab + \operatorname{Ker}\varphi) = \varphi(ab) = \varphi(a) \cdot \varphi(b) = \\ &= f(a + \operatorname{Ker}\varphi) \cdot f(b + \operatorname{Ker}\varphi). \end{aligned}$$

2) f – injekcija.

Tarkime priešingai, egzistuoja du skirtingi sluoksniai $a + \operatorname{Ker}\varphi$ ir $b + \operatorname{Ker}\varphi$, kurių vaizdai sutampa:

$$f(a + \operatorname{Ker}\varphi) = f(b + \operatorname{Ker}\varphi).$$

Tuomet $\varphi(a) = \varphi(b)$ ir $\varphi(a - b) = 0'$. Vadinasi, $a - b \in \operatorname{Ker}\varphi$ ir $a \in b + \operatorname{Ker}\varphi$. Todėl sluoksnių $a + \operatorname{Ker}\varphi$ ir $b + \operatorname{Ker}\varphi$ sankirta yra netuščia ir jie sutampa, kas prieštarauja sąlygai. Todėl atvaizdis f yra injekcija.

3) f – surjekcija. Iš tikrųjų, elemento $\varphi(a) \in \varphi(A)$ pirmvaizdžiu yra sluoksnis $a + \operatorname{Ker}\varphi$, nes

$$f(a + \operatorname{Ker}\varphi) = \varphi(a). \qquad \triangle$$

2. Tarkime, I yra žiedo A idealas. Apibrėžiame atvaizdį $\varphi : A \to A/I$ lygybe

$$\varphi(a) = a + I.$$

Šis atvaizdis – surjekcinis homomorfizmas. Iš tikrųjų,

$$\varphi(a+b) = a+b+I = (a+I)+(b+I) = \varphi(a)+\varphi(b),$$
$$\varphi(ab) = ab+I = (a+I)\cdot(b+I) = \varphi(a)\cdot\varphi(b).$$

Be to, sluoksnio $a+I$ pirmvaizdžiu (iš φ apibrėžimo) yra elementas a: $\varphi(a) = a+I$. $\triangle$

12. Pirminiai ir maksimalieji idealai

11.1. Apibrėžimas. *Žiedo A idealas I vadinamas pirminiu, jei iš sąlygos $x, y \in I$ išplaukia, kad arba $x \in I$, arba $y \in I$.*

12.2. Teorema (pirminio idealo požymis). *Žiedo A idealas yra pirminis tada ir tik tada, kai faktoržiedis A/I yra be nulio daliklių.*

Įrodymas. Būtinumas. Taikysime prieštaros metodą. Tarkime, $x+I$ ir $y+I$ yra faktoržiedžio A/I nulio dalikliai. Vadinasi $x+I$, $y+I \neq I$ ir

$$(x+I)\cdot(y+I) = I.$$

Tada $xy+I = I$ ir $xy \in I$. Bet $x, y \notin I$, vadinasi, gavome prieštarą sąlygai, kad I – pirminis idealas. $\triangle$

Pakankamumas. Taip pat taikysime prieštaros metodą. Tarkime, idealas I nėra pirminis. Vadinasi, egzistuoja elementai $x, y \in I$ tokie, kad $xy \in I$, o $x, y \notin I$. Iš paskutinės sąlygos išplaukia, kad ir $x+I$, $y+I \notin I$. Bet šių sluoksnių sandauga

$$(x+I)\cdot(y+I) = xy+I = I,$$

nes $xy \in I$. Gavome prieštarą sąlygai – faktoržiedyje A/I yra nulio daliklių. $\triangle$

12.3. Apibrėžimas. *Žiedo A idealas I vadinamas maksimaliuoju, kai jis nepriklauso jokiam kitam idealaui, išskyrus patį žiedą A.*

Iš apibrėžimo išplaukia, kad jei idealas I yra poaibis idealo J, tai arba I sutampa su J, arba J sutampa su A.

12.4. Teorema (maksimaliojo idealo požymis). *Tarkime, A yra komutatyvusis žiedas su vienetu. Žiedo A idealas I yra maksimalusis tada ir tik tada, kai faktoržiedis A/I yra kūnas.*

Įrodymas. Būtinumas. Tarkime, I yra maksimalusis idealas. Įrodysime, kad kiekvienas nenulinis faktoržiedžio A/I elementas turi atvirkštinį. Fiksuokime nenulinį faktoržiedžio A/I sluoksnį – $x+I$. Vadinasi, $x \notin I$. Sudarome žiedo A poaibį

$$(x, I) = \{ax+\alpha \mid a \in A, \alpha \in I\}.$$

Įrodysime, kad poaibis (x, I) yra žiedo A idealas.

1) Tarkime, $ax + \alpha$, $bx + \beta \in (x, I)$. Tada šių elementų skirtumas

$$(ax + \alpha) - (bx + \beta) = (a - b)x + (\alpha - \beta) \in (x, I),$$

nes $a - b \in A$, $\alpha - \beta \in I$.

2) Tarkime, $b \in A$, $ax + \alpha \in (x, I)$. Tada šių elementų sandauga

$$b(ax + \alpha) = (ba)x + (a\alpha) \in I,$$

nes $ba \in A$, $b\alpha \in I$. Vadinasi, poaibis (x, I) yra žiedo A idealas, kuriam priklauso idealas I. Kadangi $x \notin I$, idealas I yra idealo (x, I) tikrinis poaibis. Kadangi I – maksimalusis, idealas (x, I) turi sutapti su A: $(x, I) = A$. Vadinasi žiedo A vienetinis elementas e priklauso idealui (x, I). Todėl egzistuoja $y \in A$, $\alpha \in I$: $xy + \alpha = e$.

Įrodysime, kad sluoksnio $x + I$ atvirkštinis sluoksnis yra $y + I$. Iš tikrųjų,

$$e + I = xy + \alpha + I = xy + I = (x + I) \cdot (y + I).$$

Vadinasi, faktoržiedis A/I yra kūnas. $\triangle$

Pakankamumas. Tarkime, A/I yra kūnas ir idealas I priklauso idealui J. Įrodysime, kad idealas J sutampa arba su I, arba su A. Galime laikyti, kad $J \neq I$. Įrodysime, kad $J = A$. Egzistuoja elementas $x \in J$ ir $x \notin I$. Tuomet sluoksnis $x + I$ yra nenulinis. Jam egzistuoja atvirkštinis sluoksnis $y + I$:

$$(x + I) \cdot (y + I) = e + I.$$

Vadinasi, $xy + I = e + I$. Todėl $xy \in e + I$. Taigi egzistuoja $\alpha \in I$ toks, kad $xy = e + \alpha$. Išsireiškę iš šios lygybės e, turime

$$e = xy - \alpha \in J,$$

nes $x \in J$, $\alpha \in I \subset J$. Vadinasi ir bet kuris žiedo A elementas $a = a \cdot e \in J$. Todėl $A = J$ ir idealas I – maksimalusis. $\triangle$

Išvada. *Kiekvienas žiedo maksimalusis idealas yra pirminis.*

Įrodymas. Įrodymui pakanka fakto, kad kūne A/I nėra nulio daliklių. $\triangle$

Ne kiekvienas pirminis idealas yra maksimalusis. Pavyzdžiui, sveikųjų skaičių žiedo nulinis idealas (0) yra pirminis (nes $Z/(0) = Z$), bet ne maksimalusis.

12.5. Teorema. *Kiekvienas nenulinis tikrinis pirminis sveikųjų skaičių žiedo Z idealas I yra maksimalusis.*

Įrodymas. Žinome, kad idealas I yra vyriausiasis – egzistuoja $n \in N$ toks, kad $I = (n)$. Jei skaičius n būtų sudėtinis, faktoržiedis $Z/_{(n)}$ turėtų nulio daliklių. Vadinasi $I = (p)$, kur p – pirminis skaičius. Įrodysime, kad faktoržiedis $Z/_{(p)}$ yra kūnas. Tarkime, $x + (p)$ yra fiksuotas faktoržiedžio nenulinis sluoksnis. Rasime jam atvirkštinį. Kadangi $x \notin (p)$, tai $p \nmid x$. Todėl $(x, p) = 1$. Užrašome skaičių x ir p tiesinę išraišką – egzistuoja $u, v \in Z$ tokie, kad $xu + pv = 1$. Sluoksniui $x + (p)$ atvirkštinis yra sluoksnis $u + (p)$. Iš tikrųjų,

$$1 + (p) = xu + pv + (p) = xu + (p) = \big(x + (p)\big) \cdot \big(u + (p)\big).$$

Tokiu būdu įrodėme, kad idealas $I = (p)$ yra maksimalusis. $\triangle$

13. Algebrinių skaičių kūnai

Čia ir toliau nagrinėsime kompleksinių skaičių kūno C pokūnius. Tarkime, K yra vienas šių pokūnių. Kadangi $1 \in K$, tai ir

$$\underbrace{1 + 1 + \ldots + 1}_{n} = n \in K.$$

Be to, $-n \in K$, $0 \in K$. Vadinasi, sveikųjų skaičių žiedas Z yra kūno K poaibis. Jei $n, m \in Z$, $n \neq 0$, tai $m \cdot n^{-1} = \frac{m}{n} \in K$. Taigi šio kūno pokūniu yra racionaliųjų skaičių kūnas Q.

13.1. Apibrėžimas. *Jei kūnas K yra skaičių kūno L pokūnis, tai kūną L vadiname kūno K plėtiniu.*

Įsitikinsime, kad kūno K plėtinį L galima nagrinėti kaip vektorinę erdvę virš kūno K. Iš tikrųjų, L yra adicinė grupė ir yra apibrėžta daugybos operacija $K \times L \to L$, nes L – kūnas, o K – jo pokūnis.

13.2. Apibrėžimas. *Pėtinys $K \subset L$ yra vadinamas baigtiniu, kai vektorinė erdvė L virš kūno K yra baigtinio matavimo.*

Baigtinio plėtinio laipsniu yra vadinamas šios erdvės matavimas $\dim_K L$ ir žymimas $[L : K]$.

13.3. Teorema. *Jei plėtiniai $K \subset L$ ir $L \subset M$ yra baigtiniai, tai ir plėtinys $K \subset M$ yra baigtinis. Be to, plėtinių laipsniai susieti lygybe*

$$[M : K] = [M : L][L : K].$$

Įrodymas. Tarkime, $[M : L] = n$, $[L : K] = m$. Pasirinkime kurią nors erdvės L virš kūno K bazę $\alpha_1, \alpha_2, \ldots, \alpha_m$: $L = K\{\alpha_1, \alpha_2, \ldots, \ldots \alpha_m\}$ ir erdvės M virš kūno L bazę

$\beta_1, \beta_2, \dots \beta_n$: $M = L\{\beta_1, \beta_2, \dots, \beta_n\}$. Įrodysime, kad sandaugos $\alpha_i\beta_j$ $(i = \overline{1,m},\ j = \overline{1,n})$ sudaro erdvės M bazę virš kūno K. Tuo pačiu bus įrodyti abu teoremos teiginiai.

1) Įrodysime, kad elementų $\alpha_i\beta_j$, $(i = \overline{1,m}, j = \overline{1,n})$ sistema yra tiesiškai nepriklausoma virš kūno K. Tarkime, egzistuoja skaičiai $a_{ij} \in K$ tokie, kad galioja lygybė

$$\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}\alpha_i\beta_j = 0.$$

Parodysime, kad $a_{ij} = 0$ $(i = \overline{1,m}, j = \overline{1,n})$. Pastarojoje lygybėje pergrupuojame narius tokiu būdu:

$$\sum_{j=1}^{n} \beta_j \Big(\sum_{i=1}^{m} a_{ij}\alpha_i \Big) = 0.$$

Pažymėję

$$\lambda_j = \sum_{i=1}^{m} a_{ij}\alpha_j \in L,$$

turime lygybę

$$\sum_{j=1}^{m} \lambda_j\beta_j = 0.$$

Kadangi elementų sistema $\beta_1, \beta_2, \dots, \beta_n$ yra tiesiškai nepriklausoma virš kūno L, tai

$$\lambda_j = 0, \quad \text{kai } j = \overline{1,n}.$$

Vadinasi,

$$\sum_{i=1}^{m} a_{ij}\alpha_j = 0.$$

Bet elementų sistema $\alpha_1, \alpha_2, \dots, \alpha_m$ yra tiesiškai nepriklausoma virš kūno K, todėl

$$a_{ij} = 0, \quad \text{kai } i = \overline{1,m}, j = \overline{1,n}. \quad \triangle$$

2) Įrodysime, kad bet kuris kūno M elementas α yra vektorių sistemos $\{\alpha_i\beta_j\}$ $(i = \overline{1,m}, j = \overline{1,n})$ tiesinė kombinacija. Kadangi $M = L\{\beta_l, \beta_2, \dots, \beta_n\}$, egzistuoja elementai $\lambda_j \in L$, kad

$$\alpha = \sum_{j=1}^{n} \lambda_j\beta_j.$$

Kadangi $L = K\{\alpha_1, \alpha_2, \dots, \alpha_m\}$, su kiekvienu $\lambda_j \in L$ egzistuoja $a_{ij} \in K$, kad

$$\lambda_j = \sum_{i=1}^{m} a_{ij}\alpha_i.$$

Įstatę λ_j išraišką į aukščiau parašytą lygybę, turime

$$\alpha = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} \alpha_i \beta_j. \quad \triangle$$

13.4. Apibrėžimas. 1. *Kūno L skaičius α yra vadinamas algebriniu skaičiumi virš kūno K, kai egzistuoja polinomas $f(t) \in K[t]$, kurio šaknimi yra α, t. y. $f(\alpha) = 0$. Kitu atveju skaičus α yra vadinamas transcendentiniu virš kūno K.*

2. *Plėtinys $K \subset L$ yra vadinamas algebriniu virš kūno K, kai kiekvienas kūno L skaičius yra algebrinis virš to kūno. Kitu atveju plėtinys L vadinamas transcendentiniu virš kūno K.*

Pastaba. *Skaičius α yra vadinamas algebriniu (transcendentiniu), jei jis yra algebrinis (transcendentinis) virš racionaliųjų skaičių kūno Q.*

13.5. Pavyzdžiai. 1. Skaičius $\sqrt{2}$ yra algebrinis – jis yra, pavyzdžiui polinomo $f(t) = t^2 - 2$ šaknimi.

2. Menamasis vienetas i yra taip pat algebrinis – jis yra, pavyzdžiui, polinomo $f(t) = t^2 + 1$ šaknimi.

3. Yra įrodyta, kad dažnai naudojami skaičiai e, π yra transcendentiniai – nėra polinomo su racionaliaisiais koeficientais, kurių šaknimis būtų šie skaičiai.

13.6. Apibrėžimas. *Tarkime, α yra plėtinio L algebrinis skaičius virš kūno K. Skaičiaus α minimaliuoju polinomu virš kūno K vadiname mažiausio laipsnio polinomą $\varphi_\alpha(t) \in K[t]$ su vyriausiuoju koeficientu 1, kurio šaknimi yra skaičius α.*

13.7. Minimaliojo polinomo savybės. 1. *Minimalusis polinomas $\varphi_\alpha(t)$ yra neskaidus virš polinomų žiedo $K[t]$.*

2. *Bet kuris polinomas $f(t) \in K[t]$, kurio šaknimi yra skaičius α, dalosi polinomų žiede $K[t]$ iš minimaliojo polinomo $\varphi_\alpha(t)$.*

Įrodymas. 1. Tarkime priešingai, minimalus polinomas $\varphi_\alpha(t)$ yra skaidus. Vadinasi, egzistuoja polinomai $g(t)$, $h(t) \in K[t]$, $0 < \deg g(t), \deg h(t) < \deg \varphi_\alpha(t)$, tokie, kad

$$\varphi_\alpha(t) = g(t)\, h(t).$$

Įstatę vietoje kintamojo t skaičių α, gauname lygybę

$$0 = \varphi_\alpha(\alpha) = g(\alpha) \cdot h(\alpha).$$

Kadangui kūne nėra nulio daliklių, iš šios lygybės išplaukia, kad skaičius α yra arba polinomo $g(t)$, arba polinomo $h(t)$ šaknimi. Bet kuriuo atveju, tai prieštarauja minimaliojo

polinomo apibrėžimui, nes ir vieno, ir kito polinomo laipsnis mažesnis už polinomo $\varphi_\alpha(t)$ laipsnį. $\triangle$

2. Dalome polinomą $f(t)$ iš minimaliojo polinomo $\varphi_\alpha(t)$ su liekana:

$$f(t) = \varphi_\alpha(t)q(t) + r(t),\ \ 0 \le \deg r(t) < \deg \varphi_\alpha(t).$$

Įstatę vietoje kintamojo t skaičių α, gauname lygybę

$$0 = f(\alpha) = r(\alpha).$$

Kadangi minimalusis polinomas $\varphi_\alpha(t)$ yra mažiausio laipsnio polinomas, kurio šaknimi yra skaičius α, liekana $r(t)$ turi būti tapačiai lygi nuliui. Tuo pačiu polinomas $f(t)$ dalosi iš $\varphi_\alpha(t)$. $\triangle$

Išvada. *Visų polinomų $f(t) \in K[t]$, kurių šaknimi yra skaičius α, aibė sudaro žiedo $K[t]$ vyriausiąjį idealą, kurio generuojančiuoju elementu yra minimalusis polinomas $\varphi_\alpha(t)$.*

Įrodymas. Pažymėkime

$$I = \big\{ f(t) \in K[t] \mid f(\alpha) = 0 \big\}.$$

Įrodysime, kad vyriausiasis idealas $\big(\varphi_\alpha(t)\big)$ sutampa su I.
Tarkime, $f(t) \in \big(\varphi_\alpha(t)\big)$. Vadinasi,

$$f(t) = \varphi_\alpha(t) \cdot g(t),\ \ g(t) \in K[t].$$

Įstatę vietoje kintamojo t skaičių α, gauname lygybę

$$f(\alpha = \varphi_\alpha(\alpha)\, g(\alpha) = 0.$$

Vadinasi, $f(t) \in I$ ir $\big(\varphi_\alpha(t)\big) \subset I$.

Tarkime, $f(t) \in I$. Iš antrosios teoremos dalies išplaukia, kad polinomas $f(t)$ dalosi iš $\varphi_\alpha(t)$:

$$f(t) = \varphi_\alpha(t) \cdot g(t).$$

Vadinasi, $f(t) \in \big(\varphi_\alpha(t)\big)$ ir $I \subset \big(\varphi_\alpha(t)\big)$. Tuo pačiu $I = \big(\varphi_\alpha(t)\big)$. $\triangle$

Pastaba. *Iš šios teoremos išplaukia, kad neskaidus polinomas $\varphi(t) \in K[t]$, kurio šaknimi yra skaičius α, ir yra šio skaičiaus minimalusis polinomas $\varphi_\alpha(t)$.*

13.8. Pavyzdžiai. 1. Skaičiaus $\sqrt{2}$ minimalusis polinomas yra $\varphi_{\sqrt{2}}(t) = t^2 - 2$, nes $\varphi_{\sqrt{2}}(\sqrt{2}) = 0$ ir jis yra neskaidus polinomų su racionaliaisiais koeficientais žiede $Q[t]$.

2. Skaičiaus $\sqrt[3]{2}$ minimalusis polinomas yra $\varphi_{\sqrt[3]{2}}(t) = t^3 - 2$, nes $\varphi_{\sqrt[3]{2}}\big(\sqrt[3]{2}\big) = 0$ ir jis taip pat neskaidus žiede $Q[t]$.

13.9. Teorema. *Racionaliųjų skaičių kūno Q baigtinis plėtinys K yra algebrinis.*

Įrodymas. Tarkime plėtinio $Q \subset K$ laipsnis $[K : Q] = n$ ir α – fiksuotas kūno K elementas. Elementų $1, \alpha, \alpha^2, \ldots, \alpha^n$ sistema yra tiesiškai priklausoma, nes sistemos elementų skaičius viršija plėtinio $Q \subset K$ laipsnį. Vadinasi, egzistuoja racionalieji skaičiai $a_0, a_1, a_2, \ldots, a_n$, kurių bent vienas nenulinis, tokie, kad galioja lygybė

$$a_0 \cdot 1 + a_1 \cdot \alpha + a_2\alpha^2 + \ldots + a_n \cdot \alpha^n = 0.$$

Pažymėję

$$f(t) = a_0 + a_1 t + a_2 t^2 + \ldots + a_n t^n,$$

matome, kad šio polinomo su racionaliaisiais koeficientais šaknimi yra skaičius α. Vadinasi, bet kuris plėtinio $Q \subset K$ skaičius yra algebrinis ir tuo pačiu pats plėtinys taip pat algebrinis. $\triangle$

13.10. Apibrėžimas. 1. *Baigtinį racionaliųjų skaičių kūno Q plėtinį K vadiname algebrinių skaičių kūnu.*

2. *Algebrinį skaičių α vadiname m-tojo laipsnio algebriniu skaičiumi, kai jo minimaliojo polinomo $\varphi_\alpha(t)$ laipsnis lygus m.*

13.11. Teorema. *Tarkime, α yra pėtinio $K \subset L$ m-tojo laipsnio algebrinis skaičius, kurio minimalusis polinomas*

$$\varphi_\alpha(t) = t^m + c_1 t^{m-1} + \ldots + c_{m-1}t + c_m.$$

Tada aibė elementų

$$K(\alpha) = \left\{ \sum_{i=0}^{m-1} a_i\alpha^i \mid a_i \in K,\ \ i = \overline{0, m-1} \right\}$$

yra m-tojo laipsnio kūno K plėtinys.

Įrodymas. Pirmiausia įsitikinsime, kad aibė $K(\alpha)$ sudėties ir sandaugos atžvilgiu sudaro kūną. Pažymėkime

$$f(t) = \sum_{i=0}^{m-1} a_i t^i,\ g(t) = \sum_{i=0}^{m-1} b_i t^i,\ \ a_i, b_i \in K, i = \overline{0, m-1}.$$

Tada $f(\alpha)$ ir $g(\alpha)$ yra bet kurie aibės $K(\alpha)$ elementai. Parodysime, kad $f(\alpha) + g(\alpha)$, $f(\alpha) \cdot g(\alpha) \in K(\alpha)$. Iš tikrųjų,

$$f(\alpha) + g(\alpha) = \sum_{i=0}^{m-1} (a_i + b_i)\alpha^i \in K(\alpha).$$

Padaliname sandaugą $f(t)g(t)$ iš $\varphi_\alpha(t)$ su liekana:

$$f(t)g(t) = \varphi_\alpha(t)q(t) + r(t), \ \deg r(t) < m.$$

Pažymėję polinomą $r(t) = \sum\limits_{i=0}^{m-1} d_i t^i$ ir įstatę dalybos su liekana formulėje vietoje kintamojo t skaičių α, turime

$$f(\alpha)g(\alpha) = r(\alpha) = \sum_{i=0}^{m-1} d_i \alpha^i \in K(\alpha).$$

Nesunku įsitikinti, kad apibrėžtų operacijų atžvilgiu aibė $K(\alpha)$ sudaro žiedą. Įrodysime, kad šis žiedas su vienetu yra kūnas. Tam pakanka su kiekvienu $f(\alpha) \neq 0$ žiede $K(\alpha)$ rasti jam atvirkštinį skaičių.

Kadangi $f(\alpha) \neq 0$, tai polinomas $f(t)$ nesidalo iš minimaliojo polinomo $\varphi_\alpha(t)$. Bet $\varphi_\alpha(t)$ – neskaidus, todėl $\big(\varphi_\alpha(t), f(t)\big) = 1$. Užrašome šiems polinomams tiesinę išraišką. Egzistuoja polinomai $u(t), v(t) \in K[t]$ tokie, kad

$$\varphi_\alpha(t)u(t) + f(t)v(t) = 1 \quad \text{ir}$$

$$\deg v(t) < \deg \varphi_\alpha(t), \quad \deg u(t) < \deg f(t).$$

Įstatę šioje lygybėje $t = \alpha$, turime

$$f(\alpha)v(\alpha) = 1.$$

Kadangi $v(\alpha) \in K(\alpha)$, radome skaičiui $f(\alpha)$ atvirkštinį – $v(\alpha)$. Todėl $K(\alpha)$ yra kūnas. Iš $K(\alpha)$ apibrėžimo išplaukia, kad K yra to kūno pokūnis. Įrodysime, kad plėtinio $K \subset K(\alpha)$ laipsnis lygus m. Tam pakanka įrodyti, kad skaičiai $1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$ sudaro erdvės $K(\alpha)$ bazę. Iš kūno $K(\alpha)$ apibrėžimo išplaukia, kad kiekvienas to kūno skaičius yra sistemos $1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$ tiesinė kombinacija. Parodysime, kad ši sistema yra tiesiškai nepriklausoma. Tarkime priešingai – sistema yra tiesiškai priklausoma. Tada egzistuoja nenulinis kūno K skaičių rinkinys $a_0, a_1, \ldots, a_{m-1}$ toks, kad

$$a_0 + a_1\alpha + \ldots + a_{m-1}\alpha^{m-1} = 0.$$

Pažymėkime

$$h(t) = a_0 + a_1 t + \ldots + a_{m-1}t^{m-1} \in K[t].$$

Šio polinomo šaknimi yra skaičius α. Bet $\deg h(t) < \deg \varphi_\alpha(t)$, o tai prieštarauja minimaliojo polinomo apibrėžimui. $\triangle$

13.12. Teorema. *Tarkime, α yra algebrinis skaičius virš kūno K, $\varphi_\alpha(t)$ – jo minimalusis polinomas. Tada faktoržiedis $K[t]\big/\big(\varphi_\alpha(t)\big)$ yra izomorfiškas kūnui $K(\alpha)$.*

Įrodymas. Tarkime, $f(t) \in K[t]$. Padalinę šį polinomą iš polinomo $\varphi_\alpha(t)$ su liekana:

$$f(t) = \varphi_\alpha(t)\, q(t) + r(t), \quad \deg r(t) < m,$$

apibrėžiame atvaizdį $\varphi : K[t] \to K(\alpha)$ lygybe

$$\varphi\big(f(t)\big) = r(\alpha).$$

Norėdami šiam atvaizdžiui pritaikyti pagrindinę žiedų homomorfizmo teoremą, įrodysime, kad φ yra surjekcinis žiedų homorfizmas ir $\operatorname{Ker}\varphi = \big(\varphi_\alpha(t)\big)$.

Tarkime, $g(t) \in K[t]$ – kitas polinomas. Padalinę jį iš $\varphi_\alpha(t)$ su liekana:

$$g(t) = \varphi_\alpha(t)\, q_1(t) + r_1(t), \quad \deg r_1(t) < m,$$

turime $\varphi\big(g(t)\big) = r_1(\alpha)$. Sudėję polinomų $f(t)$ ir $g(t)$ dalybos iš $\varphi_\alpha(t)$ išraiškas, turime

$$f(t) + g(t) = \varphi_\alpha(t)\big(q(t) + q_1(t)\big) + r(t) + r_1(t).$$

Kadangi $\deg\big(r(t) + r_1(t)\big) < m$, ši išraiška yra polinomo $f(t) + g(t)$ dalybos iš $\varphi_\alpha(t)$ su liekana formulė. Todėl

$$\varphi\big(f(t) + g(t)\big) = r(\alpha) + r_1(\alpha) = \varphi\big(f(t)\big) + \varphi\big(g(t)\big).$$

Taigi atvaizdis φ yra adicinis homomorfizmas.

Sudauginę polinomų $f(t)$ ir $g(t)$ dalybos iš $\varphi_\alpha(t)$ su liekana išraiškas, turime

$$f(t)\, g(t) = \varphi_\alpha(t)\, q_2(t) + r(t) r_1(t).$$

Kadangi polinomo $r(t)\, r_1(t)$ laipsnis dali būti didesnis už polinomo $\varphi_\alpha(t)$ laipsnį, dalome jį iš $\varphi_\alpha(t)$ su liekana:

$$r(t)\, r_1(t) = \varphi_\alpha(t)\, q_3(t) + r_2(t), \quad \deg r_2(t) < m.$$

Iš čia gauname polinomo $f(t) \cdot g(t)$ dalybos iš $\varphi_\alpha(t)$ su liekana išraišką:

$$f(t) \cdot g(t) = \varphi_\alpha(t)\, q_2(t) + r(t)\, r_1(t) = \varphi_\alpha(t)\, \big(q_2(t) + q_3(t)\big) + r_2(t).$$

Įstatę šiose tapatybėse $t = \alpha$, gauname lygybes

$$f(\alpha)\, g(\alpha) = r(\alpha)\, r_1(\alpha) = r_2(\alpha).$$

Iš čia

$$\varphi\big(f(t)\, g(t)\big) = r_2(\alpha) = r(\alpha)\, r_1(\alpha) = \varphi\big(f(t)\big) \cdot \varphi\big(g(t)\big).$$

Vadinasi, atvaizdis φ yra ir multiplikacinis homomorfizmas.

Įsitikinsime, kad žiedų homomorfizmas φ yra surjekcija. Tarkime,

$$f(\alpha) = \sum_{i=0}^{m-1} a_i \alpha^i \in K(\alpha).$$

Pažymėję

$$f(t) = \sum_{i=0}^{m-1} a_i t^i,$$

padaliname šį polinomą iš $\varphi_\alpha(t)$ su liekana:

$$f(t) = \varphi_\alpha(t) \cdot 0 + f(t), \quad \deg f(t) < m.$$

Iš atvaizdžio φ apibrėžimo išplaukia lygybė

$$\varphi\big(f(t)\big) = f(\alpha).$$

Vadinasi, skaičiui $f(\alpha)$ radome pirmvaizdį – polinomą $f(t)$.

Liko įrodyti, kad branduolys $\operatorname{Ker}\varphi$ sutampa su idealu $\big(\varphi_\alpha(t)\big)$.

Tarkime, $f(t) \in \operatorname{Ker}\varphi$. Padalinę $f(t)$ iš $\varphi_\alpha(t)$ su liekana, gauname lygybę

$$f(t) = \varphi_\alpha(t)\, q(t) + r(t), \quad \deg r(t) < m.$$

Todėl $\varphi\big(f(t)\big) = r(\alpha) = 0$. Vadinasi, skaičius α yra polinomo, kurio laipsnis mažesnis už to skaičiaus minimaliojo polinomo laipsnį, šaknis. Todėl $r(t) \equiv 0$. Vadinasi,

$$f(t) = \varphi_\alpha(t)\, q(t)$$

ir $f(t) \in \big(\varphi_\alpha(t)\big)$. Gauname, kad $\operatorname{Ker}\varphi \subset \big(\varphi_\alpha(t)\big)$.

Tarkime, $f(t) \in \big(\varphi_\alpha(t)\big)$. Vadinasi,

$$f(t) = \varphi_\alpha(t) \cdot q(t), \quad q(t) \in K[t].$$

Iš čia turime, kad polinomo $f(t)$ dalybos iš $\varphi_\alpha(t)$ liekana $r(t) \equiv 0$. Bet $\varphi\big(f(t)\big) = r(\alpha)$. Todėl $\varphi\big(f(t)\big) = 0$. Vadinasi, $f(t) \in \operatorname{Ker}\varphi$ ir $\big(\varphi_\alpha(t)\big) \subset \operatorname{Ker}\varphi$. Tuo pačiu $\operatorname{Ker}\varphi = \big(\varphi_\alpha(t)\big)$.

Teoremos teiginys dabar išplaukia iš pagrindinės žiedų homomorfizmų teoremos. $\triangle$

Išvada. *Vyriausiasis žiedo $K[t]$ idealas $\big(\varphi_\alpha(t)\big)$ – maksimalusis.*

Įrodymas. Įrodymui pakanka pasinaudoti maksimaliojo idealo požymiu – faktoržiedis

$$K[t]\big/\big(\varphi_\alpha(t)\big) \cong K(\alpha)$$

yra kūnas. $\triangle$

14. Norma ir pėdsakas

Nagrinėsime algebrinių skaičių kūno K n-tojo laipsnio plėtinį L. Plėtinys L – taip pat algebrinių skaičių kūnas, nes K – baigtinis racionaliųjų skaičių kūno Q plėtinys.

Tarkime, $\alpha \in L$ ir jo minimalusis polinomas

$$\varphi_\alpha(t) = t^m + c_1 t^{m-1} + \ldots + c_{m-1}t + c_m, \quad c_i \in K,\ i = \overline{0,m}.$$

Apibrėžiame atvaizdį $f_\alpha : L \to L$ lygybe

$$f_\alpha(\beta) = \alpha\beta \qquad \forall\, \beta \in L.$$

Šis atvaizdis – tiesinė transformacija. Iš tikrųjų,

$$f_\alpha(b\,\beta + c\,\gamma) = \alpha(b\,\beta + c\,\gamma) = b \cdot \alpha\beta + c \cdot \alpha\gamma = \\ = b\,f_\alpha(\beta) + c\,f_\alpha(\gamma).$$

14.1. Apibrėžimas. *Tarkime, A yra tiesinės transformacijos f_α matrica kurioje nors bazėje. Skaičiaus α charakteringuoju polinomu vadiname tiesinės transformacijos f_α charakteringąjį polinomą $f_\alpha(t) = |tE - A|$.*

14.2. Teorema. *Tarkime, α yra n-tojo laipsnio plėtinio $K \subset L$ skaičius,* $\deg \varphi_\alpha(t) = m$, *$s = \frac{n}{m}$. Tada šio skaičiaus charakteringasis polinomas $f_\alpha(t)$ yra lygus jo minimaliojo polinomo $\varphi_\alpha(t)$ s-tajam laipsniui.*

Įrodymas. Nagrinėkime plėtinio $K \subset L$ tarpinį kūną $K(\alpha)$: $K \subset K(\alpha) \subset L$. Kadangi $[L : K] = n$, $[K(\alpha) : K] = m$, iš laipsnių formulės turime lygybę

$$[L : K(\alpha) = \frac{n}{m} = s.$$

Fiksuojame plėtinio $K(\alpha)$ bazę virš kūno K:

$$K(\alpha) = K\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$$

ir kurią nors plėtinio $K(\alpha) \subset L$ bazę virš $K(\alpha)$:

$$L = K(\alpha)\{\theta_1, \theta_2, \ldots, \theta_s\}.$$

Tuomet iš laipsnių formulės teoremos įrodymo galime parašyti plėtinio $K \subset L$ bazę virš kūno K:

$$L = K\{\theta_i\alpha^j \mid i = \overline{1,s},\ \ j = \overline{0,m-1}\}.$$

Norėdami užrašyti tiesinės transformacijos f_α matricą šioje bazėje, turime šia baze tiesiškai išreikšti skaičius $f_\alpha(\theta_i\alpha^j)$, $i=\overline{1,s}$, $j=\overline{0,m-1}$:

$$f_\alpha(\theta_1)=\theta_1\alpha=0\cdot\theta_1+1\cdot\theta_1\alpha+0\cdot\theta_1\alpha^2+\ldots+0\cdot\theta_1\alpha^{m-1}+$$
$$+0\cdot\theta_2+0\cdot\theta_2\alpha+0\cdot\theta_2\alpha^2+\ldots+0\theta_2\alpha^{m-1}+\ldots+$$
$$+0\cdot\theta_s+0\cdot\theta_s\alpha+0\cdot\theta_s\alpha^2+\ldots+0\cdot\theta_s\alpha^{m-1};$$
$$f_\alpha(\theta_1\alpha)=\theta_1\alpha^2=0\cdot\theta_1+0\cdot\theta_1\alpha+1\cdot\theta_1\alpha^2+\ldots+0\cdot\theta_1\alpha^{m-1}+$$
$$+0\cdot\theta_2+0\cdot\theta_2\alpha+0\cdot\theta_2\alpha^2+\ldots+0\cdot\theta_2\alpha^{m-1}+\ldots+$$
$$+0\cdot\theta_s+0\cdot\theta_s\alpha+0\cdot\theta_s\alpha^2+\ldots+0\cdot\theta_s\alpha^{m-1};$$
....
$$f_\alpha(\theta_1\alpha^{m-2})=\theta_1\alpha^{m-1}=0\cdot\theta_1+0\cdot\theta_1\alpha+0\cdot\theta_1\alpha^2+\ldots+0\cdot\theta_1\alpha^{m-2}+$$
$$+1\cdot\theta_1\alpha^{m-1}+0\cdot\theta_2+0\cdot\theta_2\alpha+0\cdot\theta_2\alpha^2+\ldots+$$
$$+0\cdot\theta_2\alpha^{m-1}+\ldots+0\cdot\theta_s+0\cdot\theta_s\alpha+0\cdot\theta_s\alpha^2+\cdot+0\cdot\theta_s\alpha^{m-1};$$

Kadangi $f_\alpha(\theta_1\alpha^{m-1})=\theta_1\alpha^m$ nėra bazinis skaičius, jį išskaidysime bazinių skaičių suma, pasinaudoję minimaliuoju polinomu $\varphi_\alpha(t)$. Skaičius α yra šio polinomo šaknis –

$$\alpha^m+c_1\alpha^{m-1}+\ldots+c_{m-1}\alpha+c_m=0.$$

Padauginę abi tapatybės puses iš θ_1, gausime $\theta_1\alpha^m$ išraišką baziniais skaičiais:

$$\theta_1\alpha^m=-c_m\theta_1-c_{m-1}\theta_1\alpha-\ldots-c_1\theta_1\alpha^{m-1}.$$

Analogiškai išskaidome skaičius $f_\alpha(\theta_i\alpha^j)$, kai $i=\overline{2,s}$, $j=\overline{0,m-1}$. Gausime transformacijos f_α matricą A, sudarytą iš s blokų A_m pagrindinėje įstrižainėje bei visų kitų nulinių blokų O:

$$A=\begin{pmatrix} A_m & O & \ldots & O\\ O & A_m & \ldots & O\\ \ldots & \ldots & \ldots & \ldots\\ O & O & \ldots & A_m\end{pmatrix},$$

$$A_m=\begin{pmatrix} 0 & 1 & 0 & \ldots & 0 & 0\\ 0 & 0 & 1 & \ldots & 0 & 0\\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\\ 0 & 0 & 0 & \ldots & 0 & 1\\ -c_m & -c_{m-1} & -c_{m-2} & \ldots & -c_2 & -c_1\end{pmatrix}.$$

Tuomet charakteringąjį polinomą $f_\alpha(t)$ galima užrašyti pavidalu:

$$f_\alpha(t)=|tE-A|=|tE-A_m|^s.$$

Pažymėkime $D_m = |tE - A_m|$ – m-tosios eilės determinantą. Šiam determinantui paskaičiuoti išvesime rekurentinę formulę. Skleidžiame determinantą D_m pirmuoju stulpeliu:

$$D_m = \begin{vmatrix} t & -1 & 0 & \dots & 0 & 0 \\ 0 & t & -1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & t & -1 \\ c_m & c_{m-1} & c_{m-2} & \dots & c_2 & t + c_1 \end{vmatrix} =$$

$$= (-1)^{1+1} \cdot t \begin{vmatrix} t & -1 & 0 & \dots & 0 & 0 \\ 0 & t & -1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & t & -1 \\ c_{m-1} & c_{m-2} & c_{m-3} & \dots & c_2 & t + c_1 \end{vmatrix} +$$

$$+(-1)^{m+1} \cdot c_m \begin{vmatrix} -1 & 0 & 0 & \dots & 0 & 0 \\ t & -1 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & t & -1 \end{vmatrix} =$$

$$= t\, D_{m-1} + (-1)^{m+1} \cdot c_m \cdot (-1)^{m-1} = t\, D_{m-1} + c_m.$$

Paskaičiuojame determinantą D_2 tiesiogiai:

$$D_2 = \begin{vmatrix} t & -1 \\ c_2 & t + c_1 \end{vmatrix} = t^2 + c_1 t + c_2.$$

Determinantui D_3 paskaičiuoti taikome rekurentinę formulę:

$$D_3 = tD_2 + c_3 = t(t^2 + c_1 t + c_2) + c_3 =$$

$$= t^3 + c_1 t^2 + c_2 t + c_3.$$

Iš determinantų D_2 ir D_3 išraiškų darome indukcinę prielaidą, kad

$$D_m = t^m + c_1 t^{m-1} + \ldots + c_{m-1} t + c_m.$$

Įrodymui taikome indukciją.

1^0. Kai $k = 2$, jau įrodyta.

2^0. Darome indukcinę prielaidą su visais $k \le m - 1$. Įrodysime teiginį, kai $k = m$. Pasinaudoję rekurentine formule bei indukcine prielaida, gauname lygybę

$$D_m = tD_{m-1} + c_m = t\big(t^{m-1} + c_1 t^{m-2} + \ldots + c_{m-2} t + c_{m-1}\big) + c_m =$$

$$= t^m + c_1 t^{m-1} + \ldots + c_{m-1} t + c_m = \varphi_\alpha(t).$$

Vadinasi,

$$f_\alpha(t) = |tE - A_m|^s = D_m^s = \big(\varphi_\alpha(t)\big)^s. \quad \triangle$$

14.3. Teorema. 1. *Panašių matricų determinantai sutampa.*

2. *Panašių matricų pėdsakai sutampa.*

Įrodymas. 1. Tarkime, matricos A ir B yra panašios. Vadinasi, egzistuoja neišsigimusi matrica T:

$$B = TAT^{-1}.$$

Tuomet

$$|B| = |TAT^{-1}| = |T|\,|A|\,|T^{-1}| = |A|. \quad \triangle$$

2. Pažymėkime $AT^{-1} = B$. Tuomet $A = BT$ ir $TAT^{-1} = TB$. Todėl pakanka įrodyti, kad komutuojančių matricų pėdsakai sutampa, t. y. $Tr(BT) = Tr(TB)$.

Tarkime, $B = (b_{ij})$, $T = (t_{ij})$. Tuomet

$$BT = \left(\sum_{k=1}^{n} b_{ik}\, t_{kj}\right), \quad TB = \left(\sum_{k=1}^{n} t_{ik}\, b_{kj}\right).$$

Vadinasi,

$$Tr(BT) = \sum_{i=1}^{n}\sum_{k=1}^{n} b_{ik}t_{ki},$$

$$Tr(TB) = \sum_{i=1}^{n}\sum_{k=1}^{n} t_{ik}b_{ki}.$$

Kadangi šių lygybių dešiniosios pusės lygios, tai $Tr(BT) = Tr(TB)$. $\quad \triangle$

Išvada. *Tiesinės transformacijos matricos determinanto ir pėdsako reikšmės nepriklauso nuo bazės parinkimo.*

Įrodymas. Iš tikrųjų, žinome, kad tiesinės transformacijos matricos skirtingose bazėse yra panašios. $\quad \triangle$

14.4. Apibrėžimas. *Plėtinio $K \subset L$ skaičiaus α norma $N_{L/K}(\alpha)$ vadinamas tiesinės transformacijos f_α matricos A kurioje nors bazėje determinantas – $N_{L/K}(\alpha) = |A|$, o skaičiaus α pėdsaku – tos transformacijos matricos pėdsakas – $Tr_{L/K}(\alpha) = Tr(A)$.*

Pastaba. *Jei plėtinys $K \subset L$ fiksuotas, rašome tiesiog $N(\alpha)$ ir $Tr(\alpha)$ vietoje $N_{L/K}(\alpha)$ ir $Tr_{L/K}(\alpha)$.*

14.5. Pavyzdys. Paskaičiuosime plėtinio $Q \subset Q\big(\sqrt[3]{2}\big)$ skaičiaus $\alpha = 1 + \sqrt[3]{2} + \sqrt[3]{4}$ normą ir pėdsaką.

Skaičiaus $\sqrt[3]{2}$ minimalusis polinomas yra $\varphi_{\sqrt[3]{2}}(t) = t^3 - 2$, todėl skaičiai 1, $\sqrt[3]{2}$, $\sqrt[3]{4}$ sudaro plėtinio $Q \subset Q\big(\sqrt[3]{2}\big)$ bazę. Užrašome $f_\alpha(1)$, $f_\alpha\big(\sqrt[3]{2}\big)$, $f_\alpha\big(\sqrt[3]{4}\big)$ šios bazės skaičių

tiesinėmis išraiškomis:

$$f_\alpha(1) = \alpha \cdot 1 = \left(1 + \sqrt[3]{2} + \sqrt[3]{4}\right) \cdot 1 = 1 \cdot 1 + 1 \cdot \sqrt[3]{2} + 1 \cdot \sqrt[3]{4};$$

$$f_\alpha\left(\sqrt[3]{2}\right) = \left(1 + \sqrt[3]{2} + \sqrt[3]{4}\right) \cdot \sqrt[3]{2} = 2 \cdot 1 + 1 \cdot \sqrt[3]{2} + 1 \cdot \sqrt[3]{4};$$

$$f_\alpha\left(\sqrt[3]{4}\right) = \alpha \cdot \sqrt[3]{4} = \left(1 + \sqrt[3]{2} + \sqrt[3]{4}\right) \cdot \sqrt[3]{4} = 2 \cdot 1 + 2 \cdot \sqrt[3]{2} + 1 \cdot \sqrt[3]{4}.$$

Vadinasi, šios transformacijos matrica

$$\begin{pmatrix} 1 & 1 & 1 \\ 2 & 1 & 1 \\ 2 & 2 & 1 \end{pmatrix}.$$

Taigi,

$$N(\alpha) = |A| = 1,$$

$$Tr(\alpha) = Tr(A) = 3.$$

14.6. Teorema. *Nagrinėjame n-tojo laipsnio plėtinį $K \subset L$ ir to plėtinio skaičių normas ir pėdsakus. Yra teisingos lygybės:*

1. $N(\alpha\beta) = N(\alpha)\, N(\beta) \quad \forall \alpha, \beta \in L^*$

(t. y. norma – multiplikacinės grupės L^* homomorfizmas į multiplikacinę grupę K^*).

2. $N(a\alpha) = a^n N(\alpha) \quad \forall a \in K^*, \alpha \in L^*.$
3. $N(a) = a^n \quad \forall a \in K^*.$
4. $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta) \quad \forall \alpha, \beta \in L$

(t. y. pėdsakas – adicinės grupės L homomorfizmas į adicinę grupę K).

5. $Tr(a\alpha) = a\, Tr(\alpha) \quad \forall a \in K, \alpha \in L.$
6. $Tr(a) = na \quad \forall a \in K.$

Įrodymas . 1. Pirmiausia įrodysime, kad $f_{\alpha\beta} = f_\alpha \circ f_\beta$ Iš tikrųjų,

$$f_\alpha \circ f_\beta(\gamma) = f_\alpha\big(f_\beta(\gamma)\big) = f_\alpha(\beta\gamma) = \alpha\beta\gamma = f_{\alpha\beta}(\gamma) \quad \gamma \in L.$$

Tarkime, kurioje nors bazėje transformacijos f_α matrica yra A, transformacijos f_β – matrica B. Kadangi $f_{\alpha\beta} = f_\alpha \circ f_\beta$, transformacijos $f_{\alpha\beta}$ matrica C toje pat bazėje yra lygi matricų B ir A sandaugai. Vadinasi,

$$N(\alpha\beta) = |C| = |BA| = |B||A| = N(\alpha)\, N(\beta). \quad \triangle$$

2; 6. Fiksuokime kurią nors plėtinio $K \subset L$ bazę $\alpha_1, \alpha_2, \ldots, \alpha_n$ ir paskaičiuokime vaizdų $f_a(\alpha_i)$ koordinates šioje bazėje:

$$f_a(\alpha_i) = a\alpha_i = 0 \cdot \alpha_1 + 0 \cdot \alpha_2 + \ldots + 0 \cdot \alpha_{i-1} + a \cdot \alpha_i + 0 \cdot \alpha_{i+1} + \ldots + 0 \cdot \alpha_n, \quad (i = \overline{1, n}).$$

Vadinasi, transformacijos f_a matrica A šioje bazėje yra

$$A = \begin{pmatrix} a & 0 & \dots & 0 \\ 0 & a & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a \end{pmatrix}.$$

Iš čia

$$N(a) = |A| = a^n,$$

$$Tr(a) = Tr\, A = na. \quad \triangle$$

3. Ši savybė yra 1-osios ir 2-osios savybių išvada. $\triangle$

4. Įrodysime lygybę $f_{\alpha+\beta} = f_\alpha + f_\beta$. Iš tikrųjų,

$$f_{\alpha+\beta}(\gamma) = (\alpha+\beta)\gamma = \alpha\gamma + \beta\gamma = f_\alpha(\gamma) + f_\beta(\gamma) \qquad \forall \gamma \in L.$$

Vadinasi, transformacijos $f_{\alpha+\beta}$ matrica C yra lygi transformacijų f_α ir f_β matricų A ir B sumai: $C = A + B$. Iš čia

$$Tr(\alpha+\beta) = Tr(C) = Tr(A+B) = Tr(A) + Tr(B) = Tr(\alpha) + Tr(\beta). \quad \triangle$$

5. Tarkime, plėtinio $K \subset L$ bazėje $\alpha_1, \alpha_2, \dots, \alpha_n$ transformacijos f_α matrica

$$A = \big(a_{ij}\big), \quad \big(i = \overline{1,n},\ j = \overline{1,n}\big).$$

Vadinasi,

$$f_\alpha(\alpha_i) = \sum_{j=1}^{n} a_{ij}\alpha_j, \quad i = \overline{1,n}.$$

Paskaičiuokime transformacijos $f_{a\alpha}$ matricą B šioje bazėje:

$$f_{a\alpha}(\alpha_i) = a\alpha\alpha_i = a\sum_{j=i}^{n} a_{ij}\alpha_j =$$

$$= \sum_{j=1}^{n} \big(aa_{ij}\big)\alpha_j, \quad i = \overline{1,n}.$$

Vadinasi, $B = aA$. Iš čia

$$Tr(a\alpha) = Tr(B) = Tr(aA) = \sum_{i=1}^{n} aa_{ii} =$$

$$= a\sum_{i=1}^{n} a_{ii} = a\, TrA = aTr(\alpha). \quad \triangle$$

15. Polinomo skaidinio kūnas

Tarkime, $f(t) \in K[t]$, K – algebrinių skaičių kūnas. Be to, tarkime, $\alpha_1, \alpha_2, \ldots, \alpha_m$ yra visos šio polinomo šaknys. Šių šaknų egzistavimas išplaukia iš pagrindinės algebros teoremos. Prijungę šias šaknis prie algebrinių skaičių kūno K, gausime plėtinį $L = K(\alpha_1, \alpha_2, \ldots, \alpha_m)$, kuriame polinomas $f(t)$ išsiskaido tiesinių daugiklių sandauga:

$$f(t) = a \prod_{i=1}^{m} \big(t - \alpha_i\big).$$

15.1. Apibrėžimas. *Kūną, gautą prijungus prie algebrinių skaičių kūno K polinomo $f(t) \in K[t]$ šaknis, vadiname to polinomo skaidinio kūnu.*

15.2. Teorema. *Polinomo $f(t) \in K[t]$ skaidinio kūnas $K(\alpha_1, \alpha_2, \ldots, \alpha_m)$ yra minimalus kūnas, kuriame šis polinomas išsiskaido tiesinių daugiklių sandauga.*

Pastaba. *Minimalumą suprantame taip: jei $K \subset L$ – plėtinys, kuriame polinomas $f(t)$ išsiskaido tiesinių daugiklių sandauga, tai*

$$K\big(\alpha_1, \alpha_2, \ldots, \alpha_m\big) \subset L.$$

Įrodymas. Tarkime, plėtinyje $K \subset L$ polinomas $f(t)$ išsiskaido tiesinių daugiklių sandauga –

$$f(t) = a \prod_{i=1}^{m} \big(t - \alpha_i\big).$$

Vadinasi, visos šio polinomo šaknys α_i $(i = \overline{1, m})$ priklauso kūnui L. Todėl ir visos tų šaknų sandaugų tiesinės kombinacijos

$$\sum a_{i_1 i_2 \ldots i_s}\, \alpha_{i_1} \alpha_{i_2} \ldots \alpha_{i_s}$$

taip pat priklauso L. Iš čia

$$K(\alpha_1, \alpha_2, \ldots, \alpha_m) \subset L. \quad \triangle$$

Tarkime, α yra plėtinio $K \subset L$ skaičius, $K(\alpha_1, \alpha_2, \ldots, \alpha_m)$ – jo minimaliojo polinomo $\varphi_\alpha(t)$ skaidinio kūnas. Kadangi šio skaičiaus charakteringasis polinomas $f_\alpha(t)$ yra minimaliojo polinomo natūralusis laipsnis, tai kūnas $K(\alpha_1, \alpha_2, \ldots, \alpha_m)$ yra ir charakteringojo polinomo $f_\alpha(t)$ skaidinio kūnas.

15.3. Apibrėžimas. *Charakteringojo polinomo $f_\alpha(t)$ šaknys yra vadinamos jungtinėmis šakniai α.*

15.4. Teorema. *n-tojo laipsnio plėtinio $K \subset L$ skaičiaus α norma $N(\alpha)$ lygi to skaičiaus jungtinių šaknų sandaugai, o pėdsakas $Tr(\alpha)$ – jungtinių šaknų sumai:*

$$N(\alpha) = \prod_{i=1}^{n} \alpha_i, \quad Tr(\alpha) = \sum_{i=1}^{n} \alpha_i$$

(čia $\alpha_1 = \alpha$).

Įrodymas. Užrašome skaičiaus α charakteringąjį polinomą:

$$f_\alpha(t) = |tE - A| = \begin{vmatrix} t - a_{11} & -a_{12} & \dots & -a_{1n} \\ -a_{21} & t - a_{22} & \dots & -a_{2n} \\ \dots & \dots & \dots & \dots \\ -a_{n1} & -a_{n2} & \dots & t - a_{nn} \end{vmatrix} =$$

$$= t^n + t^{n-1} \cdot \left(-\sum_{i=1}^{n} a_{ii} \right) + \ldots + (-1)^n |A| =$$

$$= t^n - t^{n-1} \cdot Tr(A) + \ldots + (-1)^n |A| =$$

$$t^n - t^{n-1} \cdot Tr(\alpha) + \ldots + (-1)^n N(\alpha).$$

Iš Vijeto formulių išplaukia lygybės

$$Tr(\alpha) = \sum_{i=1}^{n} \alpha_i, \quad N(\alpha) = \prod_{i=1}^{n} \alpha_i. \quad \triangle$$

15.5. Apibrėžimas. *Plėtinys $K \subset L$ vadinamas paprastuoju, kai egzistuoja toks kūno L skaičius θ, kad $L = K(\theta)$.*

Skaičius θ, generuojantis plėtinį L, yra vadinamas primityviuoju skaičiumi.

15.6. Teorema. *Baigtinis plėtinys $K \subset L$ gali būti gautas, prijungiant prie kūno K baigtinį skaičių algebrinių skaičių.*

Įrodymas. Tarkime, plėtinio L laipsnis lygus n. Jei $L = K$, tai galima laikyti, kad $L = K(1)$. Tarkime, $L \neq K$. Tuomet egzistuoja plėtinio L skaičius α_1, nepriklausantis kūnui K, ir jo minimaliojo polinomo $\varphi_{\alpha_1}(t)$ laipsnis m_1 didesnis už 1. Kūnas $K(\alpha_1)$ yra tarpinis plėtinio $K \subset L$ kūnas:

$$K \subset K(\alpha_1) \subset L.$$

Iš laipsnių formulės išplaukia, kad

$$[L : K(\alpha_1)] = \frac{n}{m_1} < n.$$

Jei $L = K(\alpha_1)$, teiginys įrodytas.

Tarkime, $L \neq K(\alpha_1)$. Tada analogiškai procesą tęsiame: egzistuoja plėtinio L skaičius α_2, nepriklausantis kūnui $K(\alpha_1)$, ir to skaičiaus minimaliojo polinomo $\varphi_{\alpha_2}(t)$ laipsnis m_2 didesnis už 1. Prijungiame skaičių α_2 prie kūno $K(\alpha_1)$:

$$K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset L.$$

Vėlgi iš laipsnių formulės gauname nelygybę

$$\big[L : K(\alpha_1, \alpha_2)\big] < \frac{n}{m_1}.$$

Jei $L = K(\alpha_1, \alpha_2)$, teiginys įrodytas. Jei $L \neq K(\alpha_1, \alpha_2)$, tęsiame prijungimo procesą. Procesas baigtinis, nes plėtinio $K(\alpha_1, \alpha_2, \ldots, \alpha_s) \subset L$ laipsnis mažėja su kiekvienu naujo skaičiaus prijungimu. Vadinasi, egzistuoja natūralusis skaičius r toks, kad

$$\big[L : K(\alpha_1, \alpha_2, \ldots, \alpha_r)\big] = 1.$$

Iš čia išplaukia lygybė $L = K(\alpha_1, \alpha_2, \ldots, \alpha_r)$. $\triangle$

15.7. Lema. *Baigtinio plėtinio $K \subset L$ skaičiaus α minimaliojo polinomo $\varphi_\alpha(t)$ šaknys skirtingos.*

Įrodymas. Tarkime, $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_m$ yra visos minimaliojo polinomo $\varphi_\alpha(t)$ šaknys ir šaknis α_k – kartotinė. Vadinasi, skaičius α_k yra ir polinomo $\varphi_\alpha(t)$ išvestinės $\varphi'_\alpha(t)$ šaknimi.

Polinomas $\varphi_\alpha(t)$ yra ir skaičiaus α_k minimalusis polinomas, nes jis yra neskaidus. Todėl gauname prieštarą minimaliojo polinomo apibrėžimui, nes

$$\deg \varphi'_\alpha(t) < \deg \varphi_\alpha(t). \quad \triangle$$

15.8. Teorema. *Baigtinis algebrinių skaičių kūno K plėtinys L – paprastasis.*

Įrodymas. Iš teoremos 15.6 įrodymo galima laikyti, kad $L = K(\alpha_1, \alpha_2, \ldots, \alpha_r)$. Jei įrodysime teiginį, kai $r = 2$, tai bendrasis atvejis gaunamas, pritaikius indukciją. Todėl toliau laikysime, kad $L = K(\alpha, \beta)$ ir įrodysime, kad egzistuoja skaičius θ toks, kad $L = K(\theta)$.

Pažymėkime skaičiaus α minimaliojo polinomo $\varphi_\alpha(t)$ šaknis $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_m$, o skaičiaus β minimaliojo polinomo $\varphi_\beta(t)$ šaknis – $\beta_1 = \beta, \beta_2, \ldots, \beta_n$. Iš lemos 15.7 išplaukia, kad visos polinomo $\varphi_\alpha(t)$ ir atitinkamai polinomo $\varphi_\beta(t)$ šaknys yra skirtingos. Su kiekvienu indeksu $i = \overline{1, m}$ ir $j = \overline{2, n}$ sudarome lygtį

$$\alpha + x\beta = \alpha_i + x\beta_j.$$

Ši lygtis turi vienintelį sprendinį, nes $\beta \neq \beta_j$. Kadangi lygčių skaičius yra baigtinis, tai ir šių lygčių sprendinių skaičius yra taip pat baigtinis. Todėl galime pasirinkti kūno K skaičių c tokį, kad jis nėra nė vienos lygties sprendiniu:

$$\alpha + c\beta \neq \alpha_i + c\beta_j, \quad i = \overline{1,m} \;\; j = \overline{2,n}.$$

Pažymėję $\theta = \alpha + c\beta$, įsitikinsime, kad $L = K(\theta)$, t. y. θ yra plėtinio L primityvusis skaičius.

Iš lygybės $\theta = \alpha + c\beta$ išplaukia, kad

$$K(\theta) \subset K(\alpha, \beta).$$

Įrodysime, kad $K(\alpha, \beta) \subset K(\theta)$.

Nagrinėkime polinomą $\varphi_\alpha(\theta - ct)$. Šio polinomo koeficientai priklauso kūnui $K(\theta)$. Ieškosime polinomų $\varphi_\beta(t)$ ir $\varphi_\alpha(\theta - ct)$ bendrųjų šaknų. Skaičius β yra minimaliojo polinomo $\varphi_\beta(t)$ šaknis ir, be to, polinomo $\varphi_\alpha(\theta - ct)$ šaknis:

$$\varphi_\alpha(\theta - c\beta) = \varphi_\alpha(\alpha) = 0.$$

Įrodysime, kad daugiau bendrųjų šaknų šie polinomai neturi. Tarkime priešingai, kad jie turi dar bent vieną bendrąją šaknį. Vadinasi, ši šaknis turi sutapti su kuria nors polinomo $\varphi_\beta(t)$ šaknimi, pavyzdžiui β_j $(j = \overline{2,n})$. Todėl

$$\varphi_\alpha(\theta - c\beta_j) = 0.$$

Todėl skaičius $\theta - c\beta_j$ turi sutapti su kuria nors polinomo $\varphi_\alpha(t)$ šaknimi α_i:

$$\theta - c\beta_j = \alpha_i.$$

Iš čia

$$\theta = \alpha + c\beta = \alpha_i + c\beta_j,$$

o tai yra prieštara skaičiaus c parinkimui. Vadinasi, polinomai $\varphi_\alpha(\theta - ct)$ ir $\varphi_\beta(t)$ teturi vieną bendrą šaknį β ir todėl jų didžiausias bendras daliklis $\big(\varphi_\alpha(\theta - ct), \varphi_\beta(t)\big)$ polinomų žiede $K(\theta)[t]$ yra lygus $t - \beta$. Todėl skaičius β priklauso $K(\theta)$. Bet $\alpha = \theta - c\beta$ ir todėl irgi priklauso $K(\theta)$. Vadinasi, ir skaičių α ir β generuojamas plėtinys $K(\alpha, \beta)$ priklauso kūnui $K(\theta)$: $K(\alpha, \beta) \subset K(\theta)$. Todėl $K(\alpha, \beta) = K(\theta)$. $\triangle$

16. Algebrinių skaičių kūno izomorfizmai

16.1. Apibrėžimas. *Baigtinio plėtinio $K \subset L$ izomorfizmu vadiname kūnų L ir L' izomorfizmą φ su sąlyga*

$$\varphi(a) = a \quad \forall a \in K.$$

Pastaba. *Kai K – racionaliųjų skaičių kūnas, šį izomorfizmą vadinsime algebrinių skaičių kūno L izomorfizmu.*

16.2. Teorema. *n-tojo laipsnio plėtinys $K \subset L$ turi lygiai n izomorfizmų.*

Įrodymas. Tarkime, $L = K(\theta)$, $\deg \varphi_\theta(t) = [L : K] = n$. Pažymėkime primityviojo skaičiaus θ minimaliojo polinomo $\varphi_\theta(t)$ šaknis $\theta_1 = \theta, \theta_2, \ldots, \theta_n$. Su kiekviena šaknimi θ_i $(i = \overline{1,n})$ sudarome plėtinį $K \subset K(\theta_i)$. Šio plėtinio laipsnis $[K(\theta_i) : K] = \deg \varphi_\theta(t) = n$, nes polinomas $\varphi_\theta(t)$ yra bet kurios savo šaknies minimaliuoju polinomu.

Apibrėžiame atvaizdį

$$\sigma_i : K(\theta) \to K(\theta_i) \quad \text{lygybe}$$

$$\sigma_i\Big(\sum_{j=0}^{n-1} a_j\theta^j\Big) = \sum_{j=0}^{n-1} a_j\theta_i^j.$$

Įsitikinsime, kad šis atvaizdis yra plėtinio $L = K(\theta)$ izomorfizmas.

1) σ_i – adicinis homomorfizmas:

$$\sigma_i\Big(\sum_{j=0}^{n-1} a_j\theta^j + \sum_{j=0}^{n-1} b_j\theta^j\Big) = \sigma_i\Big(\sum_{j=0}^{n-1} (a_j + b_j)\theta^j\Big) =$$

$$= \sum_{j=0}^{n-1} (a_j + b_j)\theta_i^j = \sum_{j=0}^{n-1} a_j\theta_i^j + \sum_{j=0}^{n-1} b_j\theta_i^j =$$

$$= \sigma_i\Big(\sum_{j=0}^{n-1} a_j\theta^j\Big) + \sigma_i\Big(\sum_{j=0}^{n-1} b_j\theta^j\Big).$$

2) σ_i – multiplikacinis homomorfizmas:

Pažymėkime žiedo $K[t]$ polinomus

$$f(t) = \sum_{j=0}^{n-1} a_j t^j, \quad g(t) = \sum_{j=0}^{n-1} b_j t^j.$$

Tada

$$f(\theta) = \sum_{j=0}^{n-1} a_j\theta^j, \quad g(\theta) = \sum_{j=0}^{n-1} b_j\theta^j.$$

Padaliname sandaugą $f(t)g(t)$ su liekana iš polinomo $\varphi_\theta(t)$:

$$f(t)g(t) = \varphi_\theta(t)q(t) + r(t), \quad \deg r(t) < n.$$

Įstatę vietoje t pirma θ, po to – θ_i, turime lygybes

$$f(\theta)\, g(\theta) = r(\theta), \quad f(\theta_i)\, g(\theta_i) = r(\theta_i).$$

Vadinasi,

$$\sigma_i\big(f(\theta)\, g(\theta)\big) = \sigma_i\big(r(\theta)\big) = r(\theta_i) =$$

$$= f(\theta_i)\, g(\theta_i) = \sigma_i\big(f(\theta)\big)\, \sigma_i\big(g(\theta)\big).$$

3) σ_i – injekcija:

Tarkime,

$$\sum_{j=0}^{n-1} a_j\theta^j \in \operatorname{Ker}\sigma_i.$$

Tada

$$\sigma_i\Big(\sum_{j=0}^{n-1} a_j\theta^j\Big) = \sum_{j=0}^{n-1} a_j\theta_i^j = 0.$$

Kadangi skaičiai $1, \theta_i, \theta_i^2, \ldots, \theta_i^{n-1}$ sudaro plėtinio $K(\theta_i)$ bazę, iš paskutiniosios lygybės išplaukia, kad $a_j = 0$, kai $j = \overline{0, n-1}$. Vadinasi, $\operatorname{Ker}\sigma_i = \{0\}$.

4) σ_i – surjekcija:

Tarkime,

$$\sum_{j=0}^{n-1} a_j\theta_i^j \in K(\theta_i).$$

Šio skaičiaus pirmvaizdžiu yra skaičius

$$\sum_{j=0}^{n-1} a_j\theta^j.$$

Iš tikrųjų,

$$\sigma_i\Big(\sum_{j=0}^{n-1} a_j\theta^j\Big) = \sum_{j=0}^{n-1} a_j\theta_i^j.$$

Įrodėme, kad atvaizdis σ_i yra kūnų $K(\theta)$ ir $K(\theta_i)$ izomorfizmas. Liko įrodyti, kad

$$\sigma_i(a) = a \quad \forall a \in K.$$

Ši lygybė išplaukia tiesiogiai iš atvaizdžio σ_i apibrėžimo:

$$\sigma_i(a) = \sigma_i\big(a\cdot 1 + 0\cdot\theta + 0\cdot\theta^2 + \ldots + 0\cdot\theta^{n-1}\big) =$$

$$= a\cdot 1 + 0\cdot\theta_i + 0\cdot\theta_i^2 + \ldots + 0\cdot\theta_i^{n-1} = a.$$

Tokiu būdu gavome n skirtingų plėtinio L izomorfizmų, nes visos šaknys θ_i $(i = \overline{1,n})$ yra skirtingos. Įsitikinsime, kad plėtinys L daugiau izomorfizmų neturi. Tuo tikslu tarkime, kad σ yra plėtinio L izomorfizmas kūne L'. Įrodysime, kad σ sutampa su vienu iš izomorfizmų σ_i.

Tarkime,

$$\varphi_\theta(t) = t^n + c_1 t^{n-1} + \ldots + c_{n-1}t + c_n.$$

Įstatę vietoje t skaičių θ, turime lygybę

$$\theta^n + c_1\theta^{n-1} + \ldots + c_{n-1}\theta + c_n = 0.$$

Paveikime abi lygybės puses izomorfizmu σ:

$$\begin{aligned}\sigma(0) = 0 &= \sigma\big(\theta^n + c_1\theta^{n-1} + \ldots + c_{n-1}\theta + c_n\big) = \\ &= \sigma(\theta^n) + \sigma(c_1\theta^{n-1}) + \ldots + \sigma(c_{n-1}\theta) + \sigma(c_n) = \\ &= \big(\sigma(\theta)\big)^n + c_1\big(\sigma(\theta)\big)^{n-1} + \ldots + c_{n-1}\sigma(\theta) + c_n.\end{aligned}$$

Vadinasi, $\sigma(\theta)$ yra minimaliojo polinomo $\varphi_\theta(t)$ šaknis ir todėl turi sutapti su kažkuriuo skaičiumi θ_i: $\sigma(\theta) = \theta_i$. Bet $\theta_i = \sigma_i(\theta)$. Vadinasi,

$$\sigma(\theta) = \sigma_i(\theta).$$

Tarkime,

$$f(\theta) = \sum_{j=0}^{n-1} a_j\theta^j \quad -$$

bet kuris plėtinio L skaičius. Parodysime, kad

$$\sigma_i\big(f(\theta)\big) = \sigma\big(f(\theta)\big).$$

Iš tikrųjų,

$$\sigma\big(f(\theta)\big) = f\big(\sigma(\theta)\big) = f\big(\sigma_i(\theta)\big) = f(\theta_i) = \sigma_i\big(f(\theta)\big). \quad \triangle$$

16.3. Pavyzdžiai. 1. Rasime visus kūno $Q\big(\sqrt[3]{2}\big)$ izomorfizmus. Kadangi

$$\varphi_{\sqrt[3]{2}}(t) = t^3 - 2 = \big(t - \sqrt[3]{2}\big)\big(t - \varepsilon\sqrt[3]{2}\big)\big(t - \varepsilon^2\sqrt[3]{2}\big),$$

kur ε – primityvioji 3-iojo laipsnio vieneto šaknis, kūnas $Q(\sqrt[3]{2})$ turi tris izomorfizmus:

$$\sigma_1 : Q(\sqrt[3]{2}) \to Q(\sqrt[3]{2}), \quad \sigma_1(\sqrt[3]{2}) = \sqrt[3]{2};$$

$$\sigma_2 : Q(\sqrt[3]{2}) \to Q(\varepsilon\sqrt[3]{2}), \quad \sigma_2(\sqrt[3]{2}) = \varepsilon\sqrt[3]{2};$$

$$\sigma_3 : Q(\sqrt[3]{2}) \to Q(\varepsilon^2\sqrt[3]{2}), \quad \sigma_3(\sqrt[3]{2}) = \varepsilon^2\sqrt[3]{2}.$$

2. Rasime visus kūno $Q(\sqrt{2})$ izomorfizmus. Kadangi

$$\varphi_{\sqrt{2}}(t) = t^2 - 2 = (t - \sqrt{2})(t + \sqrt{2}),$$

kūnas $Q(\sqrt{2})$ turi du izomorfizmus:

$$\sigma_1 : Q(\sqrt{2}) \to Q(\sqrt{2}), \quad \sigma_1(\sqrt{2}) = \sqrt{2};$$

$$\sigma_2 : Q(\sqrt{2}) \to Q(-\sqrt{2}), \quad \sigma_2(\sqrt{2}) = -\sqrt{2}.$$

Pastaba. *Aišku, kad* $Q(-\sqrt{2}) = Q(\sqrt{2})$. *Vadinasi,* σ_1 *ir* σ_2 *yra kūno* $Q(\sqrt{2})$ *automorfizmai, paliekantys vietoje racionaliuosius skaičius.*

16.4. Apibrėžimas. *Kūnai, gauti prijungus jungtinius skaičius, vadinami jungtiniais.*

17. Normalieji plėtiniai

Praeito paragrafo pavyzdžiai rodo, kad kūnas $K(\theta)$ gali sutapti su jungtiniu kūnu $K(\theta_i)$, bet gali ir nesutapti. Išskirsime tą atvejį, kai $K(\theta)$ sutampa su visais jam jungtiniais kūnais $K(\theta_i)$.

17.1. Apibrėžimas. *Baigtinis plėtinys* $K \subset L$ *yra vadinamas normaliuoju, kai visi to plėtinio primityviojo skaičiaus* θ *jungtiniai kūnai* $K(\theta_i)$ *sutampa.*

17.2. Teorema. *Polinomo skaidinio kūnas – normalusis plėtinys.*

Įrodymas. Tarkime, K yra algebrinių skaičių kūnas, $\varphi(t) \in K[t]$. Pažymėję šio polinomo šaknis $\alpha_1, \alpha_2, \ldots, \alpha_n$, sudarome jo skaidinio kūną $K(\alpha_1, \alpha_2, \ldots, \alpha_n) = L$. Įrodysime, kad plėtinys $K \subset L$ – normalusis. Pažymėkime šio plėtinio primityvųjį skaičių θ, jo minimaliojo polinomo $\varphi_\theta(t)$ šaknis – $\theta_1 = \theta, \theta_2, \ldots, \theta_m$. Įrodysime, kad $K(\theta) = K(\theta_i)$, $i = \overline{1, m}$.

Kadangi $\theta \in K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, egzistuoja n kintamųjų polinomas su koeficientais iš kūno K $g(t_1, t_2, \ldots, t_n)$ toks, kad $\theta = g(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Sudarome $n + 1$ kintamojo polinomą

$$F(t, t_1, t_2, \ldots, t_n) = \prod_{\sigma \in S_n} \big(t - g_\sigma(t_1, t_2, \ldots, t_n)\big),$$

kur sandauga imama pagal visus simetrinės grupės S_n elementus σ,

$$g_\sigma(t_1, t_2, \ldots, t_n) = g\big(t_{\sigma(1)}, t_{\sigma(2)}, \ldots, t_{\sigma(n)}\big).$$

Įrodysime, kad šis polinomas yra simetrinis kintamųjų $t_1, t_2, \ldots, t_n$ atžvilgiu. Fiksuojame simetrinės grupės S_n elementą τ ir juo paveikiame kintamųjų $t_1, t_2, \ldots, t_n$ indeksus polinome $F\big(t, t_1, t_2, \ldots, t_n\big)$:

$$F\big(t, t_{\tau(1)}, t_{\tau(2)}, \ldots, t_{\tau(n)}\big) = \prod_{\sigma \in S_n} \big(t - g_\sigma\big(t_{\tau(1)}, t_{\tau(2)}, \ldots, t_{\tau(n)}\big).$$

Pertvarkome narį $g_\sigma\big(t_{\tau(1)}, t_{\tau(2)}, \ldots, t_{\tau(n)}\big)$:

$$g_\sigma\big(t_{\tau(1)}, t_{\tau(2)}, \ldots, t_{\tau(n)}\big) = g\big(t_{\sigma\tau(1)}, t_{\sigma\tau(2)}, \ldots, t_{\sigma\tau(n)}\big) =$$

$$= g_{\sigma\tau}\big(t_1, t_2, \ldots, t_n\big).$$

Vadinasi,

$$F\big(t, t_{\tau(1)}, t_{\tau(2)}, \ldots, t_{\tau(n)}\big) = \prod_{\sigma \in S_n} \big(t - g_{\sigma\tau}(t_1, t_2, \ldots, t_n)\big).$$

Kai σ perbėga visus baigtinės grupės S_n elementus, tai $\sigma\tau$ taip pat perbėga visus tos grupės elementus, tik, gal būt, kita tvarka. Todėl

$$F\big(t, t_{\tau(1)}, t_{\tau(2)}, \ldots, t_{\tau(n)}\big) = \prod_{\sigma\tau \in S_n} \big(t - g_{\sigma\tau}(t_1, t_2, \ldots, t_n)\big) =$$

$$= F(t, t_1, t_2, \ldots, t_n).$$

Vadinasi, $F(t, t_1, t_2, \ldots, t_n)$ – simetrinis kintamųjų $t_1, t_2, \ldots, t_n$ polinomas.

Tarkime, id yra vienetinis simetrinės grupės S_n elementas. Tada

$$g_{id}(t_1, t_2, \ldots, t_n) = g\big(t_{id(1)}, t_{id(2)}, \ldots, t_{id(n)} = g(t_1, t_2, \ldots, t_n).$$

Pažymėkime

$$\overline{F(t)} = F\big(t, \alpha_1, \alpha_2, \ldots, \alpha_n\big) = \prod_{\sigma \in S_n} \big(t - g_\sigma(\alpha_1, \alpha_2, \ldots, \alpha_n)\big).$$

Iš pagrindinės simetrinių polinomų teoremos išvados išplaukia, kad polinomo $\overline{F(t)}$ koeficientai priklauso pagrindiniam kūnui K. Be to, skaičius θ yra šio polinomo šaknis. Iš tikrųjų, $\theta = g(\alpha_1, \alpha_2, \ldots, \alpha_n) = g_{id}(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Todėl šis polinomas dalosi iš minimaliojo polinomo $\varphi_\theta(t)$:

$$\overline{F(t)} = \varphi_\theta(t) \cdot q(t), \quad q(t) \in K[t].$$

Įstatę šioje lygybėje vietoje t skaičių θ_i, gauname lygybę

$$\overline{F(\theta_i)} = 0, \quad i = \overline{1, m}.$$

Vadinasi, egzistuoja keitinys $\sigma \in S_n$ toks, kad

$$\theta_i = g_\sigma(\alpha_1, \alpha_2, \ldots, \alpha_n) = g\big(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)}\big).$$

Todėl

$$\theta_i \in K(\alpha_1, \alpha_2, \ldots, \alpha_n) = K(\theta)$$

ir $K(\theta_i) \subset K(\theta)$. Bet $[K(\theta_i) : K] = [K(\theta) : K] = m$, todėl iš laipsnių formulės išplaukia lygybė $[K(\theta) : K(\theta_i)] = 1$. Vadinasi, $K(\theta_i) = K(\theta)$. $\triangle$

18. Baigtiniai Galua plėtiniai

18.1. Apibrėžimas. *Baigtinis normalusis plėtinys $K \subset L$ yra vadinamas baigtiniu Galua plėtiniu.*

Pažymėkime $[L : K] = n$, $L = K(\theta)$, $\theta_1 = \theta, \theta_2, \ldots, \theta_n$ – minimaliojo polinomo $\varphi_\theta(t)$ šaknis. Tada $K(\theta) = K(\theta_i)$, kai $i = \overline{1,n}$, ir izomorfizmas $\sigma_i : K(\theta) \to K(\theta_i)$ yra kūno $K(\theta)$ automorfizmas, paliekantis vietoje kūno K skaičius. Pažymėkime automorfizmų aibę

$$G = GL(L, K) = \big\{\sigma_i \mid i = \overline{1,n}\big\}.$$

Automorfizmų kompozicijos atžvilgiu ši aibė yra multiplikacinė grupė.

18.2. Apibrėžimas. *Galua plėtinio $K \subset L$ automorfizmų grupė $G = GL(L, K)$ yra vadinama šio plėtinio Galua grupe.*

Pastaba. *Iš Galua grupės apibrėžimo išplaukia, kad šios grupės eilė $|G|$ sutampa su plėtinio $K \subset L$ laipsniu $[L : K]$.*

18.3. Lema. *Jei visi Galua plėtinio $K \subset L$ automorfizmai σ palieka vietoje skaičių a, tai šis priklauso pagrindiniam kūnui K.*

Įrodymas. Turime lygybę

$$\sigma(a) = a \quad \forall \sigma \in G.$$

Skaičiaus a jungtiniai skaičiai $\sigma(a)$ sutampa su a, todėl minimalusis polinomas

$$\varphi_a(t) = t - a,$$

nes minimalusis polinomas vienodų šaknų neturi. Bet $t - a \in K[t]$, todėl $a \in K$. $\triangle$

18.4. Pagrindinė Galua teorijos teorema. *Tarp Galua plėtinio $K \subset L$ tarpinių kūnų aibės*

$$A = \{M \mid K \subset M \subset L\}$$

ir to plėtinio Galua grupės pogrupių aibės

$$B = \{H \mid H < G\}$$

egzistuoja bijekcinis ryšys.

Įrodymas. Apibrėžkime atvaizdį $f : A \to B$ lygybe

$$f(M) = \{\sigma \in G \mid \sigma(\alpha) = \alpha \quad \forall \alpha \in M\}, \ M \in A.$$

Įrodysime, kad $f(M)$ yra grupės G pogrupis, t. y. atvaizdis f apibrėžtas korektiškai.

Tarkime, $\sigma, \tau \in f(M)$. Vadinasi,

$$\sigma\tau(\alpha) = \sigma\big(\tau(\alpha)\big) = \sigma(\alpha) = \alpha \quad \forall \alpha \in M.$$

Todėl $\sigma\tau \in f(M)$.

Tarkime $\sigma \in f(M)$. Parodysime, kad $\sigma^{-1} \in f(M)$. Tuo tikslu abi lygybės

$$\sigma(\alpha) = \alpha$$

puses paveikime automorfizmu σ^{-1}:

$$\sigma^{-1}\sigma(\alpha) = \sigma^{-1}(\alpha) = \alpha.$$

Vadinasi, $\sigma^{-1} \in f(M)$ ir tuo pačiu $f(M)$ yra grupės G pogrupis.

Kadangi $K \subset L$ yra normalusis plėtinys, tai ir $M \subset L$ yra normalusis plėtinys ir iš $f(M)$ apibrėžimo išplaukia, kad šis pogrupis yra Galua plėtinio $M \subset L$ Galua grupė: $f(M) = GL(L, M)$.

Įrodysime, kad atvaizdis f yra injekcija. Taikome prieštarą. Tarkime, $M_1 \neq M_2$, o $f(M_1) = f(M_2)$. Parodysime, kad M_1 turi sutapti su M_2.

Tarkime $\alpha \in M_1$. Tada $\sigma(\alpha) = \alpha \quad \forall \sigma \in f(M_1)$. Bet $f(M_1) = f(M_2)$. Vadinasi, $\sigma(\alpha) = \alpha \quad \forall \sigma \in f(M_2)$. Kadangi $f(M_2) = GL(L, M_2)$, iš lemos 18.3 išplaukia, kad $\alpha \in M_2$. Vadinasi $M_1 \subset M_2$.

Analogiškai įrodę, kad $M_2 \subset M_1$, gauname $M_1 = M_2$, o tai prieštara sąlygai.

Vadinasi, atvaizdis f – injekcija.

Įrodysime, kad f yra surjekcija.

Su kiekvienu aibės B elementu H turėtų egzistuoti toks aibės A elementas M, kad $f(M) = H$.

Pažymėkime

$$M = \{\alpha \in L \mid \sigma(\alpha) = \alpha \quad \forall \sigma \in H\}.$$

Įrodysime, kad M yra aibės A elementas, t. y. tarpinis kūnas.

Tarkime, $\alpha, \beta \in M$. Tuomet

$$\sigma(\alpha) = \alpha,\ \sigma(\beta) = \beta \quad \forall \sigma \in H.$$

Vadinasi,

$$\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta) = \alpha + \beta,$$

$$\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = \alpha\beta,$$

t. y. $\alpha + \beta, \alpha\beta \in M$. Todėl M yra kūnas. Be to, $M \subset L$ iš M apibrėžimo ir $K \subset M$, nes

$$\sigma(a) = a \quad \forall a \in G.$$

Įsitikinsime, kad pogrupis H sutampa su $f(M)$.

Tarkime, $\sigma \in H$. Vadinasi, $\sigma(\alpha) = \alpha \quad \forall \alpha \in M$. Bet tokiu atveju $\sigma \in f(M)$. Taigi $H \subset f(M)$.

Parodysime, kad baigtinių pogrupių H ir $f(M)$ eilės $|H|$ ir $|f(M)|$ sutampa. Iš čia išplauks šių pogrupių lygybė.

Tarkime, $L = K(\theta)$. Vadinasi, $L = M(\theta)$.

Pažymėkime plėtinio $M \subset L$ primityviojo skaičiaus θ minimalųjį polinomą $\varphi_\theta^{(M)}(t)$. Sudarykime polinomą

$$\varphi(t) = \prod_{\sigma \in H} \big(t - \sigma(\theta)\big).$$

Šio polinomo koeficientai priklauso kūnui M ir θ yra jo šaknis, nes pogrupio H elementų tarpe yra ir vienetinis. Iš minimaliojo polinomo savybių polinomas $\varphi(t)$ dalosi iš polinomo $\varphi_\theta^{(M)}(t)$. Todėl

$$\deg \varphi(t) \geq \deg \varphi_\theta^{(M)}(t).$$

Bet $\deg \varphi(t) = |H|$, $\deg \varphi_\theta^{(M)}(t) = [L : M] = |f(M)|$. Vadinasi, $|H| \geq |f(M)|$. Bet H yra dalis $f(M)$, todėl $|H| = |f(M)|$. Tuo pačiu $H = f(M)$.

Vadinasi aibių A ir B atvaizdis F yra bijekcija. $\triangle$

Išvada. *Tarkime, tarpinį kūną M atitinka Galua grupės G pogrupis H. Tuomet indeksas $[G : H]$ sutampa su laipsniu $[M : K]$.*

Įrodymas išplaukia iš lygybių

$$|G| = |H|\,[G : H],$$

$$[L : K] = [L : M]\,[M : K],$$

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

$$|H| = [L : M]. \quad \triangle$$

18.5. Pavyzdys. Nagrinėkime plėtinį $Q \subset Q(\varepsilon)$, kur ε – primityvioji 9-ojo laipsnio vieneto šaknis. Rasime visus to plėtinio tarpinius kūnus. Pirmiausia paskaičiuosime skaičiaus ε minimalųjį polinomą. Polinomas $f(t) = t^9 - 1$, kurio šaknimi yra ε, negali būti minimaliuoju, nes jis skaidus:

$$t^9 - 1 = \big(t^3 - 1\big)\big(t^6 + t^3 + 1\big).$$

Įrodysime, kad $\varphi_\varepsilon(t) = t^6+t^3+1$. Pirmiausia $\varphi_\varepsilon(\varepsilon) = 0$, nes $\varepsilon^3 \neq 1$, kadangi ε – primityvioji šaknis. Liko įrodyti, kad $\varphi_\varepsilon(t)$ yra neskaidus polinomas virš racionaliųjų skaičių kūno. Tam pakanka parodyti, kad polinomas $\varphi_\varepsilon(t+1)$ yra neskaidus. Iš tikrųjų,

$$\begin{aligned}\varphi_\varepsilon(t+1) &= (t+1)^6 + (t+1)^3 + 1 = \\ &= t^6 + 6t^5 + 15t^4 + 21t^3 + 18t^2 + 9t + 3,\end{aligned}$$

ir $\varphi_\varepsilon(t+1)$ yra neskaidus pagal Eizenšteino kriterijų.

Taigi $\varphi_\varepsilon(t) = t^6 + t^3 + 1$ ir $[Q(\varepsilon) : Q] = \deg \varphi_\varepsilon(t) = 6$.

Iš primityviosios šaknies savybių išplaukia, kad jai jungtinėmis šaknimis yra skaičiai

$$\varepsilon, \varepsilon^2, \varepsilon^4, \varepsilon^5, \varepsilon^7, \varepsilon^8,$$

t. y. visi skaičiaus ε laipsniai, kurių rodikliai yra mažesni už n ir tarpusavyje pirminiai su 9. Iš čia išplaukia, kad plėtinys $Q \subset Q(\varepsilon)$ yra normalusis ir jo Galua grupė G lygi

$$G = \big\{\sigma_1, \sigma_2, \sigma_4, \sigma_5, \sigma_7, \sigma_8\big\},$$

kur

$$\begin{aligned}\sigma_1(\varepsilon) &= \varepsilon,\\ \sigma_2(\varepsilon) &= \varepsilon^2,\\ \sigma_4(\varepsilon) &= \varepsilon^4,\\ \sigma_5(\varepsilon) &= \varepsilon^5,\\ \sigma_7(\varepsilon) &= \varepsilon^7,\\ \sigma_8(\varepsilon) &= \varepsilon^8.\end{aligned}$$

Rasime visus šios grupės tikrinius pogrupius. Tam pirmiausia paskaičiuosime visų elementų eiles:

1) $|\sigma_1| = 1$, nes $\sigma_1(\varepsilon) = \varepsilon$;

2) $\sigma_2^2(\varepsilon) = \sigma_2\big(\sigma_2(\varepsilon)\big) = \sigma_2(\varepsilon^2) = \big(\sigma_2(\varepsilon)\big)^2 = (\varepsilon^2)^2 = \varepsilon^4$,
$\sigma_2^3(\varepsilon) = \sigma_2\big(\sigma_2^2(\varepsilon)\big) = \sigma_2(\varepsilon^4) = \big(\sigma_2(\varepsilon)\big)^4 = (\varepsilon^2)^4 = \varepsilon^8$.

Vadinasi, $|\sigma_2| \neq 2, 3$, todėl $|\sigma_2| = 6$, nes elemento eilė dalo grupės eilę;

3) $\sigma_4^2(\varepsilon) = \sigma_4\big(\sigma_4(\varepsilon)\big) = \sigma_4(\varepsilon^4) = \big(\sigma_4(\varepsilon)\big)^4 = (\varepsilon^4)^4 = \varepsilon^{16} = \varepsilon^7$,

$$\sigma_4^3(\varepsilon) = \sigma_4\big(\sigma_4^2(\varepsilon)\big) = \sigma_4(\varepsilon^7) = \big(\sigma_4(\varepsilon)\big)^7 = (\varepsilon^4)^7 = \varepsilon^{28} = \varepsilon.$$

Vadinasi, $|\sigma_4| = 3$;

4) $\sigma_5^2(\varepsilon) = \sigma_5\big(\sigma_5(\varepsilon)\big) = \sigma_5(\varepsilon^5) = \big(\sigma_5(\varepsilon)\big)^5 = (\varepsilon^5)^5 = \varepsilon^{25} = \varepsilon^7,$

$\sigma_5^3(\varepsilon) = \sigma_5\big(\sigma_5^2(\varepsilon)\big) = \sigma_5(\varepsilon^7) = \big(\sigma_5(\varepsilon)\big)^7 = (\varepsilon^5)^7 = \varepsilon^{35} = \varepsilon^8.$

Kaip ir antruoju atveju, $|\sigma_5| = 6$;

5) $\sigma_7^2(\varepsilon) = \sigma_7\big(\sigma_7(\varepsilon)\big) = \sigma_7(\varepsilon^7) = \big(\sigma_7(\varepsilon)\big)^7 = (\varepsilon^7)^7 = \varepsilon^{49} = \varepsilon^4,$

$\sigma_7^3(\varepsilon) = \sigma_7\big(\sigma_7^2(\varepsilon)\big) = \sigma_7(\varepsilon^4) = \big(\sigma_7(\varepsilon)\big)^4 = (\varepsilon^7)^4 = \varepsilon^{28} = \varepsilon.$

Vadinasi, $|\sigma_7| = 3$;

6) $\sigma_8^2(\varepsilon) = \sigma_8\big(\sigma_8(\varepsilon)\big) = \sigma_8(\varepsilon^8) = \big(\sigma_8(\varepsilon)\big)^8 = (\varepsilon^8)^8 = \varepsilon^{64} = \varepsilon.$

Vadinasi, $|\sigma_8| = 2$.

Taigi grupė G turi du tikrinius pogrupius:

$$H_1 = \big\{\sigma_1, \sigma_4, \sigma_7\big\} \quad \text{ir} \quad H_2 = \big\{\sigma_1, \sigma_8\big\}.$$

Rasime tuos pogrupius atitinkančius tarpinius kūnus.

1. Tarkime, pogrupį H_1 atitinka kūnas M_1. Vadinasi,

$$M_1 = \big\{\alpha \in Q(\varepsilon) \,|\, \sigma_4(\alpha) = \alpha,\ \sigma_7(\alpha) = \alpha\big\}.$$

Galima laikyti, kad skaičius ε yra plėtinio $M_1 \subset Q(\varepsilon)$ primityvusis skaičius: $M_1(\varepsilon) = Q(\varepsilon)$. Šiam skaičiui jungtiniai yra

$$\sigma_1(\varepsilon) = \varepsilon,\ \sigma_4(\varepsilon) = \varepsilon^4,\ \sigma_7(\varepsilon) = \varepsilon^7.$$

Todėl skaičiaus ε minimalusis polinomas $\varphi_\varepsilon^{(1)}(t)$ virš kūno M_1 yra

$$\varphi_\varepsilon^{(1)}(t) = (t-\varepsilon)(t-\varepsilon^4)(t-\varepsilon^7) =$$

$$= t^3 - t^2\,(\varepsilon + \varepsilon^4 + \varepsilon^7) + t\,(\varepsilon^5 + \varepsilon^8 + \varepsilon^2) - \varepsilon^{12} = t^3 - \varepsilon^3.$$

(Čia pritaikome tapatybes $\varepsilon^9 = 1$, $\varepsilon^6 + \varepsilon^3 + 1 = 0$).

Matome, kad $\varepsilon^3 \in M_1$. Paskaičiuosime skaičiaus ε^3 minimalųjį polinomą $\varphi_{\varepsilon^3}(t)$ virš racionaliųjų skaičių kūno Q. Tuo tikslu rasime visus to skaičiaus jungtinius:

$$\sigma_1\big(\varepsilon^3\big) = \varepsilon^3,\ \sigma_2\big(\varepsilon^3\big) = \varepsilon^6,\ \sigma_5\big(\varepsilon^3\big) = \varepsilon^6,\ \sigma_8\big(\varepsilon^3\big) = \varepsilon^6.$$

Taigi skaičiui ε^3 jungtiniai yra ε^3 ir ε^6. Todėl minimalusis polinomas

$$\varphi_{\varepsilon^3}(t) = (t-\varepsilon^3)(t-\varepsilon^6) = t^2 + t + 1.$$

Šio polinomo šaknys yra $\frac{1}{2}\Big(-1 \pm \sqrt{-3}\Big)$. Todėl

$$M_1 = Q(\varepsilon^3) = Q\Big(\sqrt{-3}\Big).$$

18.6. Apibrėžimas. *Plėtinys, gautas prie racionaliųjų skaičių kūno prijungus neskaidaus kvadratinio polinomo menamąją šaknį, vadinamas menamuoju kvadratinių skaičių kūnu, o realiąją šaknį – realiuoju kvadratinių skaičių kūnu.*

Taigi šiame pavyzdyje tarpinis kūnas $M_1 = Q\Big(\sqrt{-3}\Big)$ yra menamųjų kvadratinių skaičių kūnas.

2. Tarkime, pogrupį H_2 atitinka kūnas M_2. Vadinasi,

$$M_2 = \big\{\alpha \in Q(\varepsilon) \mid \sigma_8(\alpha) = \alpha\big\}.$$

Turime antrojo laipsnio plėtinį $M_2 \subset Q(\varepsilon)$. Vėlgi galime laikyti, kad $Q(\varepsilon) = M_2(\varepsilon)$. Skaičiaus ε jungtiniais yra $\sigma_1(\varepsilon) = \varepsilon$ ir $\sigma_8(\varepsilon) = \varepsilon^8$. Todėl skaičiaus ε minimalusis polinomas $\varphi_\varepsilon^{(2)}(t)$ virš kūno M_2 yra

$$\varphi_\varepsilon^{(2)}(t) = (t-\varepsilon)(t-\varepsilon^8) = t^2 - t(\varepsilon+\varepsilon^8) + 1.$$

Pažymėkime $\theta = \varepsilon + \varepsilon^8$. Šis skaičius priklauso kūnui M_2. Paskaičiuojame jo jungtinius virš racionaliųjų skaičių kūno Q:

$$\sigma_1(\varepsilon+\varepsilon^8) = \varepsilon+\varepsilon^8,\ \ \sigma_2(\varepsilon+\varepsilon^8) = \varepsilon^2+\varepsilon^7,\ \ \sigma_4(\varepsilon+\varepsilon^8) = \varepsilon^4+\varepsilon^5,$$

$$\sigma_5(\varepsilon+\varepsilon^8) = \varepsilon^5+\varepsilon^4,\ \ \sigma_7(\varepsilon+\varepsilon^8) = \varepsilon^7+\varepsilon^2.$$

Vadinasi, skaičiui $\varepsilon+\varepsilon^8$ jungtiniai yra $\varepsilon+\varepsilon^8$, $\varepsilon^2+\varepsilon^7$, $\varepsilon^4+\varepsilon^5$ ir jo minimalusis polinomas $\varphi_\theta(t)$ virš racionaliųjų skaičių kūno Q yra

$$\varphi_\theta(t) = (t-\varepsilon-\varepsilon^8)(t-\varepsilon^2-\varepsilon^7)(t-\varepsilon^4-\varepsilon^5) = t^3 - 3t + 1.$$

Kadangi $\deg\varphi_\theta(t) = 3 = [M_2 : Q]$, skaičius $\theta = \varepsilon+\varepsilon^8$ generuoja kūną M_2 virš racionaliųjų skaičių kūno Q: $Q(\theta) = Q(\varepsilon+\varepsilon^8) = M_2$.

19. Grupės C_n ir M_n

Su kiekvienu natūraliuoju skaičiumi n pažymėkime

$$C_n = \big\{\overline{a} \mid (a,n) = 1\big\}\ -$$

multiplikacinę liekanų klasių grupę moduliu n. Žinoma, kad šios grupės eilė yra $\varphi(n)$ $\big(\varphi(n)$ – Oilerio funkcija$\big)$. Be to, grupė C_n yra Abelio grupė.

Nagrinėkime aibę

$$M = \big\{(a,b) \mid a,b \in Z,\ (a,n) = 1\big\}.$$

Šioje aibėje apibrėžiame ekvivalentumo ryšį: sakome, kad pora (a, b) ekvivalenti porai (c, d) tada ir tik tada, kai

$$a \equiv c \bmod n, \quad b \equiv d \bmod n.$$

Įrodysime, kad šis ryšys iš tikrųjų yra ekvivalentumo ryšys:

1) $(a, b) \sim (a, b)$, nes $a \equiv a \bmod n$, $b \equiv b \bmod n$.

2) Tarkime $(a, b) \sim (c, d)$. Tuomet $a \equiv c \bmod n$, $b \equiv d \bmod n$. Iš čia išplaukia, kad $c \equiv a \bmod n$ ir $d \equiv b \bmod n$. Todėl $(c, d) \sim (a, b)$.

3) Tarkime, $(a, b) \sim (c, d)$ ir $(c, d) \sim (g, h)$. Vadinasi, $a \equiv c \bmod n$, $b \equiv d \bmod n$ ir $c \equiv g \bmod n$, $d \equiv h \bmod n$. Tuomet $a \equiv g \bmod n$, $b \equiv h \bmod n$ ir todėl $(a, b) \sim (g, h)$. $\triangle$

Pažymėkim aibės M faktoraibę pagal apibrėžtą ekvivalentumo sąryšį

$$M_n = \left\{ \overline{(a, b)} \mid (a, n) = 1, \ \ a, b \bmod n \right\}.$$

Iš apibrėžimo išplaukia, kad šios aibės klasių skaičius yra lygus $n\varphi(n)$.

Aibėje M_n apibrėžiame algebrinę operaciją lygybe

$$\overline{(a, b)} \cdot \overline{(c, d)} = \overline{(ac, bc + d)}.$$

Kadangi apibrėžiame operaciją tarp klasių per atstovus, iškyla apibrėžimo korektiškumo klausimas. Tarkime,

$$\overline{(a', b')} = \overline{(a, b)}, \ \ \overline{(c', d')} = \overline{(c, d)} \quad \text{ir}$$

$$\overline{(a', b')} \cdot \overline{(c', d')} = \overline{(a'c', b'c' + d')}.$$

Mes turime įrodyti, kad

$$\overline{(ac, bc + d)} = \overline{(a'c', b'c' + d')}.$$

Kadangi

$$a \equiv a' \bmod \mathrm{n}, \quad \mathrm{b} \equiv \mathrm{b}' \bmod \mathrm{n},$$

$$c \equiv c' \bmod \mathrm{n}, \quad \mathrm{d} \equiv \mathrm{d}' \bmod \mathrm{n},$$

iš lyginių savybių išplaukia, kad

$$ac \equiv a'c' \bmod n,$$

$$bc + d \equiv b'c' + d' \bmod n.$$

Vadinasi, klasės $\overline{(ac, bc + d)}$ ir $\overline{(a'c', b'c' + d')}$ kertasi netuščiai, todėl sutampa.

Šios operacijos atžvilgiu aibė M_n sudaro grupę:

1) operacija asociatyvi –

$$\left(\left(\overline{(a, b)} \cdot \overline{(c, d)} \right) \cdot \overline{(g, h)} \right) = \overline{(ac, bc + d)} \cdot \overline{(g, h)} = \overline{(acg, \ bcg + dg + h)} =$$

$$= \overline{(a, b)} \cdot \overline{(cg, \ dg + h)} = \overline{(a, b)} \cdot \left(\overline{(c, d)} \cdot \overline{(g, h)} \right);$$

2) egzistuoja vienetinis elementas $\overline{(1,0)}$ –

$$\overline{(1,0)} \cdot \overline{(a,b)} = \overline{(a, 0 \cdot a + b)} = \overline{(a,b)};$$

3) klasei $\overline{(a,b)}$ atvirkštinė klasė yra $\overline{(c,-bc)}$, kur $ac \equiv 1 \bmod \mathrm{n}$. Iš tikrųjų, $\overline{(a,b)} \cdot \overline{(c,-bc)} = \overline{(ac, bc-bc)} = \overline{(1,0)}$, nes $ac \equiv 1 \bmod \mathrm{n}$.

Vadinasi, M_n yra multiplikacinė grupė. Ši grupė yra nekomutatyvi: pavyzdžiui,

$$\overline{(1,1)} \cdot \overline{(2,0)} = \overline{(2,2)}, \quad \text{o}$$

$$\overline{(2,0)} \cdot \overline{(1,1)} = \overline{(2,1)}.$$

19.1. Teorema. *Grupė M_n yra išsprendžiama.*

Įrodymas. Apibrėžkime grupės M_n atvaizdį φ grupėje C_n lygybe

$$\varphi\left(\overline{(a,b)}\right) = \overline{a}.$$

Įrodysime, kad atvaizdžio φ apibrėžimas yra korektiškas. Tarkime, $\overline{(a',b')} = \overline{(a,b)}$ ir

$$\varphi\Big(\overline{(a',b')}\Big) = \overline{a}'.$$

Iš klasių lygybės išplaukia, kad $a \equiv a' \bmod \mathrm{n}$, todėl $\overline{a} = \overline{a}'$.

Atvaizdis φ yra surjekcinis homomorfizmas. Iš tikrųjų:

1) $\varphi\Big(\overline{(a,b)} \cdot \overline{(c,d)}\Big) = \varphi\Big(\overline{(ac, bc+d)}\Big) = \overline{ac} = \overline{a} \cdot \overline{c} = \varphi\Big(\overline{(a,b)}\Big)\, \varphi\Big(\overline{(c,d)}\Big)$;

2) klasei $\overline{a} \in C_n$ pirmvaizdžiu yra klasė $\overline{(a,1)}$:

$$\varphi\Big(\overline{(a,1)}\Big) = \overline{a}. \quad \triangle$$

Pritaikę atvaizdžiui φ pagrindinę grupių homomorfizmų teoremą, gauname, kad faktorgrupė $M_n/_{\mathrm{Ker}\,\varphi}$ yra izomorfiška grupei C_n. Vadinasi, faktorgrupė $M_n/_{\mathrm{Ker}\,\varphi}$ yra Abelio grupė.

Paskaičiuosime tiksliau branduolį $\mathrm{Ker}\,\varphi$. Tarkime, $\overline{(a,b)} \in \mathrm{Ker}\,\varphi$. Tuomet $\varphi\Big(\overline{(a,b)}\Big) = \overline{a} = \overline{1}$. Vadinasi,

$$\mathrm{Ker}\,\varphi = \big\{\overline{(1,b)},\ b \bmod \mathrm{n}\big\}.$$

Įrodysime, kad $\mathrm{Ker}\,\varphi$ yra izomorfiška ciklinei grupei Z_n. Grupės $\mathrm{Ker}\,\varphi$ atvaizdį ψ grupėje Z_n apibrėžiame lygybe

$$\psi\Big(\overline{(1,b)}\Big) = \overline{b}.$$

1) ψ – homomorfizmas:

$$\psi\Big(\overline{(1,b)} \cdot \overline{(1,c)}\Big) = \psi\Big(\overline{(1,b+c)}\Big) = \overline{b+c} = \overline{b} + \overline{c} =$$

$$= \psi\Big(\overline{(1,b)}\Big) + \psi\Big(\overline{(1,c)}\Big);$$

2) ψ – injekcija:

Tarkime, $\overline{(1,b)} \in \operatorname{Ker}\psi$. Tuomet

$$\psi\Big(\overline{(1,b)}\Big) = \overline{b} = \overline{0}.$$

Vadinasi, $b \equiv 0 \bmod n$ ir $\overline{(1,b)} = \overline{(1,0)}$. Taigi, $\operatorname{Ker}\psi = \big\{\overline{(1,0)}\big\}$;

3) ψ – surjekcija:

Klasei $\overline{b} \in Z_n$ pirmvaizdžiu yra klasė $\overline{(1,b)}$:

$$\psi\Big(\overline{(1,b)}\Big) = \overline{b}. \quad \triangle$$

Tokiu būdu, grupė $\operatorname{Ker}\varphi$ yra Abelio grupė. Teoremos teiginys dabar išplaukia iš lemos:

19.2. Lema. *Jei G/H ir H yra Abelio grupės, tai faktorgrupė G/H yra išsprendžiama.*

Įrodymas. Kadangi G/H yra Abelio grupė, jos komutantas $\big(G/H\big)' = \{H\}$. Įrodysime, kad grupės G komutantas G' yra H pogrupis. Tarkime, $g_1, g_2 \in G$ ir sudarykime komutatorių $[g_1, g_2]$. Kadangi

$$\begin{aligned} H &= g_1H \cdot g_2H\big(g_1H\big)^{-1}\big(g_2H\big)^{-1} = \\ &= g_1H \cdot g_2H \cdot g_1^{-1}Hg_2^{-1}H = g_1g_2g_1^{-1}g_2^{-1}H, \end{aligned}$$

tai $g_1g_2g_1^{-1}g_2^{-1} = [g_1, g_2] \in H$.

Taigi $G' \subset H$. Bet $\big(G'\big)' \subset H'$ ir $H' = \{e\}$, nes H – Abelio. Vadinasi, grupės G komutantų eilutė nutrūksta jau antrame žingsnyje ir todėl G – išsprendžiama. $\triangle$ $\triangle$

20. Paprastieji radikalieji plėtiniai

20.1. Apibrėžimas. *Tarkime, K yra algebrinių skaičių kūnas ir polinomas $\varphi(t) = t^n - a \in K[t]$. Polinomo $\varphi(t)$ skaidinio kūną vadiname paprastuoju radikaliuoju kūno K plėtiniu.*

Tarkime, $K \subset L$ yra paprastasis radikalusis plėtinys, gautas, prijungus polinomo $\varphi(t) = t^n - a$ šaknis. Jei θ yra šio polinomo šaknis, tai kitos šaknys yra $\theta \cdot \varepsilon^k$, $k = \overline{1, n-1}$, o ε – primityvioji n-tojo laipsnio vieneto šaknis. Iš tikrųjų,

$$\left(\theta \cdot \varepsilon^k\right)^n = \theta^n \cdot \left(\varepsilon^k\right)^n = \theta^n \cdot \left(\varepsilon^n\right)^k = a.$$

Vadinasi kūną L galima gauti, prijungus prie kūno K skaičius θ ir ε: $L = K(\theta, \varepsilon)$. Be to, šis plėtinys yra Galua plėtinys, nes polinomo skaidinio kūnas yra normalusis plėtinys.

20.2. Teorema. *Paprastojo radikaliojo plėtinio $K \subset L$ Galua grupė $G = GL(L, K)$ yra išsprendžiama.*

Įrodymas. Tarkime, σ yra bet kuris grupės G automorfizmas. Paveikę juo abi lygybės $\theta^n = a$ puses, turime, kad $\left(\sigma(\theta)\right)^n = a$. Vadinasi, $\sigma(\theta)$ yra taip pat polinomo $\varphi(t) = t^n - a$ šaknis ir todėl $\sigma(\theta) = \theta \cdot \varepsilon^b$, $b \bmod n$. Paveikę automorfizmu σ abi lygybės $\varepsilon^n = 1$ puses, gauname lygybę $\left(\sigma(\varepsilon)\right)^n = 1$. Vadinasi, $\sigma(\varepsilon)$ yra n-tojo laipsnio vieneto šaknis. Parodysime, kad tai yra primityvioji šaknis. Tarkime, $\sigma(\varepsilon) = \varepsilon^a$ ir d yra skaičių a ir n didžiausias bendras daliklis (a, n). Reikia įrodyti, kad $d = 1$. Pakėlę skaičių ε^a laipsniu $\frac{n}{d}$, turime:

$$\left(\varepsilon^a\right)^{\frac{n}{d}} = \varepsilon^{\frac{na}{d}} = \left(\varepsilon^n\right)^{\frac{a}{d}} = 1.$$

Vadinasi,

$$\left(\sigma(\varepsilon)\right)^{\frac{n}{d}} = \left(\varepsilon^a\right)^{\frac{n}{d}} = 1.$$

Todėl

$$\sigma\left(\varepsilon^{\frac{n}{d}}\right) = 1.$$

Paveikę abi šios lygybės puses automorfizmu σ^{-1}, gauname lygybę

$$\varepsilon^{\frac{n}{d}} = 1.$$

Kadangi ε yra primityvioji n-tojo laipsnio vieneto šaknis, didžiausias bendras daliklis $d = 1$. Taigi, $\sigma(\varepsilon) = \varepsilon^a$ ir $(a, n) = 1$.

Jei $\varepsilon^a = \varepsilon^{a'}$, tai $a \equiv a' \bmod n$ ir

jei $\theta\varepsilon^b = \theta\varepsilon^{b'}$, tai $b \equiv b' \bmod n$.

Todėl galima apibrėžti grupės G atvaizdį φ grupėje M_n lygybe

$$\varphi(\sigma) = \overline{(a, b)},$$

kur a ir b tokie skaičiai, kad $\sigma(\varepsilon) = \varepsilon^a$ ir $\sigma(\theta) = \theta\varepsilon^b$.

Įrodysime, kad atvaizdis φ yra injekcinis homomorfizmas:

1) φ – homomorfizmas:

Tarkime $\tau \in G$ ir $\tau(\varepsilon) = \varepsilon^c$, $\tau(\theta) = \theta\varepsilon^d$. Tuomet

$$\sigma\tau(\varepsilon) = \sigma\big(\tau(\varepsilon)\big) = \sigma\big(\varepsilon^c\big) = \big(\sigma(\varepsilon)\big)^c = \big(\varepsilon^a\big)^c = \varepsilon^{ac} \quad \text{ir}$$

$$\sigma\tau(\theta) = \sigma\big(\tau(\theta)\big) = \sigma\big(\theta\varepsilon^d\big) = \sigma(\theta)\cdot\sigma\big(\varepsilon^d\big) = \sigma(\theta)\cdot\big(\sigma(\varepsilon)\big)^d = \theta\varepsilon^b\cdot\big(\varepsilon^a\big)^d = \theta\cdot\varepsilon^{ad+b}.$$

Vadinasi,

$$\varphi(\sigma\tau) = \overline{(ac, ad+b)} = \overline{(c,d)}\cdot\overline{(a,b)} = \varphi(\tau)\cdot\varphi(\sigma);$$

2) φ – injekcija:

Tarkime, $\sigma \in \operatorname{Ker}\varphi$. Tuomet

$$\varphi(\sigma) = \overline{(a,b)} = \overline{(1,0)}.$$

Todėl $\sigma(\varepsilon) = \varepsilon^1$ ir $\sigma(\theta) = \theta\cdot\varepsilon^0$, t. y. $\sigma(\varepsilon) = \varepsilon$ ir $\sigma(\theta) = \theta$. Tarkime,

$$g(\varepsilon,\theta) = \sum_{i=0}^{k}\sum_{j=0}^{l} a_{ij}\varepsilon^i\theta^j$$

yra bendrasis plėtinio L narys. Paveikę jį automorfizmu σ, gauname lygybę

$$\begin{aligned}\sigma\big(g(\varepsilon,\theta)\big) &= \sigma\Big(\sum_{i=0}^{k}\sum_{j=0}^{l} a_{ij}\varepsilon^i\theta^j\Big) = \\ &= \sum_{i=0}^{k}\sum_{j=0}^{l}\sigma\Big(a_{ij}\varepsilon^i\theta^j\Big) = \sum_{i=0}^{k}\sum_{j=0}^{l}\sigma\big(a_{ij}\big)\,\sigma\big(\varepsilon^i\big)\,\sigma\big(\theta^j\big) = \\ &= \sum_{i=0}^{k}\sum_{j=0}^{l} a_{ij}\big(\sigma(\varepsilon)\big)^i\,\big(\sigma(\theta)\big)^j = \sum_{i=0}^{k}\sum_{j=0}^{l} a_{ij}\varepsilon^i\theta^j = g(\varepsilon,\theta).\end{aligned}$$

Vadinasi, σ yra tapatusis automorfizmas id ir $\operatorname{Ker}\varphi = \{id\}$.

Iš čia išplaukia, kad grupė G yra izomorfiška grupės M_n pogrupiui $\varphi(G)$ ir todėl yra išsprendžiama grupė, nes kiekvienas išsprendžiamos grupės pogrupis yra išsprendžiamas. $\triangle$

21. Cikliniai plėtiniai

21.1. Apibrėžimas. *Baigtinis Galua plėtinys $K \subset L$ yra vadinamas cikliniu, kai jo Galua grupė G yra ciklinė.*

21.2. Teorema. *Tarkime, algebrinių skaičių kūnui K priklauso primityvioji n-tojo laipsnio vieneto šaknis ε, o $K \subset L$ yra ciklinis n-tojo laipsnio plėtinys. Tada šis plėtinys yra paprastasis radikalusis plėtinys ir jį generuojantis polinomas yra $t^n - a$.*

Įrodymas. Pažymėkime plėtinio $K \subset L$ Galua grupę G. Tarkime, grupę G generuoja automorfizmas $\sigma : G =< \sigma >$. Be to, $|G| = [L : K] = n$. Vadinasi,

$$G = \left\{id, \sigma, \sigma^2, \ldots, \sigma^{n-1}\right\}.$$

Tarkime, $\alpha \in L$ ir sudarykime šio skaičiaus Lagranžo rezolventę, atitinkančią skaičių t ($t \in Z$):

$$\left(\varepsilon^t, \alpha\right) = \alpha + \varepsilon^t\sigma(\alpha) + \varepsilon^{2t}\sigma^2(\alpha) + \ldots + \varepsilon^{(n-1)t}\sigma^{n-1}(\alpha).$$

Prijungę prie kūno K skaičių α, gauname tarpinį kūną $K(\alpha)$: $K \subset K(\alpha) \subset L$. Šiam kūnui atitinka grupės G pogrupis H ir $H = GL\left(L, K(\alpha)\right)$. Kadangi G – ciklinė grupė, pogrupis H yra taip pat ciklinis ir yra generuojamas automorfizmo σ^d (čia $dm = n$, $m = |H|$). Kadangi pogrupio H automorfizmai palieka vietoje visus tarpinio kūno $K(\alpha)$ elementus, $\sigma^d(\alpha) = \alpha$. Padalinę natūraliųjį skaičių k iš d su liekana: $k = di + j$, paskaičiuokime $\sigma^k(\alpha)$:

$$\sigma^k(\alpha) = \sigma^{id+j}(\alpha) = \sigma^j\,\sigma^{id}(\alpha) = \sigma^j \cdot \left(\sigma^d\right)^i(\alpha) = \sigma^j(\alpha),$$

nes $\left(\sigma^d\right)^i \in H$.

Pertvarkome Lagranžo rezolventę (ε, α):

$$\begin{aligned}
(\varepsilon, \alpha) &= \alpha + \varepsilon\sigma(\alpha) + \varepsilon^2\sigma^2(\alpha) + \ldots + \varepsilon^d\sigma^d(\alpha) + \varepsilon^{d+1}\sigma^{d+1}(\alpha) + \varepsilon^{d+2}\sigma^{d+2}(\alpha) + \ldots + \\
&+ \varepsilon^{2d}\sigma^{2d}(\alpha) + \ldots + \varepsilon^{di+1}\sigma^{di+1}(\alpha) + \varepsilon^{di+2}\sigma^{di+2}(\alpha) + \ldots + \varepsilon^{d(i+1)}\sigma^{d(i+1)}(\alpha) + \\
&+ \ldots + \varepsilon^{(m-1)d+1}\sigma^{(m-1)d+1}(\alpha) + \varepsilon^{(m-1)d+2}\sigma^{(m-1)d+2}(\alpha) + \ldots + \\
&+ \varepsilon^{(m-1)d+d-1}\sigma^{(m-1)d+d-1}(\alpha) = \alpha + \varepsilon\sigma(\alpha) + \varepsilon^2\sigma^2(\alpha) + \ldots + \varepsilon^{d-1}\sigma^{d-1}(\alpha) + \\
&+ \varepsilon^d\left(\alpha + \varepsilon\sigma(\alpha) + \varepsilon^2\sigma^2(\alpha) + \ldots + \varepsilon^{d-1}\sigma^{d-1}(\alpha)\right) + \ldots + \varepsilon^{(m-1)d}\left(\alpha + \varepsilon\sigma(\alpha) + \right. \\
&\left. + \varepsilon^2\sigma^2(\alpha) + \ldots + \varepsilon^{d-1}\sigma^{d-1}(\alpha)\right) = \left(\alpha + \varepsilon\sigma(\alpha) + \varepsilon^2\sigma^2(\alpha) + \ldots + \right. \\
&\left. + \varepsilon^{d-1}\sigma^{d-1}(\alpha)\right)\left(1 + \varepsilon^d + \varepsilon^{2d} + \ldots + \varepsilon^{(m-1)d}\right) = \\
&= \begin{cases} \left(\alpha + \varepsilon\sigma(\alpha) + \varepsilon^2\sigma^2(\alpha) + \ldots + \varepsilon^{d-1}\sigma^{d-1}(\alpha)\right) \cdot m, & \text{jei } \varepsilon^d = 1; \\ \left(\alpha + \varepsilon\sigma(\alpha) + \varepsilon^2\sigma^2(\alpha) + \ldots + \varepsilon^{d-1}\sigma^{d-1}(\alpha)\right) \cdot \frac{\varepsilon^{md}-1}{\varepsilon^d-1}, & \text{jei } \varepsilon^d \neq 1. \end{cases}
\end{aligned}$$

Bet $\varepsilon^{md} = \varepsilon^n = 1$, vadinasi, jei $\varepsilon^d \neq 1$, Lagranžo rezolventė $(\varepsilon, \alpha) = 0$. Kadangi ε yra primityvioji n-tojo laipsnio vieneto šaknis, tai $\varepsilon^d \neq 1$, kai $d < n$. Vadinasi, jei Lagranžo rezolventė $(\varepsilon, \alpha) \neq 0$, būtinai d sutampa su n. O tai reiškia, kad $H =< \sigma^n >=< id >= \{id\}$, t.y. $|H| = 1 = [L : K(\alpha)]$. Todėl kūnas L turi sutapti su $K(\alpha)$.

Rasime kūne L tokį skaičių α, kad jo Lagranžo rezolventė $(\varepsilon, \alpha) \neq 0$. Tarkime, skaičius θ yra plėtinio $K \subset L$ primityvusis skaičius: $L = K(\theta)$. Pažymėkime skaičiaus θ minimalųjį polinomą $\varphi_\theta(t)$:

$$\varphi_\theta(t) = \prod_{\sigma \in G} \big(t - \sigma(\theta)\big).$$

Įrodysime, kad bent viena iš rezolvenčių $(\varepsilon, \theta), (\varepsilon, \theta^2), \ldots, (\varepsilon, \theta^{n-1})$ yra nelygi nuliui. Tarkime priešingai, visos šios rezolventės lygios nuliui:

$$\theta + \varepsilon\sigma(\theta) + \varepsilon^2\sigma^2(\theta) + \ldots + \varepsilon^{n-1}\sigma^{n-1}(\theta) = 0,$$

$$\theta^2 + \varepsilon\sigma(\theta^2) + \varepsilon^2\sigma^2(\theta^2) + \ldots + \varepsilon^{n-1}\sigma^{n-1}(\theta^2) = 0,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\theta^{n-1} + \varepsilon\sigma\big(\theta^{n-1}\big) + \varepsilon^2\sigma^2\big(\theta^{n-1}\big) + \ldots + \varepsilon^{n-1}\sigma^{n-1}\big(\theta^{n-1}\big) = 0.$$

Prie šių lygybių prirašykime tapatybę

$$1 + \varepsilon + \varepsilon^2 + \ldots + \varepsilon^{n-1} = 0.$$

Vadinasi, $\big(1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}\big)$ yra nenulinis lygčių sistemos

$$\begin{array}{lllll}
x_1 & +x_2 & +\ldots+x_n & = 0, \\
x_1\theta & +x_2\sigma(\theta) & +\ldots+x_n\sigma^{n-1}(\theta) & = 0, \\
\ldots & \ldots & \ldots \quad \ldots & \ldots \\
x_1\theta^{n-1} & +x_2\sigma(\theta^{n-1}) & +\ldots+x_n\sigma^{n-1}(\theta^{n-1}) & = 0
\end{array}$$

sprendinys. Todėl šios sistemos determinantas yra lygus nuliui:

$$\begin{vmatrix}
1 & 1 & 1 & \ldots & 1 \\
\theta & \sigma(\theta) & \sigma^2(\theta) & \ldots & \sigma^{n-1}(\theta) \\
\theta^2 & \sigma(\theta^2) & \sigma^2(\theta^2) & \ldots & \sigma^{n-1}(\theta^2) \\
\ldots & \ldots & \ldots & \ldots & \ldots \\
\theta^{n-1} & \sigma(\theta^{n-1}) & \sigma^2(\theta^{n-1}) & \ldots & \sigma^{n-1}(\theta^{n-1})
\end{vmatrix} = 0.$$

Kadangi $\sigma^k(\theta^l) = \big(\sigma(\theta^l)\big)^k = \Big(\big(\sigma(\theta)\big)^l\Big)^k = \big(\sigma(\theta)\big)^{lk}$, šis determinantas yra Vandermondo determinantas:

$$\begin{vmatrix}
1 & 1 & 1 & \ldots & 1 \\
\theta & \sigma(\theta) & \sigma^2(\theta) & \ldots & \sigma^{n-1}(\theta) \\
\theta^2 & \big(\sigma(\theta)\big)^2 & \big(\sigma^2(\theta)\big)^2 & \ldots & \big(\sigma^{n-1}(\theta)\big)^2 \\
\ldots & \ldots & \ldots & \ldots & \ldots \\
\theta^{n-1} & \big(\sigma(\theta)\big)^{n-1} & \big(\sigma^2(\theta)\big)^{n-1} & \ldots & \big(\sigma^{n-1}(\theta)\big)^{n-1}
\end{vmatrix} = 0.$$

Todėl

$$\prod_{0\le i<j\le n-1}\Big(\sigma^i(\theta)-\sigma^j(\theta)\Big)=0.$$

Vadinasi, bent vienas dauginamasis lygus nuliui:

$$\sigma^k(\theta)-\sigma^l(\theta)=0.$$

Bet ir $\sigma^k(\theta)$, ir $\sigma^l(\theta)$ yra minimaliojo polinomo $\varphi_\theta(t)$ šaknys, o jos yra skirtingos. Vadinasi, gavome prieštarą prielaidai, kad visos rezolventės

$$(\varepsilon,\theta),(\varepsilon,\theta^2),\ldots,(\varepsilon,\theta^{n-1})$$

yra lygios nuliui. Tokiu būdu, plėtinyje L egzistuoja toks skaičius α, kad $(\varepsilon,\alpha)\neq 0$, ir šis skaičius generuoja plėtinį: $L=K(\alpha)$.

Su kiekvienu sveikuoju skaičiumi t nagrinėjame Lagranžo rezolventę

$$(\varepsilon^t,\alpha)=\alpha+\varepsilon^t\sigma(\alpha)+\ldots+\varepsilon^{t(n-1)}\sigma^{n-1}(\alpha).$$

Paveikime abi šios lygybės puses automorfizmu σ:

$$\begin{aligned}\sigma\big((\varepsilon^t,\alpha)\big)&=\sigma(\alpha)+\sigma\big(\varepsilon^t\sigma(\alpha)\big)+\ldots+\sigma\big(\varepsilon^{t(n-1)}\sigma^{n-1}(\alpha)\big)=\\&=\sigma(\alpha)+\varepsilon^t\sigma^2(\alpha)+\ldots+\varepsilon^{t(n-1)}\sigma^n(\alpha)=\\&=\sigma(\alpha)+\varepsilon^t\sigma^2(\alpha)+\ldots+\varepsilon^{t(n-1)}\alpha=\\&=\varepsilon^{-t}\Big(\alpha+\varepsilon^t\sigma(\alpha)+\varepsilon^{2t}\sigma^2(\alpha)+\ldots+\varepsilon^{t(n-1)}\sigma^{n-1}(\alpha)\Big)=\\&=\varepsilon^{-t}\big(\varepsilon^t,\alpha\big).\end{aligned}$$

(Įrodinėjant šią lygybę, naudojamės tuo, kad $\varepsilon\in K$, todėl $\sigma(\varepsilon^k)=\varepsilon^k$, bei tuo, kad $\sigma^n=id$).

Imkime šioje lygybėje $t=1$:

$$\sigma\big((\varepsilon,\alpha)\big)=\varepsilon^{-1}(\varepsilon,\alpha).$$

Pakeliame abi lygybės puses laipsniu t:

$$\Big(\sigma\big((\varepsilon,\alpha)\big)\Big)^t=\varepsilon^{-t}(\varepsilon,\alpha)^t.$$

Vadinasi,

$$\sigma\big((\varepsilon,\alpha)^t\big)=\varepsilon^{-t}(\varepsilon,\alpha)^t,$$

ir

$$\frac{\sigma\big((\varepsilon^t,\alpha)\big)}{\sigma\big((\varepsilon,\alpha)^t\big)}=\frac{(\varepsilon^t,\alpha)}{(\varepsilon,\alpha)^t}.$$

Galutinai gauname lygybę

$$\sigma\left(\frac{(\varepsilon^t,\alpha)}{(\varepsilon,\alpha)^t}\right)=\frac{\big(\varepsilon^t,\alpha\big)}{\big(\varepsilon,\alpha\big)^t}.$$

Pažymėję

$$\frac{\big(\varepsilon^t,\alpha\big)}{\big(\varepsilon,\alpha\big)^t}=a_t,$$

turime, kad $\sigma(a_t)=a_t$. Kadangi automorfizmas σ generuoja visą Galua grupę,

$$\sigma^k(a_t)=a_t,$$

t.y. visi grupės G automorfizmai skaičių a_t palieka vietoje, todėl a_t yra pagrindinio kūno K skaičius: $a_t\in K$.

Iš skaičiaus a_t išraiškos gauname lygybę

$$\big(\varepsilon^t,\alpha\big)=a_t\big(\varepsilon,\alpha\big)^t.$$

Pažymėkime $\big(\varepsilon,\alpha\big)=\beta$. Tada kūnas $K(\beta)$ yra kūno $K(\alpha)$ pokūnis: $K(\beta)\subset K(\alpha)$. Įrodysime, kad ir kūnas $K(\alpha)$ yra $K(\beta)$ pokūnis.

Paskaičiuokime visų rezolvenčių $\big(\varepsilon^t,\alpha\big)$ sumą, kai $t=\overline{0,n-1}$:

$$\begin{aligned}
&(\varepsilon^0,\alpha)+(\varepsilon,\alpha)+(\varepsilon^2,\alpha)+\ldots+(\varepsilon^{n-1},\alpha)=\\
&=\alpha+\sigma(\alpha)+\sigma^2(\alpha)+\ldots+\sigma^{n-1}(\alpha)+\\
&+\alpha+\varepsilon\sigma(\alpha)+\varepsilon^2\sigma^2(\alpha)+\ldots+\varepsilon^{n-1}\sigma^{n-1}(\alpha)+\\
&+\alpha+\varepsilon^2\sigma^2(\alpha)+\varepsilon^4\sigma^2(\alpha)+\ldots+\varepsilon^{2(n-1)}\sigma^{n-1}(\alpha)+\ldots+\\
&+\alpha+\varepsilon^{n-1}\sigma(\alpha)+\varepsilon^{2(n-1)}\sigma^2(\alpha)+\ldots+\varepsilon^{(n-1)(n-1)}\sigma^{n-1}(\alpha)=\\
&=n\alpha+\sigma(\alpha)\big(1+\varepsilon+\varepsilon^2+\ldots+\varepsilon^{n-1}\big)+\sigma^2(\alpha)\big(1+\varepsilon^2+\varepsilon^4+\ldots+\varepsilon^{2(n-1)}\big)+\\
&+\ldots+\sigma^{n-1}(\alpha)\big(1+\varepsilon^{n-1}+\varepsilon^{2(n-1)}+\ldots+\varepsilon^{(n-1)(n-1)}\big).
\end{aligned}$$

Bet

$$1+\varepsilon^k+\varepsilon^{2k}+\ldots+\varepsilon^{(n-1)k}=\frac{\varepsilon^{kn}-1}{\varepsilon^k-1}=0,\quad \text{kai } k=\overline{1,n-1}.$$

Todėl

$$(\varepsilon^0,\alpha)+(\varepsilon,\alpha)+(\varepsilon^2,\alpha)+\ldots+(\varepsilon^{n-1},\alpha)=n\alpha.$$

Visos rezolventės $(\varepsilon^t,\alpha)\in K(\beta)$, todėl $\alpha\in K(\beta)$ ir $K(\alpha)\subset K(\beta)$.

Vadinasi, skaičius β generuoja plėtinį L: $L=K(\beta)$. Paskaičiuosime šio skaičiaus minimalųjį polinomą. Turime lygybę

$$\sigma\big((\varepsilon,\alpha)\big)=\varepsilon^{-1}(\varepsilon,\alpha),$$

t.y.

$$\sigma(\beta) = \varepsilon^{-1}\beta.$$

Paveikime automorfizmu σ skaičių β^n:

$$\sigma(\beta^n) = \big(\sigma(\beta)\big)^n = \big(\varepsilon^{-1}\beta\big)^n = \beta^n.$$

Vadinasi, skaičius β^n yra pagrindinio kūno K skaičius. Pažymėkime $\beta^n = a \in K$. Tuomet skaičius β yra n-tojo laipsnio polinomo $t^n - a$ šaknis. Kadangi β generuoja n-tojo laipsnio plėtinį, šis polinomas yra neskaidus ir todėl yra skaičiaus β minimalusis polinomas:

$$\varphi_\beta(t) = t^n - a.$$

Vadinasi, plėtinys $K \subset L$ yra paprastasis radikalusis plėtinys. $\triangle$

22. Radikalieji plėtiniai

22.1. Apibrėžimas. *Plėtinys $K \subset L$ yra vadinamas radikaliuoju, kai egzistuoja tarpinių kūnų eilutė*

$$K = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_s \subset L,$$

tokia, kad plėtinys $K_i \subset K_{i+1}$ ($i = \overline{0, s-1}$) yra paprastasis radikalusis plėtinys.

Pastaba. *Nors kiekvienas tarpinis plėtinys $K_i \subset K_{i+1}$ yra normalusis, nebūtinai plėtinys $K \subset L$ turi būti normalusis.*

22.2. Lema. *Tarkime, $K \subset M$ ir $M \subset L$ yra normalieji plėtiniai. Plėtinys $K \subset L$ yra normalusis tada ir tik tada, kai egzistuoja polinomas $\varphi(t)$ su koeficientais iš kūno K, kurio skaidinio kūnu virš kūno M būtų kūnas L.*

Įrodymas. Būtinumas. Tarkime, $K \subset L$ yra normalusis plėtinys ir $L = K(\theta)$. Tuomet visos minimaliojo polinomo šaknys $\theta_1 = \theta, \theta_2, \ldots, \theta_n$ priklauso kūnui L ir galime laikyti, kad skaičius θ yra plėtinio $M \subset L$ primityvusis skaičius: $L = M(\theta)$. Vadinasi, polinomo $\varphi_\theta(t) \in K[t]$ skaidinio kūnas virš kūno M ir yra kūnas L. $\triangle$

Pakankamumas. Tarkime, $L = M(\alpha_1, \alpha_2, \ldots, \alpha_m)$ yra polinomo $\varphi(t) \in K[t]$ skaidinio kūnas. Kadangi plėtinys $K \subset M$ yra normalusis, tai to plėtinio primityviojo skaičiaus θ minimaliojo polinomo $\varphi_\theta(t)$ šaknys $\theta_1 = \theta, \theta_2, \ldots, \theta_n \in M$. Todėl galima laikyti, kad $M = K(\theta_1, \theta_2, \ldots, \theta_n)$. Tuomet $L = K(\theta_1, \theta_2, \ldots, \theta_n, \alpha_1, \alpha_2, \ldots, \alpha_m)$. Vadinasi, plėtinys $K \subset L$ yra polinomo $\varphi(t) \cdot \varphi_\theta(t)$ skaidinio kūnas ir todėl yra normalusis. $\triangle$

22.3. Apibrėžimas. *Plėtinys $K \subset L$ yra vadinamas normaliuoju radikaliuoju, kai jis yra kartu ir normalusis, ir radikalusis.*

22.4. Teorema. *Bet kurį radikalųjį plėtinį $K \subset L$ galima įdėti į normalųjį radikalųjį plėtinį $K \subset L \subset \overline{L}$.*

Įrodymas. Tarkime, plėtinio $K \subset L$ radikalioji eilutė yra

$$K = K_0 \subset K_1 \subset \ldots \subset K_i \subset K_{i+1} \subset \ldots \subset K_s = L.$$

Taikysime indukciją pagal s.

1. Kai $s = 1$, L yra paprastasis radikalusis plėtinys, vadinasi, ir normalusis.

2. Darome indukcinę prielaidą visiems radikaliesiems plėtiniams, turintiems radikaliąsias eilutes ilgio $s-1$. Nagrinėjame radikalųjį plėtinį, kurio radikalioji eilutė yra ilgio s. Plėtiniui $K \subset K_{s-1}$ galime taikyti indukcinę prielaidą – egzistuoja kūno K normalusis radikalusis plėtinys $\overline{K}$ toks, kad $K_{s-1} \subset \overline{K}$. Kūnas $L = K_s$ yra kūno K_{s-1} paprastasis radikalusis plėtinys, t. y.

$$L = K_{s-1}(\varepsilon, \theta),$$

kur ε yra n-tojo laipsnio primityvioji vieneto šaknis, o θ – polinomo

$$\varphi(t) = t^n - \beta \quad \big(\beta \in K_{s-1}\big)$$

šaknis. Pažymėkime $\varphi_\beta(t)$ skaičiaus β minimalųjį polinomą virš kūno K. Kadangi plėtinys $K \subset \overline{K}$ yra normalusis ir $\beta \in K_{s-1} \subset \overline{K}$, tai kūnui $\overline{K}$ priklauso visos polinomo $\varphi_\beta(t)$ šaknys $\beta_1 = \beta, \beta_2, \ldots, \beta_m$. Nagrinėkime lygtį

$$t^n - \beta_i = 0 \quad (i = \overline{1, m}).$$

Tarkime, α_i yra šios lygties šaknis (kai $i = 1$, pažymėkime $\alpha_1 = \theta$). Prijunkime prie kūno $\overline{K}$ skaičius $\varepsilon, \alpha_1, \alpha_2, \ldots, \alpha_m$:

$$\overline{L} = \overline{K}\big(\varepsilon, \alpha_1, \alpha_2, \ldots, \alpha_m\big).$$

Kadangi $\alpha_1 = \theta$, kūnas L yra kūno $\overline{L}$ pokūnis. Be to, plėtinys $\overline{L}$ virš kūno $\overline{K}$ turi radikaliąją eilutę

$$\overline{K} = \overline{K}_0 \subset \overline{K}_1 \subset \ldots \subset \overline{K}_m = \overline{L}, \quad \text{kur}$$

$$\overline{K}_i = \overline{K}_{i-1}(\varepsilon, \alpha_i), \;\; i = \overline{1, m}.$$

Pratęsę plėtinio $K \subset \overline{K}$ radikaliąją eilutę šia eilute, gauname plėtinio $K \subset \overline{L}$ radikaliąją eilutę

$$K = K_0 \subset K_1 \subset \ldots \subset K_s \subset \overline{K}_0 \subset \overline{K}_1 \subset \ldots \subset \overline{K}_m = \overline{L}.$$

Įrodysime, kad šis plėtinys yra normalusis.

Pažymėkime $\varphi(t) = \varphi_\beta(t^n) \in K[t]$. Kadangi

$$\varphi(t) = \big(t^n - \beta_1\big)\big(t^n - \beta_2\big)\ldots\big(t^n - \beta_m\big),$$

šio polinomo šaknimis yra skaičiai $\alpha_1, \alpha_2, \ldots, \alpha_m,$. Visos kitos šio polinomo šaknys yra skaičių α_i ir ε sandaugos. Todėl kūnui $\overline{L}$ priklauso visos šio polinomo šaknys. Vadinasi, polinomo $\varphi(t)$ skaidinio kūnas M yra kūno $\overline{L}$ pokūnis. Bet kūnas $\overline{K}$ yra kūno M pokūnis, todėl plėtinys $\overline{L} = \overline{K}\big(\varepsilon, \alpha_1, \alpha_2, \ldots, \alpha_m\big)$ yra taip pat kūno M pokūnis. Vadinasi, $\overline{L} = M$, t. y. kūnas $\overline{L}$ yra polinomo $\varphi(t)$ skaidinio kūnas, todėl $K \subset \overline{L}$ yra normalusis plėtinys. $\triangle$

23. Galua plėtiniai su išsprendžiama Galua grupe

23.1. Teorema. *Normaliojo radikaliojo plėtinio $K \subset L$ Galua grupė $G = GL(L, K)$ yra išsprendžiama.*

Įrodymas. Tarkime,

$$K = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_i \subset K_{i+1} \subset \ldots \subset K_s = L$$

yra plėtinio $K \subset L$ radikalioji eilutė. Šią eilutę atitinka Galua grupės G pogrupių eilutė

$$G = G_0 \supset H_1 \supset H_2 \supset \ldots \supset H_i \supset H_{i+1} \supset \ldots \supset H_s = \{id\}.$$

Įrodymui pritaikysime teiginį iš išsprendžiamų grupių teorijos – *jei grupė turi normaliąją eilutę su išsprendžiamais faktoriais, tai ji pati yra išsprendžiama.*

Pogrupį H_i galima nagrinėti kaip plėtinio $K_i \subset L$ Galua grupę $GL(L, K_i)$ $(i = \overline{0, s-1})$. Nagrinėkime plėtinius

$$K_i \subset K_{i+1} \subset L \quad \big(i = \overline{0, s-1}\big).$$

Kadangi plėtinys $K_i \subset K_{i+1}$ yra paprastasis radikalusis plėtinys, pogrupis H_{i+1} yra grupės H_i normalusis daliklis. Todėl grupės G pogrupių eilutė yra normalioji eilutė su faktoriais

$$H_i\big/_{H_{i+1}} \cong GL\big(K_i, K_{i+1}\big).$$

Bet paprastojo radikaliojo plėtinio $K_i \subset K_{i+1}$ Galua grupė yra išsprendžiama, todėl visi normaliosios eilutės faktoriai yra išsprendžiami. $\triangle$

23.2. Teorema. *Tarkime, $K \subset L$ yra Galua plėtinys, M – tarpinis normalusis kūnas. Be to, $G = GL(L, K)$ ir $G' = GL(M, K)$ yra plėtinių $K \subset L$ ir $K \subset M$ Galua grupės, ir grupės G pogrupis H atitinka tarpinį kūną M. Tuomet pogrupis H yra grupės G normalusis daliklis ir faktorgrupė $G\big/_H$ yra izomorfiška G'.*

Įrodymas. Tarkime, θ yra plėtinio $K \subset M$ primityvusis skaičius – $M = K(\theta)$, $\sigma \in H$, $\tau \in G$. Įrodysime, kad $\tau\sigma\tau^{-1} \in H$, t. y. $H \lhd G$. Pakanka įrodyti, kad

$$\tau\sigma\tau^{-1}(\theta) = \theta.$$

Kadangi $\tau^{-1}(\theta)$ yra minimalioji polinomo $\varphi_\theta(t)$ šaknis, tai $\tau^{-1}(\theta) \in M$. Tuomet $\sigma\big(\tau^{-1}(\theta)\big) = \tau^{-1}(\theta)$. Paveikę šios lygybės abi puses atvaizdžiu τ, turime lygybę

$$\tau\Big(\sigma\big(\tau^{-1}(\theta)\big)\Big) = \tau\big(\tau^{-1}(\theta)\big) = \theta.$$

Vadinasi, $\tau\sigma\tau^{-1}(\theta) = \theta$ ir H yra grupės G normalusis daliklis pagal II-ąjį normaliojo daliklio kriterijų.

Nagrinėkime atvaizdį

$$\varphi : G \to G',$$

apibrėžtą lygybe

$$\varphi(\sigma) = \sigma\,|_M \quad \forall\sigma \in G,$$

(t.y. apribojame automorfizmą σ kūne M). Įrodysime, kad atvaizdis apibrėžtas korektiškai, t.y. $\sigma(M) \subset M$. Tarkime, $\alpha \in M$. Parodysime, kad $\sigma(\alpha) \in M$. Skaičius $\sigma(\theta) \in M$, nes jis yra minimaliojo polinomo $\varphi_\theta(t)$ šaknis, o visos šaknys priklauso M, nes M – normalusis plėtinys. Tarkime, deg $\varphi_\theta(t) = m$. Tuomet

$$\alpha = \sum_{i=0}^{m-1} a_i\,\theta^i, \quad a_i \in K,\ i = \overline{0, m-1}$$

ir

$$\sigma(\alpha) = \sigma\Big(\sum_{i=0}^{m-1} a_i\,\theta^i\Big) = \sum_{i=0}^{m-1} a_i\big(\sigma(\theta)\big)^i \in M.$$

Įrodysime, kad atvaizdis φ yra surjekcinis homomorfizmas.

1) φ – homomorfizmas:

Tarkime, $\sigma, \tau \in G$. Tuomet

$$\varphi(\sigma\tau) = \sigma\tau\,|_M = \sigma\,|_M \cdot \tau\,|_M = \varphi(\sigma) \cdot \varphi(\tau).$$

2) φ – surjekcija:

Tarkime, $\sigma \in G'$. Įrodysime, kad egzistuoja $\tau \in G$ toks, kad

$$\varphi(\tau) = \tau\,|_M = \sigma.$$

Pažymėkime plėtinio $M \subset L$ primityvųjį skaičių $\overline{\theta} : L = M(\overline{\theta})$; jo minimalųjį polinomą – $\varphi_{\overline{\theta}}(t)$, deg $\varphi_{\overline{\theta}}(t) = s$. Tarkime, $\alpha \in L$. Tuomet

$$\alpha = \sum_{i=0}^{s-1} a_i \overline{\theta}^i, \quad a_i \in M, \ i = \overline{0, s-1}.$$

Apibrėžkime atvaizdį

$$\tau : L \to L$$

lygybe

$$\tau(\alpha) = \tau\Big(\sum_{i=0}^{s-1} a_i \overline{\theta}^i\Big) = \sum_{i=0}^{s-1} \sigma(a_i)\big(\tau(\overline{\theta})\big)^i,$$

kur $\tau(\overline{\theta})$ yra kuri nors fiksuota minimaliojo polinomo $\varphi_{\overline{\theta}}(t)$ šaknis. Iš apibrėžimo išplaukia lygybė

$$\tau(\alpha) = \sigma(\alpha), \quad \text{kai } \alpha \in M.$$

Įrodysime, kad τ yra kūno L automorfizmas.

1) τ – adicinis homomorfizmas:

Tarkime, $\beta \in L$ ir

$$\beta = \sum_{i=0}^{s-1} b_i \overline{\theta}^i.$$

Tuomet

$$\tau(\alpha+\beta) = \tau\Big(\sum_{i=0}^{s-1} a_i \overline{\theta}^i + \sum_{i=0}^{s-1} b_i \overline{\theta}^i\Big) =$$

$$= \tau\Big(\sum_{i=0}^{s-1} \big(a_i + b_1\big)\overline{\theta}^i\Big) = \sum_{i=0}^{s-1} \sigma\big(a_1 + b_1\big)\big(\tau(\overline{\theta})\big)^i =$$

$$= \sum_{i=0}^{s-1} \sigma(a_i)\big(\tau(\overline{\theta})\big)^i + \sum_{i=0}^{s-1} \sigma(b_i)\big(\tau(\overline{\theta})\big)^i = \tau(\alpha) + \tau(\beta).$$

2) τ – multiplikacinis homomorfizmas:

$$\tau(\alpha\beta) = \tau\Big(\sum_{i=0}^{s-1} a_i \overline{\theta}^i \cdot \sum_{j=0}^{s-1} b_j \overline{\theta}^j\Big) = \tau\Big(\sum_{i=0}^{s-1}\sum_{j=0}^{s-1} a_i b_j \overline{\theta}^{i+j}\Big) =$$

$$= \sum_{i=0}^{s-1}\sum_{j=0}^{s-1} \sigma(a_i b_j)\big(\tau(\overline{\theta})\big)^{i+j} = \sum_{i=0}^{s-1}\sum_{j=0}^{s-1} \sigma(a_i)\,\sigma(b_j)\cdot\big(\tau(\overline{\theta})\big)^i \cdot \big(\tau(\overline{\theta})\big)^j =$$

$$= \sum_{i=0}^{s-1} \sigma(a_i)\big(\tau(\overline{\theta})\big)^i \cdot \sum_{j=0}^{s-1} \sigma(b_j)\big(\tau(\overline{\theta})\big)^j = \tau(\alpha)\cdot\tau(\beta).$$

3) τ – injekcija:

Tarkime, $\alpha \in \operatorname{Ker}\tau$. Tuomet

$$\tau(\alpha) = \tau\Big(\sum_{i=0}^{s-1} a_i\overline{\theta}^i\Big) = \sum_{i=0}^{s-1}\sigma(a_i)\big(\tau(\overline{\theta})\big)^i = 0.$$

Skaičiai $1, \tau(\overline{\theta}), \big(\tau(\overline{\theta})\big)^2, \ldots, \big(\tau(\overline{\theta})\big)^{s-1}$ sudaro plėtinio $M \subset L$ bazę, todėl

$$\sigma(a_i) = 0, \quad i = \overline{0, s-1}.$$

Bet σ – automorfizmas, todėl

$$a_i = 0, \quad i = \overline{0, s-1}.$$

Vadinasi, $\alpha = 0$ ir $\operatorname{Ker}\tau = \{0\}$. Todėl atvaizdis τ – injekcija.

4) τ – surjekcija:

Tarkime, $\alpha \in L$ ir

$$\alpha = \sum_{i=0}^{s-1} a_i\overline{\theta}^i.$$

Pažymėkime minimaliojo polinomo $\varphi_{\tau(\overline{\theta})}(t) = \varphi_{\overline{\theta}}(t)$ šaknį $\overline{\theta} = \tau^{-1}\big(\tau(\overline{\theta})\big)$. Tuomet skaičiaus α pirmvaizdžiu yra skaičius

$$\beta = \sum_{i=0}^{s-1} a_i\big(\tau^{-1}(\overline{\theta})\big)^i.$$

Iš tikrųjų

$$\tau(\beta) = \tau\Big(\sum_{i=0}^{s-1} a_i\big(\tau^{-1}(\overline{\theta})\big)^i\Big) =$$

$$= \sum_{i=0}^{s-1}\sigma(a_i)\Big(\tau\big(\tau^{-1}(\overline{\theta})\big)\Big)^i = \sum_{i=0}^{s-1}\sigma(a_i)\overline{\theta}^i = \alpha.$$

Vadinasi, atvaizdis τ yra surjekcija ir tuo pačiu kūno L automorfizmas, todėl $\tau \in G$. Be to,

$$\varphi(\tau) = \tau\,|_M = \sigma.$$

Todėl φ – surjekcinis homomorfizmas. Įrodysime, kad jo branduolys $\operatorname{Ker}\varphi$ sutampa su pogrupiu H.

Tarkime, $\sigma \in \operatorname{Ker}\varphi$. Tuomet

$$\varphi(\sigma) = \sigma\,|_M = id.$$

Todėl $\sigma(\alpha) = \alpha \quad \forall\alpha \in M$. Vadinasi, $\sigma \in H$ ir $\operatorname{Ker}\varphi \subset H$.

Tarkime, $\sigma \in H$. Vadinasi,

$$\sigma(\alpha) = \alpha \quad \forall \alpha \in M.$$

Todėl $\sigma\,|_M = id$ ir $\sigma \in \operatorname{Ker}\varphi$. Tuo pačiu $H \subset \operatorname{Ker}\varphi$ ir $H = \operatorname{Ker}\varphi$.

Dabar teoremos įrodymas išplaukia iš pagrindinės grupių homomorfizmų teoremos:

$$G/_{\operatorname{Ker}\varphi} = G/_H \cong G'. \quad \triangle$$

23.3. Teorema. *Normaliojo radikaliojo plėtinio normaliojo pokūnio Galua grupė yra išsprendžiama.*

Įrodymas. Tarkime, $K \subset L$ yra normalusis radikalusis plėtinys, $G = GL(L, K)$ – šio plėtinio Galua grupė, M – tarpinis normalusis kūnas, $G' = GL(M, K)$ – šio kūno Galua grupė. Iš praeitos teoremos išplaukia, kad grupė G' yra izomorfiška faktorgrupei $G/_H$ (čia H – tarpinį kūną M atitinkantis Galua grupės G pogrupis). Kadangi grupė G yra išsprendžiama, tai ir jos faktorgrupė $G/_H$, o tuo pačiu ir grupė G', yra išsprendžiama. $\triangle$

23.4. Teorema. *Bet kuris normalusis plėtinys su išsprendžiama Galua grupe yra normaliojo radikaliojo plėtinio pokūnis.*

Įrodymas. Skirsime du atvejus.

1. Tarkime, $K \subset M$ yra normalusis m-tojo laipsnio plėtinys su cikline Galua grupe $G =< \sigma >$. Pažymėkime $M = K(\theta)$, $L = M(\varepsilon)$ (ε – m-tojo laipsnio primityvioji vieneto šaknis). Tuomet $L = K(\theta, \varepsilon) = K(\theta + c\varepsilon)$, kur c – fiksuotas kūno K skaičius. Visos skaičiaus $\theta + c\varepsilon$ jungtinės šaknys turi pavidalą $\sigma^i(\theta) + c\varepsilon^j$, vadinasi, priklauso L. Todėl $K \subset L$ yra normalusis plėtinys. Plėtinio $K(\varepsilon) \subset K(\theta, \varepsilon)$ Galua grupė yra izomorfiška plėtinio $K \subset K(\theta)$ Galua grupės pogrupiui ir todėl yra ciklinė. Be to, šios grupės eilė $n = \big[K(\theta, \varepsilon) : K(\varepsilon)\big]$ dalo skaičių m, todėl n-tojo laipsnio primityvioji vieneto šaknis η yra skaičiaus ε laipsnis, vadinasi, priklauso $K(\varepsilon)$. Taigi kūnas $K(\varepsilon, \theta)$ yra kūno $K(\varepsilon)$ n-tojo laipsnio ciklinis plėtinys, kuriam priklauso to paties laipsnio primityvioji vieneto šaknis, ir todėl yra paprastasis radikalusis kūno K plėtinys. $\triangle$

2. Tarkime, $K \subset L$ yra normalusis plėtinys su išsprendžiama Galua grupe G. Sudarykime šios grupės normaliąją eilutę su Abelio faktoriais

$$G = H_0 \supset H_1 \supset \ldots \supset H_i \supset H_{i+1} \supset \ldots \supset H_s = \{id\}. \tag{1}$$

Taikysime indukciją pagal eilutės ilgį s.

1) Kai $s = 1$, įrodyta pirmojoje dalyje, nes šiuo atveju grupė G yra ciklinė.

2) Darome indukcinę prielaidą visiems normaliesiems plėtiniams, kurių Galua grupės turi normaliąsias eilutes su Abelio faktoriais ilgio $s-1$. Įrodysime teiginį, kai eilutės ilgis lygus s.

Tarkime, plėtinyje $K \subset L$ pogrupį H_1 atitinka tarpinis kūnas M. Plėtinys $K \subset M$ yra normalusis ir jo Galua grupė $GL(M,K)$ izomorfiška faktorgrupei $G/_{H_1}$, todėl yra ciklinė grupė. Vadinasi, kūnas M priklauso kūno K normaliajam radikaliajam plėtiniui $\overline{M}$. Tarkime $\overline{M} = K(\alpha)$, $L = K(\theta)$. Pažymėkime $N = K(\alpha,\theta)$. Kadangi plėtinio $\overline{M} \subset N$ Galua grupė $GL(N,\overline{M})$ izomorfiška plėtinio $M \subset L$ Galua grupės $GL(L,M) = H_1$ pogrupiui. Bet grupė H_1, o tuo pačiu ir kiekvienas jos pogrupis, turi normaliąją eilutę su Abelio faktoriais ilgio $s-1$. Todėl pagal indukcinę prielaidą kūną N, o tuo pačiu ir kūną M, galima įdėti į plėtinio $L \subset \overline{M}$ normalųjį radikalųjį plėtinį. Tuo pačiu plėtinys $K \subset L$ bus taip pat radikaliuoju plėtiniu. Žinome, kad kiekvienas radikalusis plėtinys, o tuo pačiu ir plėtinys $K \subset L$, yra įdedamas į normalųjį radikalųjį plėtinį. $\triangle$

24. Lygtys, išsprendžiamos radikalais

24.1. Apibrėžimas. *Sakome, kad polinomo $\varphi(t)$ su koeficientais iš algebrinių skaičių kūno K šaknis θ yra išreiškiama radikalais, kai egzistuoja kūno K radikalusis plėtinys L, kuriam priklauso θ.*

24.2. Teorema. *Jei neskaidaus polinomo $\varphi(t)$ bent viena šaknis išreiškiama radikalais, tai ir likusios šaknys taip pat išreiškiamos radikalais.*

Įrodymas. Tarkime, polinomo $\varphi(t)$ šaknis θ priklauso kūno K radikaliajam plėtiniui L. Radikalųjį plėtinį $K \subset L$ galime praplėsti iki normaliojo radikaliojo plėtinio $K \subset \overline{L}$. Kadangi $\theta \in \overline{L}$, tai ir visos likusios polinomo $\varphi(t)$ šaknys taip pat priklauso $\overline{L}$. Tuo pačiu visos šio polinomo šaknys išreiškiamos radikalais. $\triangle$

24.3. Teorema (Polinomo šaknų išreiškimo radikalais kriterijus). *Neskaidaus polinomo $\varphi(t) \in K[t]$ šaknys išreiškiamos radikalais tada ir tik tada, kai to polinomo skaidinio kūno Galua grupė yra išsprendžiama.*

Įrodymas. Būtinumas. Tarkime, polinomo $\varphi(t)$ šaknys išreiškiamos radikalais. Tada egzistuoja normalusis radikalusis plėtinys L, kuriam priklauso visos šaknys. Todėl polinomo $\varphi(t)$ skaidinio kūnas M yra plėtinio $K \subset L$ normalusis pokūnis. Būtinumo įrodymą gauname, šiam pokūniui pritaikę 23.3 teoremą. $\triangle$

Pakankamumas. Tarkime, polinomo $\varphi(t)$ skaidinio kūnas M yra su išsprendžiama Galua grupe. Iš 23.4 teoremos išplaukia, kad šis kūnas yra normaliojo radikaliojo plėtinio $K \subset L$ pokūnis. Todėl ir visos šio polinomo šaknys priklauso plėtiniui $K \subset L$. $\triangle$

Pastaba. *Egzistuoja polinomai su racionaliaisiais koeficientais, kurių skaidinių kūnų Galua grupės yra simetrinės grupės. Todėl jau penktojo laipsnio polinomų šaknys bendruoju atveju gali būti neišreiškiamos radikalais, pavyzdžiui,*

$$\varphi(t) = t^5 + pt + p,$$

kai p – bet kuris pirminis skaičius.

Tikimybių teorijos ir skaičių teorijos katedra
Kompiuterinis rinkimas ir maketavimas: *Vita Verikaitė*