5 paskaita. *Dalumas su liekana. BDD. Tarpusavyje pirminiai polinomai. Neredukuojami polinomai. Skirtingo laipsnio polinomų išskyrimas.*

Panašiai kaip ir sveikųjų skaičių žiede, taip ir polinomų virš kūno žiede yra teisinga dalumo su liekana teorema.

Teorema(dalumas su liekana). *Tegu* $f(x)$, $g(x) \in K[x], g(x) \neq 0$. *Tada egzistuoja vienintėliai polinomai* $q(x)$ *ir* $r(x)$ *su kuriais teisinga lygybė* $f = gq+r$, *čia* $\deg r(x) < \deg g(x)$.

Įrodymas. *Egzistavimas.* Matematinė indukcija pagal $n = \deg f(x)$.

1. Indukcijos bazė: $n = 0$, t.y. $f(x) = a \in K$. Galimi du atvejai:

(i) $\deg g(x) = 0$, t.y. $g(x) = b \neq 0$. Tada $f = g \cdot \frac{a}{b} + 0$ ir $-\infty = \deg 0 < \deg g = 0$.

(ii) $\deg g(x) > 0$. Tada $f = g \cdot 0 + f$ ir $0 = \deg f < \deg g$.

2. Indukcijos prielaida. Tegu teiginys yra teisingas visiems polinomams, kurių laipsnis $< n$.

3. Indukcijos teiginį įrodysime n - ojo laipsnio polinomui $f(x)$. Tegu polinomo f vyriausias koeficientas yra a_n, o polinomo g laipsnis yra m, o vyriausias koeficientas b_m. galimi du atvejai:

(i) $n < m$. Tada $f(x) = g(x) \cdot 0 + f(x)$ ir $n = \deg f(x) < \deg g(x) = m$.

(ii) $n \geq m$. Tada polinomo $f_1(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$ laipsnis yra $< n$ ir pagal indukcijos prielaidą turime, kad egzistuoja tokie polinomai $q_1(x)$ ir $r(x)$ iš $K[x]$, kad $f_1(x) = g(x) \cdot q(x) + r(x)$, $\deg r(x) < \deg g(x)$. Tada

$$f(x) = g(x) \cdot \left(\frac{a_n}{b_m} x^{n-m} + q_1(x) \right) g(x) + r(x), \deg r(x) < \deg g(x).$$

Vienatinumas. Tegu $f(x) = g(x) \cdot p(x) + s(x)$, $\deg s(x) < \deg g(x)$. Tada

$$\begin{gathered} 0 = g(x) \cdot (q(x) - p(x)) + (r(x) - s(x)) \\ g(x) \cdot (q(x) - p(x)) = (s(x) - r(x)) \end{gathered}$$

ir

$$\deg g(x) + \deg (q(x) - p(x)) = \deg (s(x) - r(x)).$$

Tai įmanoma tik tuo atveju, kai $q(x) - p(x) = s(x) - r(x) = 0$.
Įrodyta.

Apibrėžimas. *Tegu* $f(x)$, $g(x) \in K[x], g(x) \neq 0$. *Didžiausio laipsnio polinomas* $d(x) \in K[x]$, *kurio vyriausias koeficientas yra lygus* 1, *vadinamas polinomų* f *ir* g ***bendru didžiausiu dalikliu****, jeigu*

1. $f \vdots d, g \vdots d$.

2. Jeigu $f \vdots d_1, g \vdots d_1$, *čia* $d_1(x) \in K[x]$, *tai* $d \vdots d_1$.
Bendro didžiausio daliklio žymuo: $d(x) = \mathrm{BDD}(f(x), g(x)) = (f(x), g(x))$.

Teorema. *Su visais* $f, g \in K[x], f \neq 0, g \neq 0$ *egzistuoja tokie polinomai* $a_0(x), b_0(x) \in K[x]$, *kad* $(f(x), g(x)) = f(x) a_0(x) + g(x) b_0(x)$.

Įrodymas paliekamas skaitytojui.

Euklido algoritmas BDD skaičiavimui. Turime du polinomus $f(x), g(x) \in K[x], g \neq 0$.Rašysime dalybos su liekana teoremą
Tegu $a_0 = f$ ir $a_1 = g$. Tada

$$\begin{array}{cc}
a_0 = a_1 q_1 + a_2 & \deg a_2 < \deg a_1 \\
a_1 = a_2 q_2 + a_3 & \deg a_3 < \deg a_2 \\
\cdots & \cdots \\
a_{k-2} = a_{k-1} q_{k-1} + a_k & \deg a_k < \deg a_{k-1} \\
a_{k-1} = a_k q_k. &
\end{array}$$

Sveikieji skaičiai sudaro mažėjančią seką $\deg a_1 > \deg a_2 > \deg a_3 > \cdots > \deg a_k > \deg a_{k+1} > 0$. Tada $(a, b) = a_k$.

Apibrėžimas. *Du polinomai* $f, g \in K[x]$ *vadinami tarpusavyje pirminiais, jeigu* $(f, g) = 1$.

Teorema. *Polinomai* $f, g \in K[x]$ *yra tarpusavyje pirminiai tada ir tik tada, kada egzistuoja tokie* $a(x), b(x) \in K[x]$, *kad* $f \cdot a + g \cdot b = 1$.

Įrodymas. Teiginys iš kairės į dešinę yra teisingas pagal apibrėžimą. Tegu dabar $f \cdot a + g \cdot b = 1$ ir $(f, g) = d$. Tada

$$1 = \underbrace{\underbrace{f \cdot a}_{\text{dalijasi iš } d} + \underbrace{g \cdot b}_{\text{dalijasi iš } d}}_{\text{dalijasi iš } d},$$

t,y. 1 dalijasi iš d ir todėl $d = 1$.
Įrodyta.

Teiginys(tarpusavyje pirminių polinomų savybė). *Tegu* $f_1, ..., f_m$ *ir* $g_1, ..., g_n$ *yra dvi tokios polinomų sekos, kad* $(f_i, g_j) = 1$ *su visais* $1 \leq i \leq m, 1 \leq j \leq n$. *Tada* $(f_1 \cdots f_m, g_1 \cdots g_n) = 1$.
Be įrodymo.

Dabar pateiksime teiginį, kurio analogo sveikųjų skaičių žiede nėra.

Teiginys. *Jeigu* f *ir* g *yra tarpusavyje pirminiai polinomai virš kūno* K, *tai jie neturi bendrų šaknų jokiame kūno* K *plėtinyje, t.y. tokiame kūne* L, *kad* $L \supseteq K$.

Įrodymas.[..........]

Apibrėžimas. *Teigiamo laipsnio polinomas* $f(x) \in K[x]$ *vadinamas neredukuojamu polinomu virš kūno* K, *jeigu jis turi tik šiuos daliklius:* $a, a \cdot f(x)$, *čia* $a \in K$.

Teiginys. *Bet kuris teigiamo laipsnio polinomas iš* $K[x]$ *dalijasi iš kurio nors neredukuojamo polinomo virš* K.

Teorema. *Yra be galo daug neredukuojamų polinomų virš bet kurio kūno.*

Įrodymas. Įrodysime prieštaros būdu. Sakykime, egzistuoja baigtinis neredukuojamų polinomų kiekis: $p_1, p_2, ..., p_m$. Polinomas $f = p_1 p_2 \cdots p_m + 1$ dalijasi iš neredukuojamo polinomo, taigi egzistuoja toks $i, 1 \leq i \leq m$, kad $f \vdots p_i$. Tada

$$1 = \underbrace{\underbrace{f}_{\text{dalijasi iš } p_i} - \underbrace{p_1 p_2 \cdots p_m}_{\text{dalijasi iš } p_i}}_{\text{dalijasi iš } p_i},$$

t.y. $1 \vdots p_i$, o tai prieštarauja neredukuojamo polinomo apibrėžimui(deg $p_i > 0$).
Įrodyta.

Teiginys(neredukuojamų polinomų savybė). *Tegu $f_1, ..., f_m$ yra tokia polinomų iš $K[x]$ seka, kad polinomas $f_1 \cdots f_m$ dalijasi iš neredukuojamo polinomo $p(x) \in K[x]$. Tada egzistuoja toks $j, 1 \leq j \leq m$, kad f_j dalijasi iš p.*
Be įrodymo.

Pateiksime teiginį, kurio analogo sveikųjų skaičių žiede nėra.

Teiginys. *Jeigu neredukuojamas virš kūno K polinomas $p(x) \in K[x]$ ir polinomas $f(x) \in K[x]$ turi bendrą šaknį x_0 kuriame nors kūno K plėtinyje $L \supset K, x_0 \in L$, tai $f(x) \vdots p(x)$.*

Įrodymas. Iš sąlygos matome, kad $(f(x), p(x)) \neq 1$, nes ir $f(x)$, ir $p(x)$ dalijasi iš $(x - x_0)$. Polinomas $p(x)$ yra neredukuojamas, todėl $f(x) \vdots p(x)$.
Įrodyta.

Teorema(kanoninis polinomo skaidinys). *Su kiekvienu teigiamo laipsnio polinomu $f(x) \in K[x]$ egzistuoja tokie neredukuojami virš kūno k polinomia $p_1, p_2, ..., p_s$ (tarp jų gali būti sutampančių), kad $f = a \cdot p_1 \cdot p_2 \cdot \dots \cdot p_s$, čia $a-$ polinomo f koeficientas prie x^n, kai $n = \deg f$. (Šiame skaidinyje sutraukę panašius daugiklius turėsime kanoninį polinomo f skaidinį: $f = a \cdot p_{i_1}^{k_1} \cdot p_{i_2}^{k_2} \cdots p_{i_s}^{k_s}, p_i \neq p_j$.)*

Be įrodymo.

Grįžkime prie neredukuojamų polinomų virš realiųjų skaičių kūno $\mathbf{R}$ ir virš kompleksinių skaičių kūno $\mathbf{C}$. Fundamentalioji algebros teorema teigia:

Fundamentalioji algebros teorema. *Bet kokia algebrinė lygtis $a_n x^n + \cdots + a_1 x + a_0 = 0$, $n \geq 1$ su kompleksiniais koeficientais $a_i \in \mathbf{C}$ $(0 \leq i \leq n)$ turi mažiausiai vieną sprendinį $x_0 \in \mathbf{C}$.*
Be įrodymo.

Matome, kad $n-$ ojo laipsnio polinomas virš kopleksinių skaičių kūno $\mathbf{C}$ turi lygiai n šaknų. Tokiu atveju sakome, kad $\mathbf{C}$ yra **algebriškai uždaras kūnas**.

Akivaizdu, kad neredukuojami polinomai virš $\mathbf{C}$ yra tik pirmojo laipsnio polinomai $x-a, a \in \mathbf{C}$.

Lema. 1. Tegu polinomas $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbf{C}[x]$ ir $\bar{f}(x) = \bar{a}_n x^n + \cdots + \bar{a}_1 x + \bar{a}_0$. Tada $\overline{f(z)} = \bar{f}(\bar{z})$.

2. Tegu polinomas $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbf{R}[x]$. Tada $\overline{f(z)} = f(\bar{z})$.

Neredukuojamus polinomus virš realiųjų skaičių kūno $\mathbf{R}$ aprašo tokia teorema.

Teorema. *Neredukuojami polinomai virš realiųjų skaičių kūno $\mathbf{R}$ yra arba pirmojo laipsnio polinomai $x-a, a \in \mathbf{R}$, arba tokie kvadratiniai trinariai x^2+px+q, kad $p^2-4q<0$.*

Įrodymas. Įrodysime, kad neredukuojamas virš $\mathbf{R}$ polinomas $f(x) \in \mathbf{R}[x]$ yra arba $f(x) = x-a$, arba toks $f(x) = x^2+px+q$, kad $p^2-4q<0$ (aišku, kad šie polinomai yra neredukuojami virš $\mathbf{R}$). Į polinomą $f(x)$ galima žiūrėti ir kaip į polinomą virš $\mathbf{C}$. Tada polinomas $f(x)$ turi kompleksinę šaknį $\alpha = a+ib$ ($\mathbf{C}-$ algebriškai uždaras kūnas): $f(\alpha)=0$. Galimi du atvejai.

1) Jeigu $\alpha \in \mathbf{R}$, tai $f(x) \vdots (x-\alpha)$ ir kadangi $f-$ neredukuojamas, tai $f(x) = x-\alpha$.

2) Jeigu $\alpha \notin \mathbf{R}$, tai $\alpha \in \mathbf{C}$ ir $\bar{\alpha} \neq \alpha$. Turime $f(\alpha)=0 \Rightarrow \overline{f(\alpha)} \overset{\text{Lema}}{=} f(\bar{\alpha}) = 0$, t.y polinomas f turi mažiausiai dvi šaknis α ir $\bar{\alpha}$. Tada $f(x) \vdots (x-\alpha)(x-\bar{\alpha})$. Pastebėsime, kad $(x-\alpha)(x-\bar{\alpha}) = x^2 - x(\alpha+\bar{\alpha}) + \alpha\cdot\bar{\alpha} = x^2-2ax+(a^2+b^2) \in \mathbf{R}[x]$ ir $D = 4a^2-4a^2-4b^2 = -4b^2 < 0$, taigi $(x-\alpha)(x-\bar{\alpha})$ yra neredukuojamas polinomas virš $\mathbf{R}$. Tada $f(x) = (x-\alpha)(x-\bar{\alpha}) = x^2-2ax+(a^2+b^2)$.

Įrodyta.

Skirtingo laipsnio dauginamųjų išskyrimas.

Apibrėžimas. *Tegu $f(x) \in K[x]$. Elementas $c \in K$ yra poinomo $f(x)$ $k-$ kartotinė šaknis, jeigu $f(x) = (x-c)^k \cdot f_1(x)$, $f_1(c) \neq 0$. Jeigu $k=1$, tai sakome, kad c yra paprastoji polinomo f šaknis.*

Apibrėžimas. *Jeigu kūno K elementų sekoje $\{1, 1+1, 1+1+1, ...\}$ nėra* 0, *tai sakome, kad kūno K charakteristika yra lygi* 0, *o jeigu skaičius p yra* *mažiausias toks, kad* $\underbrace{1+1+\cdots+1}_{p \text{ kartų}} = 0$ *sakome, kad kūno* K *charakteristika yra lygi* p.

Teiginys. *Jeigu* x_0 *yra polinomo* $f(x) \in K[x]$ *papratastoji šaknis, tai* $f'(x_0) \neq 0$.

Įrodymas.[.........]

Teiginys. *Jei polinomo* $f(x) \in K[x]$ *šaknies kartotinumas yra lygus* k*, ir* k *nesidalija iš kūno* K *charakteristikos, tai išvestinės* $f'(x)$ *šaknies c kartotinumas lygus* $k-1$.

Įrodymas.[.........]

Paskutinius teiginius galime apibendrinti. Tegu kūno K charakteristika yra lygi 0, o polinomo $f \in K[x]$ kanoninis skaidinys virš K yra $a \cdot p_1^{k_1} \cdot p_2^{k_2} \cdots p_s^{k_s}, p_i \neq p_j$.

Teiginys. *Tegu polinomo* f *neredukuojamo daliklio* $p_i \in K[x]$ *kartotinumas yra lygus* $1(\ k_i = 1)$. *Tada šio polinomo nėra išvestinės* f' *kanoniniame skaidinyje .*

Įrodymas.[.........]

Teiginys. *Tegu polinomo* f *neredukuojamo daliklio* $p_i \in K[x]$ *kartotinumas yra lygus* k_i. *Tada polinomo* p_i *kartotinumas išvestinės* f' *kanoniniame skaidinyje yra lygus* $k_i - 1$ *.*

Įrodymas.[.........]

Paskutiniojo teiginio pagalba polinomą f galima suskaidyti dauginamaisiais taip: $f = aF_{r_1}(x) \cdots F_{r_l}(x)$, kad polinomo F_{r_i} kanoniniame skaidinyje visų neredukuojamų polinomų kartotinumas yra lygus r_i ($r_i \neq r_j$, kai $i \neq j$). Tai ir yra skirtingo laipsnio dauginamųjų išskyrimas.