4 paskaita.

Dalumas su liekana. BDD. Tarpusavyje pirminiai polinomai. Neredukuojami polinomai. Skirtingo laipsnio polinomų išskyrimas. Lyginiai ir faktoržiedis.

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.[.....]

Apibrėžimas. Tegu $f(x)$, $g(x) \in K[x], g(x) \neq 0$. Didžiausio laipsnio polinomas $d(x) \in K[x]$, kurio koeficientas prie didžiausio laipsnio 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.[.....]

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 $f = a \cdot p_1 \cdot p_2 \cdot \cdots \cdot p_s$, 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.

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.

Lyginiai

Apibrėžimas. Tegu $K-$ kūnas, o $f(x), g(x), m(x) \in K[x]$ ir $\deg m(x) \geq 1$. Sakysime, kad polinomas $f(x)$ lygsta polinomui $g(x)$ moduliu $m(x)$, jeigu $(f(x) - g(x)) \vdots m(x)$. Rašysime $f(x) \equiv g(x) \pmod{m(x)}$.

Pagrindinės lyginių savybės yra šios:

1. Refleksyvumas: su visais $f \in K[x]$, $f \equiv f \pmod{m(x)}$.

2. Simetriškumas: $\left.\begin{array}{c} f, g \in K[x] \\ f \equiv g \pmod{m(x)} \end{array}\right\} \Longleftrightarrow g \equiv f \pmod{m}$.

3. Tranzityvumas: $\left.\begin{array}{c} f, g, h \in K[x] \\ f \equiv g \pmod{m(x)} \\ g \equiv h \pmod{m(x)} \end{array}\right\} \Longrightarrow f \equiv g \pmod{m(x)}$.

4. $\left.\begin{array}{c} f, g, c, d \in Z \\ f \equiv c \pmod{m} \\ g \equiv d \pmod{m} \end{array}\right\} \Longrightarrow f \pm g \equiv c \pm d \pmod{m(x)}$.

5. $\left.\begin{array}{c} f, g, c, d \in Z \\ f \equiv c \pmod{m} \\ g \equiv d \pmod{m} \end{array}\right\} \Longleftrightarrow f \cdot g \equiv c \cdot d \pmod{m}$.

6. Kiekvienas polinomas $f(x)$ lygsta moduliu $m(x)$ tik su vienu polinomu tokiu polinomu $r(x)$, kad $\deg r(x) < \deg m(x)$. Šis polinomas $r(x)$ yra ne kas kitas kaip polinomų poros f ir m dalybos su liekana teoremos liekana: $f(x) = m(x) q(x) + r(x)$. Tada $f(x) \equiv r(x) \pmod{m(x)}$.

Liekanų klasės.

Apibrėžimas. Tegu $f, m \in K[x]$, ir $\deg m \geq 1$. Polinomų žiedo $K[x]$ poaibį

$$\{g \in K[x] \,|\, g \equiv f \pmod{m(x)}\}$$

vadinsime **liekanų klase** moduliu $m(x)$, kuriai atstovauja f, arba tiesiog liekanų klase, ir žymėsime ${}_mK_f$, arba K_f, arba $[f(x)]_{m(x)} = [f(x)]$.

Svarbiausios **liekanų klasių savybės** yra šios:

1. Refleksyvumas: $f \in K[x] \Longrightarrow f \in K_f$.

2. Simetriškumas: $f \in K_g \Longrightarrow g \in K_f$.

3. Tranzityvumas: $\left.\begin{array}{c} f \in K_g \\ g \in K_f \end{array}\right\} \Longrightarrow f \in K_g$.

4. Tegu $m(x) \in K[x], \deg m(x) \geq 1$. Atsižvelgę į tai, kad su kiekvienu polinomu $f(x)$ yra teisinga $f(x) \equiv r(x) (\mathrm{mod}\, m(x))$, čia $r(x)$ – vienintėlė tokia polinomo f dalybos su liekana iš m liekana, kad $\deg r < \deg m$, liekanų klasės $\left\{K_{r(x)} | \deg r(x) < \deg m(x)\right\}$ yra polinomų aibės $K[x]$ *skaidinys,* t.y.
(a) $K[x] = \underset{r \in K[x], \deg r < \deg m}{\cup} K_{r(x)}$
(b) jeigu $K_{r_1} \cap K_{r_2} \neq \emptyset$, tai $K_{r_1} = K_{r_2}$.

Apibrėžimas. Tegu $m(x) \in K[x], \deg m(x) \geq 1$. Aibę

$$\left\{K_{r(x)} | \deg r(x) < \deg m(x)\right\}$$

vadinsime polinomų žiedo $K[x]$ faktofaibe moduliu $m(x)$ ir žymėsime $K[x]/(m(x))$.

Aibėje $K[x]/(m(x))$ galima apibrėžti šiuos veiksmus.

Apibrėžimas. $\left.\begin{array}{c} K', K'' \in K[x]/(m(x)) \\ f \in K', g \in K'' \end{array}\right\}$, tada $\begin{array}{c} K' + K'' \overset{\mathrm{def}}{=} K_{f+g} \\ K' \cdot K'' \overset{\mathrm{def}}{=} K_{f \cdot g} \end{array}$.

Teiginys. Sudėties ir sandaugos veiksmai liekanų klasėms apibrėžti korektiškai, t.y. jie nepriklauso nuo klasių atstovų f ir g parinkimo.

Įrodymas.[.....]

Pavyzdžiai.[.....]

Teiginys. 1.Polinomų žiedo $K[x]$ faktofaibė moduliu $m(x)$, $K[x]/(m(x))$, sudėties ir sandaugos operacijų atžvilgiu sudaro komutatyvųjį žiedą su vienetu. $K[x]/(m(x))$ vadiname *faktoržiedžiu.*

2. Faktoržiedis $K[x]/(m(x))$ yra kūnas tada ir tik tada, kada $m(x)$ – neredukuojamas polinomas.

Be įrodymo.

Aptarkime faktoržiedžio $K[x]/(m(x))$ elementų reiškimą. Tegu $\deg m(x) = n \geq 1$.

Visų pirma, į patį kūną K galima žiūrėti kaip faktoržiedžio $K[x]/(m(x))$ poaibį: $K \subset K[x]/(m(x))$, nes su visais $a, b \in K$ yra teisinga

$$[a] = [b] \Longleftrightarrow \left\{ \begin{array}{c} a-b \text{ dalijasi iš } m(x) \\ \deg m(x) \geq 1 \end{array} \right\} \Longleftrightarrow a - b = 0 \Longleftrightarrow a = b.$$

Taigi, klasę $[a]$ galime sutapatinti su pačiu klasės polinomu a, kurio laipsnis yra $< \deg m$. Tegu $\alpha \stackrel{\text{def}}{=} [x]$. Tada kiekvieną faktoržiedžio $K[x]/(m(x))$ elementą galima reikšti

$$\begin{array}{c} [a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0] \\ = [a_{n-1}][x^{n-1}] + [a_{n-2}][x^{n-2}] + \cdots + [a_1][x] + [a_0] \\ = a_{n-1}[x]^{n-1} + a_{n-2}[x]^{n-2} + \cdots + a_1[x] + a_0 \\ = a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \cdots + a_1\alpha + a_0. \end{array}$$

Matome, kad faktoržiedžio $K[x]/(m(x))$ elementai yra tiesinės elementų $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ kombinacijos ir todėl šiuos elementus patogu įsivaizduoti kaip polinomų iš $K(x)$ (nebūtinai šių polinomų laipsnis turi būti mažesnis už n !) reikšmes elemente $\alpha = [x]$, atsižvelgiant į tai, kad $m(\alpha) = m([x]) = [m(x)] = [0] = 0$. Matome, kad α yra polinomo $m(x)$ šaknis.

Pavyzdys. Tegu K – kūnas, o $\deg m(x) = 1$. Tada

$$K[x]/(m(x)) = \{[a] \,|\, a \in K\} = K.$$

Lema. Polinomas $x^2 + 1$ yra neredukuojamas polinomas virš $\mathbf{R}$.

Įrodymas. Sakykime $x^2+1 = f(x) \cdot g(x)$. Tada $2 = \deg(x^2+1) = \deg f(x) + \deg g(x)$. Tegu $\deg f = 1$ (tada ir $\deg g = 1$) ir $f(x) = ax + b$, $a \neq 0$, o $g(x) = cx + d$, $c \neq 0$. Tada

$$x^2 + 1 = (ax + b)(cx + d) = acx^2 + (ad + bc)x + bd$$

ir todėl $ac = 1, ad + bc = 0, bd = 1$. Tada $d = -\frac{bc}{a}$ ir

$$1 = bd = -\frac{b^2 c}{a} = -\frac{b^2 c^2}{a\, c} = -b^2 c^2 = -\left(bc\right)^2 \leq 0.$$

Ši prieštara rodo, kad $\deg f \neq 1$ ir todėl arba $\deg f = 0$ (tada $\deg g = 2$), arba $\deg f = 2$ (tada $\deg g = 0$). Ir vienu ir kitu atveju turime, kad polinomas $x^2 + 1$ yra neredukuojamas polinomas virš $\mathbf{R}$.

Įrodyta.

Pavyzdys. Tegu $K = \mathbf{R}$ - realiųjų skaičių kūnas, o $m(x) = x^2 + 1 \in \mathbf{R}[x]$. Tada

$$\mathbf{C} = \mathbf{R}[x] / (x^2 + 1) = \left\{ a + b[x]_{(x^2+1)} \mid a, b \in \mathbf{R} \right\}$$

yra kūnas (nes x^2+1 yra neredukuojamas polinomas virš $\mathbf{R}$), kurio poaibiu yra realiųju skaičių kūnas. Šio kūno elementus vadiname **kompleksiniais skaičiais**, o patį kūną - **kompleksinių skaičių kūnu.** Pažymėkime $i \stackrel{\text{def}}{=} [x]_{(x^2+1)}$. Tada kompleksinį skaičių $a + b[x]$ reiškiame $a + ib$ ir turime

$i^2 = [x]^2 = [x^2] = [x^2 + 1 - 1] = [x^2 + 1] - [1] = -1.$

Veiksmai šiame kūne turi šias savybes:

1) $(a + ib) + (c + id) = (a + c) + i(b + d)$.

2) $(a + ib) \cdot (c + id) = ac + i(ad + bc) + i^2 bd = ac + i(ad + bc) - bd = (ac - bd) + i(ad + bc)$.

3) Jeigu $a + ib \neq 0$, tai $(a + ib)^{-1} = \frac{1}{a+ib} = \frac{1}{a+ib} \cdot \frac{a-ib}{a-ib} = \frac{a-ib}{a^2+b^2} = \left(\frac{a}{a^2+b^2}\right) - i\left(\frac{b}{a^2+b^2}\right)$.

Kompleksinių skaičių kūnui skirsime kitą paskaitą.