(7)

Polinomų žiedas

Tegul K – komutatyvusis žiedas su vienetu 1, A – jo požiedis, kuriam priklauso 1. Jei $t \in K$, tai mažiausias požiedis (žiedas), kuriam priklauso A ir t, susideda iš elementų pavidalo

$$(1) \qquad a(t) = a_0 + a_1 t + a_2 t^2 + \dots + a_n t^n,$$

čia $a_s \in A$, $n \in \mathbb{Z}$, $n \geq 0$.

Mes jį pažymėsime $A[t]$ ir vadinsime žiedu, gautu iš A prijungiant elementą t, o (1) išraišką – polinomu nuo t su koeficientais iš A.

Dviejų polinomų sumą ar sandaugą apibrėžime tradiciniu būdu. Jakysim, kai $n=2$, tai

$$a(t)+b(t) = (a_0+a_1t+a_2t^2)+(b_0+b_1t+b_2t^2) = \\ = (a_0+b_0)+(a_1+b_1)t+(a_2+b_2)t^2$$

$$a(t)\cdot b(t) = a_0b_0 + (a_0b_1+a_1b_0)t + (a_0b_2+a_1b_1+a_2b_0)t^2 + \\ + (a_1b_2+a_2b_1)t^3 + a_2b_2t^4$$

Aišku, kad gaunant šias formules panaudota žiedo K komutatyvumu.

Kadangi t – bet kuris žiedo K elementas, gali atsitikti taip, kad skirtingos (1) išraiškos gali iš tikrųjų sutapti. Tarkim, jei $A=\mathbb{Q}$, $t=\sqrt{2}$, tai $t^2=2$, $t^3=2t$ – sąryšiai, kurie jokiu būdu neišvedami iš formalaus polinomo apibrėžimo. Tam, kad neatsirastų tokie papildomi sąryšiai, reikia tarti, kad t – bet koks simbolis, – visai nebūtinai žiedo K elementas. Jo vaidmuo tik pagalbinis. Mums bus svarbios taisyklės, pagal kurias gaunamos išraiškos $a(t)+b(t)$, $a(t)\cdot b(t)$.

Todėl reikalingas tikslus algebrinio objekto – polinomo apibrėžimas. Jį turėdami, galėsime apibrėžti polinomų žiedą.

(7) Vieno kintamojo daugianariai. Tegul A - bet kuris ~~žiedas~~ komutatyvusis žiedas su vienetu. Sukonstruosime naują žiedą B, kurio elementai – tai begalinės sutvarkytos sekos

(2) $$f=(f_0, f_1, f_2, \dots), \quad f_i \in A,$$

tokios, kad visi f_i, išskyrus baigtinį jų skaičių, yra lygūs 0. Apibrėžime aibėje B sudėties ir daugybos operacijas tokiu būdu:

$$f+g=(f_0, f_1, f_2, \dots)+(g_0, g_1, g_2, \dots)=$$

$$=(f_0+g_0, f_1+g_1, f_2+g_2, \dots)$$

$$f\cdot g=h=(h_0, h_1, h_2, \dots),$$

kur

$$h_k=\sum_{i+j=k} f_i g_j, \quad k=0,1,2,\dots$$

Aišku, kad sudedant ir dauginant gautnamos (2) pavidalo sekos su baigtiniu nenuliniu elementų skaičiumi, taigi, sumos ir sandaugos priklausys B. Galima įsitikinti, kad tenkinamos visos ~~žiedo~~ komutatyvaus žiedo su vienetu aksiomos. (Vienetas $(1,0,0,\dots)$, nulis $(0,0,0,\dots)$

Sekos $(a,0,0,\dots)$ sudedamos ir dauginamos kaip žiedo A elementai, taigi galima sutapatinti $(a,0,,\dots 0\dots)$ su a. Tokiu būdu A yra žiedo B požiedis.

(7) Seką $(0,1,0,0,\dots)$ pažymėsime X ir pavadinsime ją kintamuoju (nežinomuoju) virš A. Įvedami žiedo B apibrėžtę daugybos operaciją randame, kad

$$X = (0,1,0,0,\dots)$$

(3)
$$X^2 = (0,0,1,0,\dots)$$
$$\dots\dots$$
$$X^n = (0,0,\dots 0,1,0,\dots)$$
↖ n-tojoje vietoje

Be to, kadangi $A \subset B$, turėsime

$$(0,0,\dots,0,a,0,\dots) = aX^n = X^n a$$

Taigi, jei f_n – paskutinis nelygus nuliui seko $f = (f_0, f_1, \dots f_n, 0, 0, \dots)$ narys, tai įvertais žymėjimais turėsime

$$f = (f_0, f_1, \dots, f_{n-1}, 0, 0, \dots) + f_n X^n =$$

(4)
$$= (f_0, \dots, f_{n-2}, 0, 0, \dots) + f_{n-1} X^{n-1} + f_n X^n =$$
$$= f_0 + f_1 X + f_2 X^2 + \dots + f_n X^n.$$

Toks elemento f paskaidalas vienintelis, kadangi $f_0, \dots, f_n$ skirtingi pasirinkę – tai seko $(f_0, \dots, f_n, 0, \dots)$ elementai, o ta seka yra nulinė tuomet ir tik tada, kai $f_0 = f_1 = \dots f_n = 0$.

Apibrėžimas. Tokiu būdu sukonstruotas žiedas nuo vieno kintamojo B yra žymimas $A[X]$ ir vadinamas polinomų žiedu virš A, o jo elementai – polinomais (daugianariais).

(7) Toliau mes skirsime daugianarį $f = X$ nuo kintamojo x, įgyjančio reikšmes tam tikroje aibėje.

Kartais naudojamas kitas daugianario f pavidalas

$$f(X) = a_0 X^n + a_1 X^{n-1} + \dots + a_n,$$

t.y., $f(X)$ užrašomas laipsnių mažėjimo tvarka.

Elementai f_i (ar a_i) vadinami polinomo f koeficientais. Daugianaris f <u>nulinis</u>, kai jo koeficientai lygūs 0. Koeficientas f_0 prie X nulinio laipsnio dar yra vadinamas <u>pastoviuoju nariu</u>. Jeigu $f_n \neq 0$, tai f_n vadinamas <u>vyriausiuoju koeficientu</u>, o n - <u>polinomo laipsniu</u> ir rašoma $n = \deg f$. Nuliniam daugianariui priskiriamas laipsnis $-\infty$. ($-\infty + (-\infty) = -\infty$, $-\infty + n = -\infty$, $-\infty < n \ \forall n \in \mathbb{N}$). Daugianariai, kurių laipsniai yra 1, 2, 3, ... vadinami atitinkamai <u>tiesiniais</u>, <u>kvadratiniais</u>, <u>kubiniais</u> ir t.t.

Vieneto vaidmenį žiede $A[X]$ atlieka žiedo A vienetas 1, neprarandamas kaip nulinio laipsnio daugianaris. Iš daugybos ir sudėties operacijų apibrėžimo žiede $A[X]$ išplaukia, kad bet kuriems dviems daugianariams

(5) $f = f_0 + f_1 X + \dots + f_n X^n$, $g = g_0 + g_1 X + \dots + g_m X^m$,

kurių laipsniai yra atitinkamai n ir m, yra teisingos nelygybės

$$\deg(f+g) \leq \max(\deg f, \deg g)$$

$$\deg(fg) \leq \deg f + \deg g$$

Antroji nelygybė iš tikrųjų yra lygybė visada, kai tik vyriausieji (5) polinomų koeficientų sandaugos nelygūs 0,

(7) kadangi

(6) $fg = f_0g_0 + (f_0g_1 + f_1g_0)X + \dots + f_ng_mX^{n+m}$

Tai reiškia, kad teisinga ši teorema:

T1. Jei A – sveikumo sritis, tai ir žiedas $A[X]$ yra sveikumo sritis.

Polinomų žiedo vietą komutatyviųjų žiedų klasėje iš dalies paaiškina ši teorema:

T2. Tegul A – komutatyviojo žiedo K požiedis. Kiekvienam elementui $t \in K$ egzistuoja vienintelis žiedų homomorfizmas

$$\Pi_t : A[X] \to K$$

toks, kad

(7) $\forall a \in A \quad \Pi_t(a) = a \quad \Pi_t(X) = t$

Įrodymas. Leiskime, kad tokis homomorfizmas Π_t egzistuoja. Kadangi $\Pi_t(f_i) = f_i$ bet kuriam polinomo f, užrašyto pavidalu (4), koeficientui ir

$$\Pi_t(X^k) = (\Pi_t(X))^k = t^k$$ (homomorfizmo savybė ir sąlyga (7)), tai

(8) $$\Pi_t(f) = \Pi_t(f_0 + f_1X + \dots + f_nX^n) = f_0 + f_1t + \dots + f_nt^n,$$

t.y., $\Pi_t(f)$ vienareikšmiškai užrašomas (8) formule.

Atvirkščiai, jei Π_t užduosime formule (8), tai patenkinsime (7) sąlygą ir teisingai žiedų homomorfizmą. Tai aišku žiedų adityviųjų grupių atvaizdavimui, o sandaugai tuo pačiu

$$\Pi_t(fg) = f_0g_0 + (f_0g_1 + f_1g_0)t + \dots + (f_ng_m)t^{n+m} =$$
$$= \left(\sum_{i=0}^{n} f_i t^i\right)\left(\sum_{j=0}^{m} g_j t^j\right) = \Pi_t(f)\cdot\Pi_t(g).$$

(8) formulės taikymo rezultatą vadinsime polinomo reikšme kai $X = t$, kadangi

$$\Pi_t(f) = f(t).$$

Žinoti $\Pi_t(f)$ – reiškia mokėti apskaičiuoti f reikšmę, kai $X = t$. Homomorfizmai Π_x, kai $x \in A$ susieja polinomo algebrinę ir funkcinę sampratas. Pagal mūsų apibrėžimą tiesinis daugianaris $X - c = (-c, 1, 0, \dots)$ niekada nėra lygus 0, bet su juo asocijuota funkcija $x \to x - c$ įgyja nulinę reikšmę, kai $x = c$. Kitas pavyzdys: nelygus 0 daugianaris $X^2 + X$ su koeficientais iš $\mathbb{F}_2$ ($\text{kur } 1+1=0$) reiškia nulinę funkciją $\tilde{f}: \mathbb{F}_2 \to \mathbb{F}_2$, kadangi $0^2+0=0$ ir $1^2+1=0$.

Elementas $t \in K$ vadinamas <u>algebriniu virš A</u>, jei $\Pi_t(f) = 0$ prie tam tikro $f \in A[X]$. Jeigu $\Pi_t: A[X] \to K$ – izomorfinis įdėtis (monomorfizmas), tai t vadinamas <u>transcendentiniu</u> virš A. Jei $A = \mathbb{Q}$ ir $K = \mathbb{C}$, tai kalbama tiesiog apie algebrinius ir transcendentinius skaičius. Pavyzdžiui, skaičiai e, π, žinomi iš analizės, yra transcendentiniai, o skaičiai $\sqrt{2}$, $\sqrt{3}$, $\sqrt{2}+\sqrt{3}$ – algebriniai.

Homomorfizmas Π_t išreiškia polinomų žiedo $A[X]$ universalią savybę. Tas universalumas dar išsamiau išreiškiamas ~~tokioje te~~ šioje teoremoje:

T3. Tegul A ir K – bet kurie komutatyvieji žiedai, $t \in K$, $\varphi: A \to K$ – homomorfizmas.

Tada egzistuoja vienintelis φ pratęsimas ilgi homomorfizmas $\varphi_t: A[X] \to K$ iš polinomų žiedo $A[X]$ į K, atvaizduojantis kintamąjį X į t.

Sveikųjų skaičių aritmetika

Pagrindinė aritmetikos teorema. Sveikas skaičius s vadinamas skaičiaus n dalikliu (arba daugikliu), jei $n = st$ kuriam tikro $t \in \mathbb{Z}$. Savo mastu n yra vadinamas skaičiaus s kartotiniu. Tai, kad n dalosi iš s žymima simboliu $s|n$, o tai, kad n nėra dalomas iš s, žymima $s \nmid n$. Dalumas – tranzityvusis sąryšis aibėje $\mathbb{Z}$. Toliau, jei $m|n$ ir $n|m$, tai $n = \pm m$ ir sveikieji skaičiai n ir m vadinami asocijuotaisiais. Sveikasis skaičius p, kurio dalikliai yra tik $\pm p$, ± 1 (ne tikrieji dalikliai), vadinamas pirminiais. Daržniausiai pirminiais skaičiais imami teigiami pirminiai skaičiai > 1.

Pirminių skaičių reikšmę atskleidžia

T. (Pagrindinė aritmetikos teorema). Kiekvieną teigiamą sveiką skaičių $n \neq 1$ galima užrašyti pirminių skaičių sandauga $n = p_1 p_2 \dots p_s$. Šis pavidalas vienintelis daugiklių užrašymo tvarkos tikslumu.

Jei surinkime vienodus pirminius daugiklius, tai galima užrašyti

$$n = p_1^{\varepsilon_1} p_2^{\varepsilon_2} \dots p_k^{\varepsilon_k}, \quad \varepsilon_i > 0, \quad 1 \le i \le k$$

Bet kuriam racionaliajam skaičiui $a = \frac{n}{m} \in \mathbb{Q}$ teisingas analogiškas išdėstymas, bet laipsnio rodikliai ε_i tokiu atveju bus tiek teigiami tiek neigiami.

Pastebėsime, kad aibė

$$P = \{2, 3, 5, 7, 11, 13, \dots\}$$

(visų pirminių skaičių aibė) yra begalinė (Euklido teorema). Iš tikrųjų, jei pirminių skaičių skaičius būtų baigtinis, tarkime $p_1, p_2, \dots, p_t$, tai pagal pagrindinę aritmetikos teoremą skaičius

$$c = p_1 p_2 \cdots p_t + 1$$

dalintųsi bent iš vieno skaičiaus p_i. Neprarasdami bendrumo galėtume teigti, kad $c = p_1 c'$. Tada

$$p_1 c' = p_1 p_2 \cdots p_t + 1 \Rightarrow p_1 (c' - p_2 \cdots p_t) = 1,$$

bet tai neįmanoma, kadangi vieneto dalikliais aibėje $\mathbb{Z}$ yra tik $+1$ ir -1.

Bendras didžiausias daliklis (BDD) ir bendras mažiausias kartotinis (BMK) aibėje $\mathbb{Z}$.

Bet kuriuos sveikuosius skaičius n ir m galima užrašyti tų pačių pirminių skaičių laipsnių sandauga

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \quad m = \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},$$

jeigu leisti naudoti nulinius laipsnių rodiklius (kaip visada, laikysime $p_i^0 = 1$). Nagrinėsime du sveikuosius skaičius

$$(1) \qquad \begin{aligned} BDD(n, m) &= p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k} \\ BMK(n, m) &= p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}, \end{aligned}$$

čia $\gamma_i = \min(\alpha_i, \beta_i)$, $\delta_i = \max(\alpha_i, \beta_i)$, $i = 1, 2, \dots, k$.

Kadangi $d \mid n \Rightarrow d = \pm p_1^{\alpha_1'} \cdots p_k^{\alpha_k'}$, $0 \le \alpha_i' \le \alpha_i$, tai iš (1) gaunamę tokius teiginius:

1°. $BDD(n,m) \mid n$, $BDD(n,m) \mid m$ ir jeigu $d \mid n$, $d \mid m$, tai $d \mid BDD(n,m)$

2°. $n \mid BMK(n,m)$, $m \mid BMK(n,m)$ ir jei $n \mid u$, $m \mid u$, tai $BMK(n,m) \mid u$.

Jei $n > 0$, $m > 0$, turėsime

(2) $$BDD(n,m) \cdot BMK(n,m) = n \cdot m$$

Sveikieji skaičiai n ir m vadinami tarpusavyje pirmiaisiais, jei $BDD(m,u) = 1$. Tokiu atveju (2) lygybė įgyja pavidalą

$$BMK(n,m) = nm$$

3. Dalybos algoritmas aibėje $\mathbb{Z}$. Jei $a, b \in \mathbb{Z}$, $b > 0$, tai visada rasis $q, r \in \mathbb{Z}$ tokie, kad

$$a = bq + r, \quad 0 \le r < b$$

(jei apsiriboti reikalavimu, kad $b \neq 0$, tai turėsime nelygybę $0 \le r < |b|$)

Įrodymui, aibė

$$S = \{a - bs : s \in \mathbb{Z},\ a - bs \ge 0\},$$

netuščia (pavyzdžiui, $a - b(-a^2) > 0$). Todėl aibė S turės mažiausią elementą, pažymėsime jį $r = a - bq$. Pagal sąlygą $r \ge 0$. Jei tarsime, kad $r \ge b$, tai gautume elementą $r - b = a - b(q+1) \in S$, mažesnį už r. Šis prieštaravimas neįmanomas tik kai $r < b$. ∎

Dalyba su liekana polinomų žiede.

Polinomų žiede $A[X]$ galima apibrėžti dalybos su liekana algoritmą, analogiškai, kaip tai buvo padaryta sveikųjų skaičių žiede $\mathbb{Z}$. Pakanka pareikalauti, kad žiedas A būtų sveikas (be nulio daliklių).

Teorema. Tegul A – sveikasis žiedas, o $g \in A[X]$ – daugianaris, kurio vyriausiasis koeficientas turi atvirkštinį žiede A. Tada kiekvienam daugianariui $f \in A[X]$ pasirinkime vieną ir tik vieną f daugianarių poros $q, r \in A[X]$, kuriems

$$f = qg + r \quad , \deg r < \deg g$$