8

8. Laukai

8.1. Pagrindinis sąvokos

Mums gerai žinomose skaičių žiedeose $\mathbb{Z}$, $\mathbb{Q}$ ir $\mathbb{R}$ ši lygybės $ab=0$ išplaukia, kad arba $a=0$ arba $b=0$. Tačiau, kaip anksčiau matėme pavyzdžiuose, matricų žiede M_n ši savybė jau nebegalioja. Gali kilti įtarimas, kad taip ~~dėl to~~ yra todėl, kad M_n nekomutatyvus. Tačiau ~~tai~~ komutatyviajame žiede $\mathbb{Z}_4$ turime lygybę $2 \cdot 2 = 0$. Pateiksime dar porą ~~tokių~~ pavyzdžių.

1 pvz. Nagrinėsime skaičių poras (a,b). Čia a, b gali priklausyti vienam iš žiedų $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$. Apibrėšime tų porų aibėje sudėtį ir daugybą formulėmis:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2).$$

Tokiu būdu gaunamo komutatyvaus žiedo su vienetu $(1,1)$. Iš viso turime tų pačių rūšių

$$(1,0) \cdot (0,1) = (0,0) = 0 \text{ (žiedo nulis)}$$

2 pvz. Imkime realiųjų funkcijų žiedą $\mathbb{R}^{\mathbb{R}}$ ir jame priklausančias dvi funkcijas

~~$f(x) = x$~~ $f(x) = |x| + x$, $g(x) = |x| - x$

~~$f(x) = |x| + x$~~ Šios funkcijos nelygios tapatingai nuliui, bet $f(x) \cdot g(x) = 0$

Apibrėžimas. Jei $ab=0$, bet $a\neq 0$ ir $b\neq 0$ žiede K, tai a vadinamas *kairiuoju*, o b - *dešiniuoju* nulio dalikliu. Jei žiedas komutatyvus, tada kalbama tiesiog apie nulio daliklius. Pats nulis žiede $K\neq 0$ - trivialusis nulio daliklis. Jei daugiau nulio daliklių nėra, tai K vadinamas *žiedu be nulio daliklių*.

Komutatyvusis žiedas su vienetu $1\neq 0$, kuriame nėra nulio daliklių vadinamas *sveikuoju žiedu* (*sveikumo žiedu* arba *sveikumo sritimi*).

Teorema. Netrivialus komutatyvusis žiedas K su vienetu yra sveikas tada ir tik tada, kada jame išpildomas prastinimo dėsnis

$$ab=ac,\ a\neq 0 \Rightarrow b=c$$

visiems $a,b,c\in K$.

Įrodymas. Tikrąjį, jei žiede K galioja prastinimas, tai iš $ab=0=a\cdot 0$ išplaukia, kad arba $a=0$, arba $a\neq 0$, bet $b=0$. Įrodykime atvirkščiai, jei K - sveikumo sritis, tai

$$ab=ac,\ a\neq 0 \Rightarrow a(b-c)=0 \Rightarrow b-c=0 \Rightarrow b=c$$

□

Žiede K su vienetu natūralu nagrinėti „apverčiamus" elementus. Elementą a vadiname apverčiamu (arba vieneto dalikliu), jei egzistuoja elementas a^{-1}, kuriam $aa^{-1}=1=a^{-1}a$. Tiesiau, reikėtų kalbėti apie apverčiamus iš kairės arba iš dešinės elementus ($ab=1$ ~~ed~~ ar $ba=1$), bet komutatyviuose žiedeose, o taip pat žiedeose be nulio daliklių tos sąvokos sutampa. Ištikrųjų, jei $ab=1$, tai $aba=a \Rightarrow a(ba-1)=0$. Kadangi $a\neq 0$, tai $ba-1=0$ ~~[illegible]~~ $ba=1$.

Žiede M_n apverčiami elementai – tai matricos, kurių determinantai nelygūs nuliui.

Apverčiamasis elementas negali būti nulio dalikliu: $ab=0 \Rightarrow a^{-1}(ab)=0 \Rightarrow (a^{-1}a)b=0 \Rightarrow 1\cdot b=0 \Rightarrow b=0$

~~Analogiškai~~ $ba=0 \Rightarrow b=0$.

Teorema 2. Visi apverčiami žiedo K su vienetu elementai sudaro ~~grupę~~ multiplikacinę grupę $U(K)$.

Ištikrųjų, kadangi $1\in U(K)$, $a\in U(K) \Rightarrow a^{-1}\in U(K)$, o, kadangi žiede K daugyba asociatyvi, tai belieka įsitikinti, kad sandauga $ab\in U(K)$, jei $a,b\in U(K)$. Tai ir tikrųjų taip, kadangi

$(ab)^{-1}=b^{-1}a^{-1}$, taigi elementas ab apverčiamas. ∎

Pvz.: $U(\mathbb{Z}) = \{\pm 1\}$ – ciklinė grupė, kurios eilė = 2.

Jei žiedo aksiomatikoje aksiomą K2 (K – pusgrupė daugybos atžvilgiu) pakeisime

K2') Aibė $K \setminus \{0\}$ atžvilgiu $\cdot$ – grupė,

tai gausime taip vadinamą žiedą su dalyba arba kūną.

Taigi kūne nėra nulio daliklių, be to kiekvienas jo elementas apverčiamas.

Jei leisime, kad K – komutatyvus, tai abi operacijos $+$ ir $\cdot$ bus beveik visiškai simetriškos. Komutatyvųjį kūną vadinsime lauku. Taigi, turime apibrėžimą.

Apibrėžimas. Laukas P – tai komutatyvus žiedas su vienetu $1 \neq 0$, kuriame kiekvienas elementas $a \neq 0$ turi atvirkštinį (t.y., apverčiamas). Grupė $P^* = U(P)$ vadinama lauko multiplikacine grupe.

Laukas – tai dviejų Abelio grupių hibridas: adicinė ir multiplikacinė grupės, susietos distributyvumo dėsniu.

Sandauga ab^{-1} paprastai užrašoma trupmena $a/b = \frac{a}{b}$ pavidalu. Taigi, trupmena a/b turi prasmę tik kai $b \neq 0$, ji yra lygties $bx = a$ sprendinys.

Trupmenų veiksmai atliekami laikantis kelių taisyklių:

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc \quad , b, d \neq 0$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad b, d \neq 0$$

$$-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b} \qquad , b \neq 0$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \qquad b, d \neq 0$$

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a} \qquad a, b \neq 0$$

Tai mums gerai žinomos „mokyklinės" taisyklės, bet jas reikia gauti iš aksiomų.

Pvz., tam, kad gauti $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$

tariame, kad

$x = \frac{a}{b}$, $y = \frac{c}{d}$ - lygčių $bx = a$ ir $dy = c$ sprendiniai. Tų šių lygčių išplaukia

$dbx = da$ $\quad bdy = bc \Rightarrow bd(x+y) = da + bc \Rightarrow$

$\Rightarrow t = x + y = \frac{da + bc}{bd}$, t - vienintelis lygties $dbt = da + bc$ sprendinys

Lauko P polaukis F vadinamas požiedis, kuris pats yra laukas. Racionaliųjų skaičių aibė $\mathbb{Q}$ – realiųjų skaičių lauko $\mathbb{R}$ polaukis.

Jei $F \subset P$, tai sakoma, kad P yra savo polaukio F praplėtimas (plėtinys). Tokiu atveju lauko P vienetas ir nulis priklauso F ir lauke F bus vienetu ir nuliu. Jeigu lauke P įeina visi polaukiai, kuriems priklauso F ir kuris nors elementas $a \in P$, $a \notin F$ sakysime, tai gausime minimalų polaukį F_1, kuriam priklauso aibė $\{F, a\}$.

Tokiu atveju sakoma, kad lauko F plėtinys F_1 gautas prijungiant prie lauko F elementą a, tai žymime $F_1 = F(a)$. Analogiškai galima kalbėti apie polaukį $F_1 = F(a_1, a_2, \dots, a_n)$, kai prie lauko F prijungiame lauko P n elementų $a_1, a_2, \dots, a_n$.

Pvz., $\mathbb{Q}(\sqrt{2})$ – tai aibė skaičių, kurių pavidalas

$$a + b\sqrt{2},$$

čia $a, b \in \mathbb{Q}$. Čia $(\sqrt{2})^2 = 2$

$$\frac{1}{a+b\sqrt{2}} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2},$$ jei tik $a + b\sqrt{2} \neq 0$.

Lygiai taip pat gaunama laukus $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$ ir t.t.

Sakome, kad laukai P ir P' izomorfiniai, jeigu jie yra izomorfiniai kaip žiedai.

Pagal apibrėžimą, jei f - izomorfizmas, tai $f(0)=0'$ ir $f(1)=1'$.

Kalbėti apie laukų homomorfizmą nėra prasmės, kadangi

$$\text{Ker } f \neq 0 \Rightarrow f(a)=0,\ a\neq 0 \Rightarrow$$
$$\Rightarrow f(1)=f(aa^{-1})=f(a)f(a^{-1})=0\cdot f(a^{-1})=0 \Rightarrow$$
$$\Rightarrow \forall b \quad f(b)=f(1\cdot b)=f(1)\cdot f(b)=0\cdot f(b)=0 \Rightarrow \text{Ker } f=P.$$

Tačiau (lauko P) automorfizmų nagrinėjimas yra svarbus laukų savybių tyrimo būdas.

Laukų plėtiniai yra analogiški žmonijos poreikiui tenkinti didesnį skaičių aibę. Tą procesą (istoriškai labai ilgą) galima pavaizduoti diagrama

$$\{\text{vienas}\} \rightsquigarrow \{\text{vienas ir vienas yra } 2\} \rightsquigarrow \mathbb{N} \rightsquigarrow \{\mathbb{N},0\} \rightsquigarrow$$
$$\rightsquigarrow \mathbb{Z} \rightsquigarrow \mathbb{Q} \sim \mathbb{Q}(\sqrt{2}) \rightsquigarrow \mathbb{R}$$

Šis procesas tęsiasi iki mūsų laikų. Šiuo metu žinoma labai daug įvairių laukų. Ne visi plėtiniai gaunami grupei algebriniais būdais. Tarkime, realieji skaičiai gaunami iš racionaliųjų kaip Koši sekų aibės. Tai jau matematinės analizės sritis.

8.2. **Lauko charakteristika.** Anksčiau mes gavome baigtinius lyginių klasių žiedus $\mathbb{Z}_m$. Jų elementus žymėjome $\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}$, daugybos ir sudėties operacijas apibrėžėme formulėmis

$$\bar{k} + \bar{e} = \overline{k+e}$$
$$\bar{k}\bar{e} = \overline{ke}$$

Jei $m = st$, $s > 1$, $t > 1$, tai $\bar{s}\cdot\bar{t} = \bar{m} = \bar{0}$, t.y. $\bar{s}$ ir $\bar{t}$ - nulio dalikliai žiede $\mathbb{Z}_m$.

Tegul p - pirminis skaičius. Įrodysim, kad $\mathbb{Z}_p$ - laukas. Kai $p = 2, 3$ tai matosi iš daugybos lentelių. Bendru atveju užtenka rasti kiekvienam nenuliniam elementui $\bar{s} \in \mathbb{Z}_p$ atvirkštinį elementą $\bar{s}'$. Tegul $\bar{s} \neq 0$

Nagrinėsime elementus

$$\bar{s}, \overline{2s}, \dots, \overline{(p-1)s} \qquad (1)$$

visi jie nelygūs 0, kadangi

$$s \not\equiv 0 \pmod{p} \Rightarrow ks \not\equiv 0 \bmod p,$$

kai $k = 1, 2, \dots, p-1$. Čia panaudojama tai, kad p - pirminis. Be to visi (1) elementai skirtingi: jei $\overline{ks} = \overline{ls}$, $k < l$, tai $\overline{(k-l)s} = \bar{0}$, o tai neįmanoma. Taigi (1) aibė sutampa su

kokia tai buvo perstatyta aibė

$$\bar{1}, \bar{2}, \dots, \overline{p-1}$$

Akivaizdu atvejui rasis s', $1 \le s' \le p-1$ toks, kad $\overline{s's} = \bar{1}$. Bet tai reiškia, kad $\bar{s}'\bar{s} = \bar{1}$, t.y., $\bar{s}'$ yra elemento $\bar{s}$ atvirkštinis. Tokia buvo, įrodinė teoremą atvirkštinis. Tokia buvo, įrodinė teoremą

T. *Liekanų klasių aibė $\mathbb{Z}_m$ yra laukas tada ir tik tada, kai $m = p$ - pirminis skaičius.*

Išvada. (Mažoji Ferma teorema). *Bet kuriam sveikam skaičiui m, kuris nėra dalus iš p, yra teisingas lyginys*

$$m^{p-1} \equiv 1 \pmod p$$

Įrodymas. Kaip matome,

$$\{\bar{m}, \bar{2}\bar{m}, \dots, \overline{(p-1)}\,\bar{m}\} = \{\bar{1}, \bar{2}, \dots, \overline{p-1}\} \quad (2)$$

(1) lygybėje reikėtų spėlioti m ir parinkandoti $\overline{km} = \bar{k}\bar{m}$, $k = 1, 2, \dots, p-1$). Tai sudauginsime (2) lygybėje visus elementus kairėje pusėje ir visus elementus dešinėje, gausime

$$\left(\prod_{k=1}^{p-1} \bar{k}\right)\bar{m}^{p-1} = \prod_{k=1}^{p-1} \bar{k} \quad (3)$$

Kadangi $\mathbb{Z}_p$ - žiedas be nulio dalikliu, tai (3) lygybę galima supaprastinti iš $\prod_{k=1}^{p-1} \bar{k}$. Gausime $\bar{m}^{p-1} = 1$

Apibrėžimas. Laukas, neturintis tikrinių polaukių vadinamas *pirminiu lauku*.

Teorema. *Kiekviename lauke yra vienas ir tik vienas pirminis polaukis P_0. Šis pirminis laukas yra izomorfinis arba $\mathbb{Q}$ arba $\mathbb{Z}_p$, kur p - tam tikras pirminis skaičius.*

Įrodymas. Tarkime, turime du skirtingus pirminius laukus P' ir $P'' \in CP$. Tada ju sankirta $P' \cap P''$ - laukas, nes-tampantis nei su P' nei su P''. Tai neįmanoma, kadangi tie laukai pirminiai. Todėl pirminis laukas vienintelis.

Laukui P_0 priklauso elementas 1 ir visi jo kartotiniai

$$n \cdot 1 = 1 + 1 + \dots + 1.$$

Naudodamiesi žiedo elementų sudėties ir daugybos savybėmis gauname

$$s \cdot 1 + t \cdot 1 = (s+t)1, \quad (s \cdot 1)(t \cdot 1) = (st) \cdot 1; \quad s, t \in \mathbb{Z}$$

Todėl žiedo $\mathbb{Z}$ atvaizdavimas į P, apibrėžtas taisykle $f(n) = n \cdot 1$ yra homomorfizmas, o jo branduolys $\ker f = m\mathbb{Z}$. Jei $m = 0$, tai f - monomorfizmas ir tada trupmenos $(s \cdot 1)/(t \cdot 1)$ funkcijos pasako lauke P, sudaro lauką P_0, izomorfišką $\mathbb{Q}$. Tai ir bus lauko P pirminis polaukis.

Jei $m>0$, tai atvaizdavimas f^*, apibrėžtas taisykle

$$f^*: \bar{k} = \{k\}_m \to f(k)$$

bus izomorfinis įdėjimas $\mathbb{Z}_m \to P$.
Taciau $\mathbb{Z}_m$ - laukas tada ir tik tada, kada $m=p$ - pirminis. Tokiu būdu ~~$f^*(\mathbb{Z}_p)$~~ $f^*(\mathbb{Z}_p)$ - lauko P pirminis polaukis.

Apibrėžimas. Sakoma, kad laukas P turi charakteristiką nulį (yra nulinės charakteristikos), jeigu jo pirminis laukas P_0 izomorfinis $\mathbb{Q}$. Sakoma, kad laukas P turi pirminę (baigtinę) charakteristiką p, jeigu $P_0 \cong \mathbb{Z}_p$. Tai žymima $\operatorname{char} P = 0$ arba $\operatorname{char} P > 0$.

Kai kada nulinę charakteristiką vadina begaline. Tai siejama su elemento 1 eile adicinėje lauko P grupėje. Tokiu atveju baigtinė charakteristika p - tai nenulinio elemento eilė adicinėje grupėje

$$px = x+x+\dots+x = 1\cdot x+\dots 1\cdot x = (1+1+\dots+1)x = (p\cdot 1)x = 0$$

Galima napisyti baigtinius laukus nebūtinai kaip (liekanų klasių) laukus $\mathbb{Z}_p$. Abstrakčiai laukai iš p elementų žymimi $\mathbb{F}_p$ arba $GF(p)$ (Galois Field – Galua laukas). Reikia turėti omenyje, kad egzistuoja baigtiniai laukai $GF(q)$, $q = p^n$, p – pirminis, o n – bet kuris natūrinis skaičius.

Pvz. $GF(4) = \{0, 1, \alpha, \beta\}$

+	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

·	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α