Kai kurių algebrinių struktūrų priminimas

1 Kūnas ir tiesinė erdvė

- *Grupė* $(B, \times)$ — tai algebrinė struktūra, kuri tenkina savybes:
  - asociatyvumo: $(a \times b) \times c = a \times (b \times c)$
  - egzistuoja neutralus elementas $i \in B$: $a \times i = a$
  - $\forall a \in B, \exists \overline{a} \in B : a \times \overline{a} = i$
- Komutatyvumas: $a \times b = b \times a$.
- *Kūnas* (kartais vadinamas *lauku*) $(A, +, \times)$ — tai algebrinė struktūra, kuri tenkina savybes:
  - $(A, +)$ — komutatyvi grupė
  - $(A \backslash \{0\}, \times)$ — grupė
  - galioja distributyvumo dėsniai:
    - $a \times (b + c) = a \times b + a \times c$,
    - $(a + b) \times c = a \times c + b \times c$.

Tegu A — kūnas, $n \geq 1$ — sveikasis skaičius.

- Aibė $V \subset A^n$ vadinama *tiesine erdve virš* A, jei

$$v, u \in V \Rightarrow av + bu \in V \; \forall \, a, b \in A.$$

- Tiesinės erdvės V vektorių rinkinys $u_1, \ldots, u_s$ vadinamas tiesiškai nepriklausomu, jei

$$(a_1 u_1 + \cdots + a_s u_s = 0, a_i \in A \; \forall i) \Rightarrow (a_1 = \cdots = a_s = 0)$$

- Tiesinės erdvės V tiesiškai nepriklausomų vektorių rinkinys $u_1, \ldots, u_s$ vadinamas erdvės V *baze*, jei kiekvieną erdvės V vektorių galima išreikšti vektorių $u_1, \ldots, u_s$ tiesine kombinacija, t.y.

$$\forall v \in V \; \exists a_1, \ldots, a_s \in A : v = a_1 u_1 + \cdots + a_s u_s.$$

Teorema 1 *Tarkime, $V \subset A^n$ yra tiesinė erdvė. Tada V turi bazę, sudarytą iš ne daugiau kaip n vektorių. Jei ji sudaryta iš s vektorių, tai:*

1. *Bet kokia $s + 1$ vektoriaus iš V aibė yra tiesiškai priklausoma.*
2. *Kiekviena V bazė yra sudaryta iš s vektorių.*
3. *Bet kurie s tiesiškai nepriklausomi V vektoriai sudaro V bazę.*
4. *Kiekvienas tiesinės erdvės V vektorius* vienareikšmiškai *išreiškiamas bazės vektorių tiesine kombinacija.*

Erdvės V *dimensija*, žymima $\dim V$, yra bazės vektorių skaičius.

2 Baigtiniai kūnai

Šiame skyrelyje prisiminsime baigtinių kūnų (dar vadinamų Galua kūnais, angl. finite fields, Galois fields) pagrindines sąvokas.

- Kūną, turintį baigtinį skaičių elementų, vadinsime *baigtiniu kūnu*. Baigtinį kūną, turintį q elementų, žymėsime $\mathbb{F}_q$ (kartais jis dar žymimas $GF(q)$).
- Sveikųjų skaičių moduliu p (p - pirminis skaičius) aibė sudaro baigtinį kūną iš p elementų

  $$\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\},$$

  vadinamą *pirminiu kūnu*. Jame operacijos atliekamos moduliu p. Pavyzdžiui, *dvinariame* kūne $\mathbb{F}_2 = \{0, 1\}$ gauname, kad $1 + 1 = 0$.
- Jei p nėra pirminis, sveikųjų skaičių moduliu p aibė nėra kūnas.
- Baigtinis kūnas iš q elementų egzistuoja tada ir tik tada, kai $q = p^m$, kur p — pirminis, $m \geq 1$. Visi baigtiniai kūnai, turintys q elementų, yra izomorfiški, todėl galima laikyti, kad toks kūnas yra vienintelis.
- Visi baigtiniai kūnai yra komutatyvūs, t.y. daugyba yra komutatyvi.
- Skaičius p yra kūno $\mathbb{F}_{p^m}$ *charakteristika*, t.y. mažiausias toks sveikas skaičius s, kad $\underbrace{1 + \cdots + 1}_{s} = 0$. Jei p yra kūno K charakteristika, tai $p\beta = 0$ visiems $\beta \in K$. Pavyzdžiui, $2\beta = 0$ visiems $\beta \in \mathbb{F}_2$. Be viso kito, tai reiškia, kad

  $$(\beta + \gamma)^p = \beta^p + \gamma^p \; \forall \beta, \gamma \in \mathbb{F}_{p^m}.$$

  Pagal indukciją gauname

  $$(\beta + \gamma)^{p^i} = \beta^{p^i} + \gamma^{p^i} \; \forall \beta, \gamma \in \mathbb{F}_{p^m} \; \forall i \geq 1.$$

- Kūnas $\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$ yra kūno $\mathbb{F}_{p^m}$ poaibis. Kūnas $\mathbb{F}_{p^m}$ yra tiesinė erdvė virš $\mathbb{F}_p$, $\dim \mathbb{F}_{p^m} = m$. Jei $\beta_0, \beta_1, \cdots, \beta_{m-1}$ yra erdvės $\mathbb{F}_{p^m}$ bazė virš $\mathbb{F}_p$, tai

  $$\mathbb{F}_{p^m} = \{a_0\beta_0 + a_1\beta_1 + \cdots + a_{m-1}\beta_{m-1} \mid a_i \in \mathbb{F}_p \; \forall i\}.$$

- Aibė $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ yra ciklinė multiplikacinė grupė, t.y.

  $$\exists \alpha \in \mathbb{F}_q^* : \mathbb{F}_q^* = \{1, \alpha, \alpha^2, \cdots, \alpha^{q-2}\}, \alpha^{q-1} = 1.$$

  Toks α yra vadinamas *primityviu kūno* $\mathbb{F}_q$ *elementu* (jis nebūtinai yra vienintelis). Ši baigtinio kūno elementų išraiška leidžia lengvai dauginti ir dalinti: dauginant (dalinant) du ciklinės grupės elementus pakanka sudėti (atimti) jų laipsnių rodiklius (moduliu $q - 1$).

- Jei $\alpha \in \mathbb{F}_{p^m}$ yra primityvus elementas, tai $\{1, \alpha, \alpha^2, \cdots, \alpha^{m-1}\}$ yra kūno $\mathbb{F}_{p^m}$ bazė virš $\mathbb{F}_p$, todėl

$$\mathbb{F}_{p^m} = \{a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} \mid a_i \in \mathbb{F}_p \ \forall i\}.$$

  Ši baigtinio kūno elementų išraiška leidžia lengvai sudėti ir atimti: sudedame (atimame) panariui koeficientus prie α laipsnių. Koeficientus sudėti (atimti) mokame, nes jie priklauso kūnui $\mathbb{F}_p$. Praktikoje į elementą $a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1}$ patogu žiūrėti kaip į vektorių $(a_0, a_1, \ldots, a_{m-1}) \in \mathbb{F}_p^m$, ir veiksmus atlikti su vektoriais.

  Jei galėtume nesunkiai pereiti nuo vienos baigtinio kūno elementų išraiškos prie kitos, tai galėtume elementus ir sudėti (atimti), ir dauginti (dalinti). Netrukus pamatysime, kaip tai padaryti. Bet prieš tai — dar viena baigtinio kūno elementų išraiška.

- Jei $f(x)$ yra pirminis m-tojo laipsnio polinomas virš $\mathbb{F}_p$, tai $\mathbb{F}_{p^m}$ yra izomorfiškas faktoržiedžiui $\mathbb{F}_p[x]/(f(x))$ (prisiminkime, kad faktoržiedis $\mathbb{F}_p[x]/(f(x))$ yra polinomų virš $\mathbb{F}_p$ dalybos iš $f(x)$ liekanų aibė, kurioje veiksmai atliekami moduliu $f(x)$). Taigi, galime laikyti, kad

$$\mathbb{F}_{p^m} = \{g(x) = g_0 + g_1 x + \cdots + g_{m-1}x^{m-1} \mid g_i \in \mathbb{F}_p \ \forall i\},$$

  ir veiksmai atliekami $\bmod f(x)$.

- Visiems p — pirminiams ir $m \geq 1$ egzistuoja toks pirminis m-tojo laipsnio polinomas $f(x) \in \mathbb{F}_p[x]$, kurio šaknis yra kūno $\mathbb{F}_{p^m}$ primityvus elementas α, t.y. $f(\alpha) = 0$. Toks polinomas vadinamas *primityviu polinomu* (jis nebūtinai yra vienintelis).

- Primityvus polinomas $f(x)$ leidžia susieti dvi baigtinio kūno $\mathbb{F}_{p^m}$ elementų išraiškas, tiksliau, leidžia primityvaus elemento laipsnius $\alpha^m, \alpha^{m+1}, \ldots, \alpha^{p^m-2}$ išreikšti bazės $1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{m-1}$ vektorių tiesine kombinacija. Iš tikro, tegu $f(x) = f_0 + f_1 x + \cdots + f_m x^m$, $f_i \in \mathbb{F}_p \ \forall i$. Kadangi $f(\alpha) = 0$, tai $f_0 + f_1\alpha + \cdots + f_m\alpha^m = 0$. Iš čia gauname, kad $\alpha^m = -\frac{1}{f_m}(f_0 + f_1\alpha + \cdots + f_{m-1}\alpha^{m-1})$ — išreiškėme bazės vektorių tiesine kombinacija. Aukštesnius α laipsnius išreiškiame taip pat, pavyzdžiui, $\alpha^{m+1} = \alpha^m\alpha$, įstatome gautą α^m išraišką ir t.t.

- Nors primityvių polinomų yra ne vienas ir visi jie gali būti naudojami veiksmams su baigtinio kūno elementais, yra tam tikri „standartiniai“ primityvūs polinomai, kurie paprastai ir yra naudojami. 1 lentelėje pateikiame kelis jų pavyzdžius mažiems p ir m.

Pavyzdys 1 Sudarykime kūną $\mathbb{F}_8$. Matome, kad $p = 2$, $m = 3$ (nes $8 = 2^3$). Žinome, kad $\mathbb{F}_8^* = \{1, \alpha, \alpha^2, \cdots, \alpha^6\}$, $\alpha^7 = 1$, kur α yra kūno $\mathbb{F}_8$ primityvus elementas. Tai leidžia dauginti kūno $\mathbb{F}_8$ elementus, pavyzdžiui, $\alpha^2\alpha^3 = \alpha^5$, $\alpha^3\alpha^6 = \alpha^9 = \alpha^7\alpha^2 = \alpha^2$ (kad $\alpha^9 = \alpha^2$, galėjome pasakyti iš karto, nes rodiklių skaičiavimai vyksta moduliu $q - 1$, t.y. $\bmod 7$). Be abejo, $0 \cdot \alpha^i = 0 \ \forall i$.

Be to, žinome, kad $\{1, \alpha, \alpha^2\}$ yra kūno $\mathbb{F}_8$ bazė virš $\mathbb{F}_2$, todėl

$$\begin{aligned} \mathbb{F}_8 &= \{a_0 + a_1\alpha + a_2\alpha^2 \mid a_i \in \mathbb{F}_2 \ \forall i\} \\ &= \{0, 1, \alpha, 1+\alpha, \alpha^2, 1+\alpha^2, \alpha+\alpha^2, 1+\alpha+\alpha^2\}. \end{aligned}$$

Tai leidžia lengvai sudėti ir atimti, pavyzdžiui, $(1+\alpha) + (\alpha+\alpha^2) = 1 + 2\alpha + \alpha^2 = 1 + \alpha^2$ (nes kūno $\mathbb{F}_8$ charakteristika yra $p = 2$, t.y. $1 + 1 = 2 = 0$ ir $-1 = 1$).

p	Primityvūs polinomai	p	Primityvūs polinomai
2	$x+1$	3	x^4+x^3+2
	x^2+x+1		$x^5+x^4+x^2+1$
	x^3+x+1		x^6+x^5+2
	x^4+x+1	5	x^2+x+2
	x^5+x^2+1		x^3+x^2+2
	x^6+x+1		x^4+x^3+x+3
	x^7+x+1	7	x^2+x+3
	$x^8+x^4+x^3+x^2+1$		x^3+x^2+x+2
	x^9+x^4+1	11	x^2+x+7
	$x^{10}+x^3+1$	13	x^2+x+2
3	$x+1$	17	x^2+x+10
	x^2+x+2	19	x^2+x+2
	x^3+2x^2+1	23	$x^2+22x+19$

Lentelė 1: Primityvūs polinomai

Kad galėtume pereiti nuo vienos išraiškos prie kitos, pasinaudosime primityviu polinomu iš 1 lentelės. Matome, kad, kai $p=2$ ir $m=3$, galime naudoti primityvų polinomą $f(x)=x^3+x+1$. Primityvus elementas α yra jo šaknis, t.y. $f(\alpha)=0$, todėl $\alpha^3+\alpha+1=0$. Iš čia $\alpha^3=-\alpha-1=\alpha+1$ — išreiškėme bazės vektorių tiesine kombinacija.

Tada

$$\begin{aligned}\alpha^4 &= \alpha^3\alpha=(\alpha+1)\alpha=\alpha^2+\alpha,\\ \alpha^5 &= \alpha^4\alpha=(\alpha^2+\alpha)\alpha=\alpha^3+\alpha^2=\alpha+1+\alpha^2,\\ \alpha^6 &= \alpha^5\alpha=(\alpha+1+\alpha^2)\alpha=\alpha^2+\alpha+\alpha^3=\alpha^2+\alpha+\alpha+1=\alpha^2+1.\end{aligned}$$

Žinome, kad $\alpha^7=1$. Patikrinkime, ar iš tikrųjų:

$$\alpha^7=\alpha^6\alpha=(\alpha^2+1)\alpha=\alpha^3+\alpha=\alpha+1+\alpha=1.$$

Taigi, dabar, atlikdami veiksmus su kūno $\mathbb{F}_8$ elementais, lengvai galime pereiti nuo vienos išraiškos prie kitos. Pavyzdžiui, $\alpha^4+\alpha^6=(\alpha^2+\alpha)+(\alpha^2+1)=\alpha+1=\alpha^3$.

Kaip buvo pastebėta, į elementą $a_0+a_1\alpha+a_2\alpha^2$ patogu žiūrėti kaip į vektorių $(a_0,a_1,a_2)\in\mathbb{F}_2^3$, ir veiksmus atlikti su vektoriais. Pavyzdžiui, elementą $\alpha^2+\alpha$ atitinka vektorius 011. Programuojant veiksmus su nedideliais baigtiniais kūnais, patogu pasidaryti lentelę, kuri susietų primityvaus elemento α laipsnius su tokiais vektoriais. Tada du elementai bus sudauginami, sudedant jų laipsnių rodiklius, o norint sudėti du elementus, lentelėje bus surandami juos atitinkantys vektoriai, sudedami (moduliu p), o rezultatas vėl paverčiamas α laipsniu. Pavyzdžiui, $\alpha^4+\alpha^6\to 011+101=110\to\alpha^3$.

Reziumuodami 2 lentelėje pateikiame kūno $\mathbb{F}_8$ elementų išraiškas. Pirmame stulpelyje yra primityvaus elemento α laipsnis, antrame — jo išraiška bazės $\{1,\alpha,\alpha^2\}$ vektorių tiesine kombinacija, ir trečiame — atitinkamas vektorius iš $\mathbb{F}_2^3$.

Pavyzdys 2 Panagrinėkime kūną $\mathbb{F}_9$. Kadangi $9=3^2$, tai $p=3$ ir $m=2$. Taigi, $\mathbb{F}_3=\{0,1,2\}$ yra kūno $\mathbb{F}_9$ poaibis ($2+2=4=1$, $3=0$, $-1=2$, $-2=1$). Taip pat žinome, kad $\mathbb{F}_9^*=\{1,\alpha,\alpha^2,\cdots,\alpha^7\}$, $\alpha^8=$

0	0	000
1	1	100
α	α	010
α^2	α^2	001
α^3	$1+\alpha$	110
α^4	$\alpha+\alpha^2$	011
α^5	$1+\alpha+\alpha^2$	111
α^6	$1+\alpha^2$	101

Lentelė 2: K$\bar{\text{u}}$no $\mathbb{F}_8$ elementai

0	0	00
1	1	10
α	α	01
α^2	$1+2\alpha$	12
α^3	$2+2\alpha$	22
α^4	2	20
α^5	2α	02
α^6	$2+\alpha$	21
α^7	$1+\alpha$	11

Lentelė 3: K$\bar{\text{u}}$no $\mathbb{F}_9$ elementai

1, kur α yra k$\bar{\text{u}}$no $\mathbb{F}_9$ primityvus elementas. Be to, $\{1, \alpha\}$ yra k$\bar{\text{u}}$no $\mathbb{F}_9$ bazė virš $\mathbb{F}_3$, todėl

$$\begin{aligned}\mathbb{F}_9 &= \{a_0 + a_1\alpha \mid a_i \in \mathbb{F}_3 \ \forall i\} \\ &= \{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\}.\end{aligned}$$

Primityvus polinomas (iš 1 lentelės) b$\bar{\text{u}}$tų $f(x) = x^2+x+2$, taigi, $\alpha^2+\alpha+2 = 0$ ir $\alpha^2 = -\alpha-2 = 2\alpha+1$. Toliau

$$\begin{aligned}\alpha^3 &= \alpha^2\alpha = (2\alpha+1)\alpha = 2\alpha^2+\alpha = 2(2\alpha+1)+\alpha = 4\alpha+2+\alpha = 2\alpha+2, \\ \alpha^4 &= \alpha^3\alpha = (2\alpha+2)\alpha = 2\alpha^2+2\alpha = 2(2\alpha+1)+2\alpha = 4\alpha+2+2\alpha = 2, \\ \alpha^5 &= \alpha^4\alpha = 2\alpha, \\ \alpha^6 &= \alpha^5\alpha = 2\alpha^2 = 2(2\alpha+1) = \alpha+2, \\ \alpha^7 &= \alpha^6\alpha = (\alpha+2)\alpha = \alpha^2+2\alpha = 2\alpha+1+2\alpha = \alpha+1.\end{aligned}$$

Dabar galime atlikti veiksmus su k$\bar{\text{u}}$no $\mathbb{F}_9$ elementais. Pavyzdžiui, $\alpha^3\alpha^6 = \alpha^9 = \alpha$, $(\alpha^2)^{-1} = \alpha^{-2} = \alpha^6$ (nes rodiklių veiksmai atliekami moduliu 8), $\alpha^6 - \alpha^3 = (\alpha+2) - (2\alpha+2) = \alpha+2-2\alpha-2 = -\alpha = 2\alpha = \alpha^5$, ir pan.

3 lentelėje pateikiame k$\bar{\text{u}}$no $\mathbb{F}_9$ elementus.