Sissejuhatus

Miks on tarvis lõplikke korpusi, kui on olemas $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$?

- Andmed tekivad diskreetsetena või muudetakse diskreetseteks.
  byte, int, float, double
  Paljudel juhtudel jäävad arvutused, kasutajale nähtamatuks.
- Reaalselt osatakse realiseerida vaid $+, -, \cdot, \square^{-1}$, ülejäänud operaatorid on defineeritud nende abil.
- Arvutused ratsionaalarvudega on $\mathcal{O}(N^2)$, küllalt tihti esineb esineb vahetulemuste piiramatu kasv $\sum_{k=0}^{2^n}(-1)^k\binom{2^n}{k} = 0$.
- Lõplikud korpused pole pidevad – funktsioonide nullkohtade leidmine on raske.

Teoreem 1. *Lõpliku korpuse K karakteristika $p = \operatorname{char} K$ on algarv ja $\langle 1 \rangle \cong \mathbb{Z}_p$*

<table>
<tr><th>Korpuse aksioomid</th><th>Vektoruumi aksioomid</th></tr>
<tr><td colspan="2" align="center">$(K;+)$ on Abeli rühm</td></tr>
<tr><td colspan="2" align="center">$a(b+c) = ab + ac$</td></tr>
<tr><td colspan="2" align="center">$(a+b)c = ac + bc$</td></tr>
<tr><td colspan="2" align="center">$(ab)c = a(bc)$</td></tr>
<tr><td colspan="2" align="center">$1a = a$</td></tr>
<tr><td align="center">$ab = ba$</td><td align="center">–</td></tr>
<tr><td align="center">$a \neq 0 \Rightarrow \exists a^{-1}$</td><td align="center">–</td></tr>
</table>

Lõplik korpus on vektorruum üle iseenda või suvalise alamkorpuse(näit. üle $\mathbb{Z}_p$). Tehted lõplikus korpuses määrab baas. Tehete keerukus sõltub baasist.

Korpuse laiendamine. Minimaalne polünoom

Korpuste laiendamine on võimalik kahte moodi.

- Lisame elemendi, koos taandamisreegliga. Et tulemuseks oleks korpus, peab reegel täitma teatud tingimusi.

  Näited

$\mathbb{Z}_2(\alpha)\ :\ \alpha^2+\alpha+1=0$		
$\times$	α	$\alpha+1$
α	$\alpha+1$	1
$\alpha+1$	1	α

  Baase on täpselt 2
  $B_1=\{1,\alpha\}$
  $B_2=\{1,\alpha+1\}$

  Laiend $\mathbb{Z}_2(\beta)\ :\ \beta^3+\beta^2+\beta+1=0$ pole korpus, sest $(\beta+1)(\beta^2+1)=\beta^3+\beta^2+\beta+1=0$!

  Järeldus 1. *Olgu $f\in K[X]$ polünoom, siis laiend $K(\alpha)$: $f(\alpha)=0$ on korpus parajasti siis, kui f on taandumatu polünoom üle K.*

- Algebraline lähenemine võtame, suurema korpuse $K\subseteq L$ elemendi α ja moodustame minimaalse korpuse $K(\alpha)$, mis sisaldab elementi α.

  Definitsioon 1. *Korpuse laiendi $L:K$ elemendi α minimaalne polünoom $m_\alpha\in K[X]$ on vähima astmega unitaarne polünoom, mille juureks on α.*

  Järeldus 2. *Elemendi α minimaalne polünoom m_α jagab kõiki polünoome, mille juureks on α.*

  Teoreem 2 (Kroneckeri teoreem). *Kui polünoom $m\in K[X]$ on taandumatu, siis $L=K[X]/(m)$ on korpus ja $m(\overline{x})=0$.*

Lähenemiste samaväärsus. Laiendi mõõde

Järeldus 3. *Kui $m_\alpha \in K[X]$ on elemendi α minimaalne polünoom, siis $K(\alpha) \cong K[X]/(m)$.*

Järeldus 4. *Kui $m_\alpha \in K[X]$ on elemendi α minimaalne polünoom, siis $[K(\alpha) : K] = \deg m_\alpha$.*

Teoreem 3. *Olgu meil laiendite ahel $K \subseteq L \subseteq M$, siis $[M : K] = [M : L][L : K]$.*

Lõplike korpuste kirjeldus

Teoreem 4 (Lahutuskorpuse ühesuse teoreem). *Igal mittkonstantsel polünoomil leidub lahutuskorpus ja see on ühene isomorfismi täpsuseni.*

Teoreem 5. *Iga lõplik kaldkorpus K on korpus ehk iga $f, g \in K[X]$ ja iga $\alpha \in K$ väärtustus $fg(\alpha) = f(\alpha)g(\alpha)$.*

Teoreem 6 (Lagrange teoreem). *Lõpliku rühma G iga elemendi α järk on rühma elementide arvu jagaja ehk* $\mathrm{ord}(a) \mid |G|$.

Teoreem 7. *Kui lõpliku korpuse K karakteristika on p, siis leidub $n \in \mathbb{N}$ nii, et $|K| = p^n$.*

Teoreem 8 (Ühesuse teoreem). *Iga $q = p^n$ korral leidub isomorfismi täpsuseni vaid üks lõplik korpus $\mathbb{F}_q$, kusjuures see on polünoomi $X^q - X$ lahutuskorpus.*

Järeldus 5. *Olgu meil taandumatu n-astme polünoom $m \in K[X]$, siis $K(\alpha) : m(\alpha) = 0$ on m lahutuskorpus.*

Multiplikatiivne rühm. Diskreetne logaritm

Kas leidub korpuse K element ξ, mille astmed moodustaksid K^*?

Algoritm (Naiivne algoritm). *Sisend K, q väljund rühma moodustaja ξ.*

1. Võtta $\alpha \in K^*$, kui $\mathrm{ord}(\alpha) = q - 1$ väljastada α.
2. Võtta $\beta \in K^*$, leida γ nii, et $\mathrm{ord}(\gamma) = \mathrm{lcm}(\mathrm{ord}(\alpha), \mathrm{ord}(\beta))$.
3. Kui $\mathrm{ord}(\gamma) = q - 1$, siis väljastada γ muidu korrata sammu 2 võttes $\alpha = \gamma$.

Teoreem 9. *Kui kommutatiivses rühmas G on elemendid järkudega m ja n, siis leidub element järguga $\mathrm{lcm}(m, n)$.*

Järeldus 6. *Lõpliku korpuse multiplikatiivses rühmas leidub suurima järguga element ξ, mille järk on $|K^*|$.*

Olgu meil $\alpha \neq 0$. Mis on $\log_\alpha \beta$?
Näide

$\mathbb{Z}_2(\alpha)\ :\ \alpha^3 + \alpha + 1 = 0$			
∞	0	3	$\alpha + 1$
0	1	4	$\alpha^2 + \alpha$
1	α	5	$\alpha^2 + \alpha + 1$
2	α^2	6	$\alpha^2 + 1$

Rakendused:

- Diffie-Hellmani võtmevahetus, El Gamal krüptosüsteem, täisarvude tegurdamine.
- Juurimine, madala astmega võrrandite lahendamine.
- Kiire korrutamine tabelit kasutades.

Galois rühm

Definitsioon 2. *Laiendi $L : K$ isomorfismiks nimetatakse kujutust, mis on kooskõlas korpuse tehetega ja mille ahend korpusel K on samasus. Kõik laiendite isomorfismid moodustavad Galois' rühma G.*

Järeldus 7. *Iga laiendte $L : K$ isomorfismi ja $p \in K[X]$ korral $\varphi(p(\alpha)) = p(\varphi(\alpha))$ ehk isomorfism viib polünoomi juured juurteks.*

Teoreem 10 (Lõpliku laiendi normaalsus). *Lõpliku laiendi $(\mathbb{F}_q)^n : \mathbb{F}_q$ element $\alpha \in \mathbb{F}_q$ parajasti siis, kui $\sigma(\alpha) = \alpha^q = \alpha$, kusjuures σ on isomorfism.*

Teoreem 11. *Lõpliku korpuse $(\mathbb{F}_q)^n : \mathbb{F}_q$ Galois' rühm on tsükliline $G = \langle \sigma \rangle$, kus $\sigma(\alpha) = \alpha^q$.*

- Isomorfism τ on ühesel määratud moodustaja ξ poolt $\tau(\xi)$.
- Element $\tau(\xi)$ peab olema primitiivne.
- Seosest $\tau(\xi) = \xi^l$ järeldub $\alpha(a) = a^l$.

Teoreem 12 (Lihtsustatud Galois' teoreem). *Lõplike korpuste lõplike laiendite korral kehtib $[L : K] = |G|$.*

Laiendi $(\mathbb{F}_q)^n : \mathbb{F}_q$ Galois' rühmaga seotud suurused jälg ja norm

$$Tr(\alpha) = \sum_{g \in G} g(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i}, \; N(\alpha) = \prod_{q \in G} g(\alpha) = \prod_{i=0}^{n-1} \alpha^{q^i}$$

Mõlemad on teisendused $Tr, N : (\mathbb{F}_q)^n \to \mathbb{Z}_q$.

Erinevad baasid. Tehete keerukus

- Baasielementide korrutiste kuju määrab ära korrutamise reeglid. Olgu $\alpha_i\alpha_j = \sum_{k=0}^{n-1} t_{ij}^{(k)}\alpha_k$, siis vektori $C = A \cdot B$ komponendid saab leida maatriksite abil $C_k = AT_kB^T$
- Kui kasutame lihtsat baasi $\left\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\right\}$, siis tuleb realiseerida kõik maatrisid T_k.
- Kasutades tsüklilisest moodustajast saadud baasi $\left\{1, \beta, \ldots \beta^{q^{n-1}}\right\}$ tuleb realiseerida vaid üks maatriks T.
- Mida vähem on vastavas maatriksis T nullist erinevaid elemente, seda parem.

Duaalset ruumi $\left((\mathbb{F}_q)^n\right)^*$ on lihtne samastada korpuse endaga $(\mathbb{F}_q)^n$.

Definitsioon 3. *Olgu meil samastus* $\alpha \rightarrowtail f_\alpha \in \left((\mathbb{F}_q)^n\right)^*$, *siis baasi* $(\alpha_i)_{i=0}^{n-1}$ *duaalne baas* $(\beta_j)_{j=0}^{n-1}$ *parajasti siis, kui* $f_{\alpha_i}(\beta_j) = \delta_{ij}$.