

Bevezetés a Számításelméletbe II. 12. előadás

Sali Attila

Budapest Műszaki és Gazdaságtudományi Egyetem
Számítástudományi Tsz.

I. B. 137/b

`sali@cs.bme.hu`

2002 április 30.

Cayley tétel

1. Definíció. Az n elemű halmaz permutációinak csoportját S_n -el jelöljük. Az S_n **szimmetrikus csoport** részcsoportjait n -ed fokú **permutációcsoportoknak** nevezzük.

2. Tétel (Cayley). Minden csoport izomorf egy permutációcsoporttal.

Tehát elég lenne a permutáció csoportokat vizsgálni.

Cél: $G \simeq H \leq S_G (\implies G \simeq H' \leq S_{|G|})$

Legyen

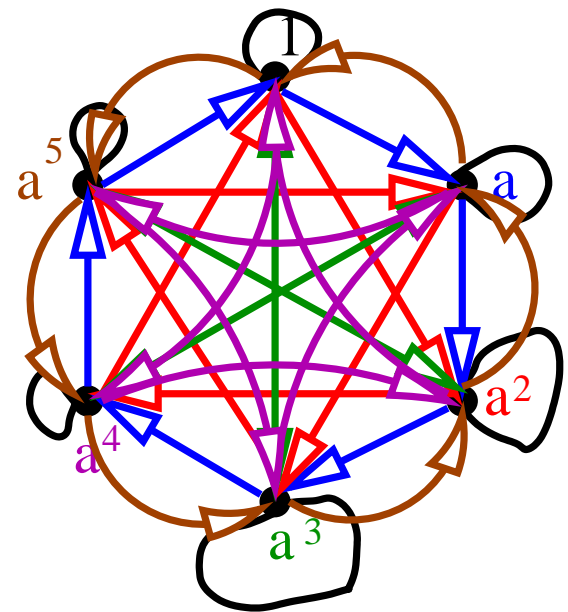
$$\begin{aligned} \phi: G &\rightarrow S_G \\ h &\rightarrow \begin{pmatrix} g \\ gh \end{pmatrix} \end{aligned}$$

ϕ minden $h \in G$ -hez G elemeinek azt a permutációját rendeli, amely bármely g -t annak h -szorosára, gh -ra képezi.

$g_1h = g_2h$ esetén $g_1 = g_2 \implies \phi$ tényleg permutáció. ϕ injektív, hiszen minden permutáció mást rendel a csoport egységeleméhez.

ϕ művelettartó, mert

$$\phi(h_1)\phi(h_2) = \begin{pmatrix} g \\ gh_1 \end{pmatrix} \begin{pmatrix} g \\ gh_2 \end{pmatrix} = \begin{pmatrix} g \\ gh_1h_2 \end{pmatrix} = \phi(h_1h_2).$$



Cayley-tábla

Példa: $G = D_4$

3. Definíció. Legyen

$G = \{g_1, g_2, \dots, g_n\}$ csoport. Ekkor azt az $n \times n$ -es táblázatot, amely i -edik sorának j -edik oszlopában $g_i g_j$ áll, a csoport **Cayley-táblázatának** nevezzük.

D_4	1	f	f^2	f^3	t_1	t_2	t_3	t_4
1	1	f	f^2	f^3	t_1	t_2	t_3	t_4
f	f	f^2	f^3	1	t_4	t_1	t_2	t_3
f^2	f^2	f^3	1	f	t_3	t_4	t_1	t_2
f^3	f^3	1	f	f^2	t_2	t_3	t_4	t_1
t_1	t_1	t_2	t_3	t_4	1	f	f^2	f^3
t_2	t_2	t_3	t_4	t_1	f^3	1	f	f^2
t_3	t_3	t_4	t_1	t_2	f^2	f^3	1	f
t_4	t_4	t_1	t_2	t_3	f	f^2	f^3	1

Kvaterniócsoport

$Q = \{1, -1, i, j, k, -i, -j, -k\}$
 ahol $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$ vala-
 mint minden $g \in Q$ -ra
 $(-1)g = g(-1) = -g$.
 Ezekből az összefüggésekből
 bármely két elem szorzata
 kiszámítható. Például:

$$\begin{aligned}
 ji &= ji1 = ji(-1)(-1) = \\
 &= jij^2(-1) = j(ij)j(-1) = \\
 &= (jk)j(-1) = ij(-1) = \\
 &= k(-1) = -k
 \end{aligned}$$

A csoport Cayley-táblázata:

Q	1	-1	i	j	k	$-i$	$-j$	$-k$
1	1	-1	i	j	k	$-i$	$-j$	$-k$
-1	-1	1	$-i$	$-j$	$-k$	i	j	k
i	i	$-i$	-1	k	$-j$	1	$-k$	j
j	j	$-j$	$-k$	-1	i	k	1	$-i$
k	k	$-k$	j	$-i$	-1	$-j$	i	1
$-i$	$-i$	i	1	$-k$	j	-1	k	$-j$
$-j$	$-j$	j	k	1	$-i$	$-k$	-1	i
$-k$	$-k$	k	$-j$	i	1	j	$-i$	-1

$D_4 \not\cong Q$, mert Q -ban **hat** negyedren-
 dű elem van ($i, j, k, -i, -j, -k$), D_4 -
 ben **kettő** (f, f^3).

Gyűrűk ura

4. Definíció. Az R halmaz $+$ és \cdot műveletekkel **gyűrű**, ha

1. $(R, +)$ Abel csoport;

2. (R, \cdot) félcsoport;

3. $(a + b) \cdot c = a \cdot c + b \cdot c \quad \forall a, b, c \in R$ esetén;

4. $c \cdot (a + b) = c \cdot a + c \cdot b \quad \forall a, b, c \in R$ esetén.

(3)-at és (4)-et jobboldali illetve baloldali *disztributív* törvénynek nevezzük.

Ha a szorzás is kommutatív, *kommutatív gyűrűről*, ha van a szorzásra nézve egységelem, *egységelemes gyűrűről* beszélünk.

A + egységelemét *nullelemnek* nevezzük és 0-val jelöljük.

Egy a R -beli elem +-ra vonatkozó inverzét *ellentettnek* hívjuk, és $-a$ -val jelöljük. Az $a - b = a + (-b)$ műveletet *kivonásnak* nevezzük.

Egyszerű következmények

5. Állítás. Legyen R gyűrű, $a, b \in R$

1. 0 nullelem és az ellentett egyértelmű; 2. $0a = a0 = 0$;
3. $(-a)b = -ab$; 4. $(-a)(-b) = ab$.

BIZONYÍTÁS 1.: R Abel-csoport az összeadásra.

2.: Adjuk $a0 = a(0 + 0) = a0 + a0$ mindkét oldalához $a0$ inverzét.

3.: $ab + (-a)b = (a - a)b = 0b = 0$.

4.: 3. alapján $(-a)(-b) = -(a(-b)) = -(-ab) = ab$.

Példák

1. Az egész számok kommutatív, egységelemes gyűrűt alkotnak a szokásos összeadásra és szorzásra. Jele \mathbb{Z} .
2. Az m -mel osztható egész számok kommutatív, egységelemes gyűrűt alkotnak a szokásos műveletekre.
3. A $\text{mod } m$ maradékosztályok a \mathbb{Z}_n gyűrűt alkotják a szokásos műveletekkel.
4. A racionális, a valós, a komplex számok kommutatív, egységelemes gyűrűt alkotnak a szokásos műveletekre.

5. Az $n \times n$ -es komplex (valós, racionális, egész) mátrixok egységelemes *nemkommutatív* gyűrűt alkotnak a mátrixösszeadásra és mátrixszorzásra. Az egységelem az egységmátrix.

6. Egy H halmaz részhalmazai az

$$A + B = (A \cup B) \setminus (A \cap B) \text{ és } AB = A \cap B$$

műveletekre kommutatív gyűrűt alkotnak. A nullelem az üres halmaz, az egységelem maga a H . Tetszőleges $a \in R$ esetén $a^2 = a$. Az ezzel a tulajdonsággal rendelkező gyűrűt *Boole-gyűrűnek* nevezzük. Az ilyen gyűrűkben az $a + a = 0$ egyenlőség is teljesül.

7. A komplex (valós, racionális, egész) együtthatós polinomok gyűrűt alkotnak a polinomösszeadásra és szorzásra. Jelölése $\mathbb{C}[x]$ ($\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}[x]$).

8. Az $a + b \cdot i$, $a, b \in \mathbb{Z}$ alakú komplex számok alkotják a *Gauss-egészek* gyűrűjét. Ebben is van egyértelmű prímtenyezős felbontás.

$$(2 = (1 + i)(1 - i))$$

Nullosztók

6. Definíció. Legyen R gyűrű. Az $0 \neq a \in R$ elemet jobboldali (baloldali) **nullosztónak** nevezzük, ha van hozzá $0 \neq b \in R$, hogy $ab = 0$ ($ba = 0$).

Van baloldali nullosztó \iff van jobboldali is.

7. Definíció. Az R gyűrűt **nullosztómentesnek** nevezzük, ha nincs benne nullosztó. A kommutatív nullosztómentes gyűrű neve **integritási tartomány**.

Példák

1. Az egész számok, a páros számok gyűrűje integritási tartomány.
2. \mathbb{Z}_6 -ban $2 \cdot 3 = 0$, ezért a 2 illetve a 3 nullosztók.
3. Egy $n \times n$ -es A mátrix baloldali nullosztó, ha az $AB = 0$ mátrixegyenletnek van 0-tól különböző megoldása, ami ekvivalens az-
zal, hogy az $A\underline{x} = 0$ lineáris egyenletrendszernek van nemtriviális meg-
oldása, azaz, ha A nem invertálható. Ugyanezzel ekvivalens az, hogy
 A jobboldali nullosztó.
4. A H halmaz részhalmazai az $A + B = (A \cup B) \setminus (A \cap B)$ és $AB = A \cap B$
műveletek esetén tartalmaz nullosztót. $A(H \setminus A) = 0$, mivel $A \cap (H \setminus$
 $A) = \emptyset$.

Részgyűrűk

Egy R gyűrű *részgyűrűje* az R' , ha *részstruktúrája*.

8. Állítás. Legyen R gyűrű. Az $R' \subseteq R$ halmaz R részgyűrűje, ha zárt a műveletekre és minden elemmel együtt benne van annak ellentettje is.

Példák

1. Az egész számok részgyűrűjét alkotják az m -mel osztható egész számok. De \mathbb{Z}_n nem!
2. A racionális számok részgyűrűje a valós, a valós számok részgyűrűje a komplex számok gyűrűjének.
3. Az $n \times n$ -es komplex (valós, racionális, egész) mátrixok részgyűrűjét alkotják azon mátrixok, amelyeknek az utolsó sora és utolsó oszlopa 0.

9. Állítás. \mathbb{Z} minden $\{0\}$ -től különböző részgyűrűje az (1) példában leírt módon kapható.

BIZONYÍTÁS Legyen $R \leq \mathbb{Z}$. Ekkor $(R, +) \leq (\mathbb{Z}, +)$, mint csoportok. $(\mathbb{Z}, +)$ ciklikus csoport (a végtelen ciklikus csoport), így minden részcsoportja is ciklikus. Tehát $(R, +) = \langle m \rangle$, azaz R pont az m többszöröseiből áll.

Testek

10. Definíció. Egy R egységelemes gyűrűt **ferdetestnek** hívunk, ha a szorzásra nézve is van inverz, azaz $\forall 0 \neq a \in R$ -hez $\exists a' \in R$, hogy $aa' = 1$. Egy ferdetestet **testnek** nevezünk, ha a szorzás kommutatív.

Azaz R test, ha $R \setminus \{0\}$ Abel-csoport a szorzásra nézve.

11. Állítás. Minden ferdetest nullosztómentes.

BIZONYÍTÁS Legyen K ferdetest, $a, b \in K$, $ab = 0$. Balról a^{-1} -gyel szorozva $b = 0$.

Példák

1. A racionális, a valós illetve a komplex számok (\mathbb{Q} , \mathbb{R} , \mathbb{C}) testet alkotnak a szokásos műveletekre.
2. A modulo 2 maradékosztályok testet alkotnak a maradékosztályok összeadása és szorzása műveletekre. Az 1-nek (m_1 -nek) van inverze: $1 \cdot 1 = 1$ miatt az 1 inverze önmaga.
3. A modulo 5 maradékosztályok testet alkotnak a maradékosztály műveletekre. Elég leellenőrizni, hogy az 1,2,3,4 elemeknek van-e inverze. $1 \cdot 1 = 1$, $2 \cdot 3 = 6 = 1$, $4 \cdot 4 = 16 = 1$ miatt az 1 és a 4 inverze önmaga, a 2-é a 3.

4. Az $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ alakú valós mátrixok testet alkotnak a mátrixműveletekre.

Ez izomorf \mathbb{C} -vel: $\varphi \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a + b \cdot i$ izomorfizmus.

5. A valós számtest feletti racionális törtfüggvények halmaza, $\mathbb{R}(x)$, testet alkot a szokásos műveletekre, azaz

$$\mathbb{R}(x) = \left\{ \frac{p(x)}{q(x)} \mid p(x), q(x) \in \mathbb{R}[x], \quad q(x) \neq 0 \right\}$$

test, ahol

$$\frac{p_1(x)}{q_1(x)} + \frac{p_2(x)}{q_2(x)} = \frac{p_1(x)q_2(x) + p_2(x)q_1(x)}{q_1(x)q_2(x)},$$

valamint

$$\frac{p_1(x)}{q_1(x)} \cdot \frac{p_2(x)}{q_2(x)} = \frac{p_1(x)p_2(x)}{q_1(x)q_2(x)}.$$

6. Legyen d négyzetmentes szám, azaz $b = p_1 p_2 \cdots p_k$, ahol a p_i -k különbözőek. $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ test a szokásos műveletekre. $\mathbb{Q}(\sqrt{d})$ gyűrű. $(a + b\sqrt{d}) \frac{a - b\sqrt{d}}{a^2 + db^2} = 1 \implies$ van inverz minden nem nulla számra. ($a^2 + db^2 \neq 0$!)

Kvaterniók ferdeteste

Tekintsük az $a + bi + cj + dk$ alakú „számokat”, ahol $a, b, c, d \in \mathbb{R}$, $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$, $ik = -j$, összeg koordinátánként, szorzat a disztributitás alapján:

$$(a_1 + b_1i + c_1j + d_1k) + (a_2 + b_2i + c_2j + d_2k) = \\ (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k$$

$$(a_1 + b_1i + c_1j + d_1k)(a_2 + b_2i + c_2j + d_2k) = \\ (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1b_2 + a_2b_1 + c_1d_2 - c_2d_1)i + \\ + (a_1c_2 + a_2c_1 + d_1b_2 - d_2b_1)j + (a_1d_2 + a_2d_1 + b_1c_2 - b_2c_1)k.$$

Konjugált, norma

$$\overline{a + bi + cj + dk} = a - bi - cj - dk \quad \text{és}$$

$$|a + bi + cj + dk|^2 = (a + bi + cj + dk) (\overline{a + bi + cj + dk}) = a^2 + b^2 + c^2 + d^2.$$

Ha $k \neq 0$ kvaternió, akkor $k \cdot \bar{k} / |k|^2 = 1 \implies$ van inverz, azaz ferdetest. A kvaterniók valóban nem test, hisz $ij \neq ji$.

Meghökkenő tények

Nem igaz, hogy $(\alpha + \beta)^2 = \alpha^2 + 2\alpha\beta + \beta^2$! $(i + j)^2 = (i + j)(i + j) = i^2 + ij + ji + j^2 = -1 + k - k - 1 = -2 \neq i^2 + 2ij + j^2 = -2 + 2k$

Az $x^2 + 1$ polinomnak végtelen sok gyöke van! Gyöke minden $bi + cj + dk$ alakú szám, ahol $b^2 + c^2 + d^2 = 1$.

$x^2 + 1 = (x + i)(x - i) = (x + j)(x - j) = (x + k)(x - k) = (x + t)(x + \ell)$, ahol t gyöke a polinomnak. Ugyanakkor: i -t helyettesítve az első három felbontásba: $i^2 + 1 = (i + i)(i - i) = 0$, $(i + j)(i - j) = -2k$, $(i + k)(i - k) = 2j$

Frobenius tétel

Az $a + bi$ ($a + bj$, $a + bk$) alakú számok a komplex számokkal izomorf résztestjét alkotják a kvaternióknak.

Van még egyéb olyan (ferde) test, aminek résztestje a valós számtest?

12. Tétel. *Legyen K a valós számokat tartalmazó ferdetest. Ekkor K izomorf a komplex számok vagy a kvaterniók valamelyikével.*

Véges testek

13. Állítás. *Minden véges integritási tartomány test.*

BIZONYÍTÁS Legyen R integritási tartomány. Legyenek a gyűrű elemei $0 = a_1, a_2, \dots, a_n$. Legyen $0 \neq a \in R$. Tekintsük az aa_1, aa_2, \dots, aa_n elemeket. $aa_i = aa_j \implies a(a_i - a_j) = 0 \implies a_i = a_j$ (nullosztómentes!) \implies az aa_i elemek mind különbözőek. Mivel n elem van, ezért felsoroltuk az összes elemet, így előállítottuk a -t is, \implies van $e \in R$, hogy $ae = a$.

$ae = a \implies$ tetszőleges $b \in R$ -re $bae = ba$, \implies a kommutativitás szerint $abe = ab$, $a(be - b) = 0$. Nullosztómentes és $a \neq 0 \implies be - b = 0$, azaz $b = be$. $\implies e$ egységelem.

Az aa_i elemek közt szerepel e is, azaz a -nak van inverze.

$$\mathbb{Z}_m$$

14. Állítás. \mathbb{Z}_m pontosan akkor test, ha m prím.

BIZONYÍTÁS \mathbb{Z}_m akkor nullosztómentes, ha $a, b \in \mathbb{Z}_m$ esetén $ab = 0$ -ból $a = 0$ vagy $b = 0$ következik, azaz $m \mid ab$ esetén $m \mid a$ vagy $m \mid b$. Ez pont a prímtulajdonság.

A \mathbb{Z}_p gyűrűt, ha mint testre gondolunk rá, \mathbb{F}_p -vel is jelöljük.

Prímtestek

15. Definíció. Egy testet **prímtestnek** nevezünk, ha nincs valódi részteste.

16. Tétel. Minden test tartalmaz prímtestet. \mathbb{Q} és \mathbb{F}_p prímtestek. Más prímtest nincs.

BIZONYÍTÁS Legyen K a test. $1 \in K \implies 1 + 1, 1 + 1 + 1, \dots, 1 + \dots + 1 \in K$.

1. $0 = \underbrace{1 + \dots + 1}_{k\text{-szor}} \implies$ A sorozat elemei ekkor éppen a \mathbb{Z}_k gyűrűt alkotják.

De mivel a test nullosztómentes, k csak egy p prímszám lehet, azaz $\mathbb{F}_p \leq K$.

2. A sorozatban nem szerepel a 0; Ekkor a test tartalmazza a természetes számokat. Mivel minden számmal az ellentettje is benne van, a test tartalmazza az egészeket, és a multiplikatív inverz létezése miatt bármely két elem hányadosát, így \mathbb{Q} -t is.

Tehát minden test tartalmazza \mathbb{F}_p -t vagy \mathbb{Q} -t, más prímtest nincs.

Véges test elemszáma

17. Tétel. *Legyen K véges test. Ekkor K elemszáma prímszám.*

BIZONYÍTÁS Van olyan p , hogy $\mathbb{F}_p \leq K$. K vektortér \mathbb{F}_p fölött. Legyen e_1, e_2, \dots, e_n a K vektortér bázisa \mathbb{F}_p felett. Ekkor minden elem egyértelműen előáll

$$\sum_{i=1}^n \alpha_i e_i \quad (\alpha_i \in \mathbb{F}_p)$$

alakban. Ezért a test elemszáma p^n .