2. tétel

D.: Az $S \neq \emptyset$ halmaz $S \times S$ Descartes-féle szorzatának S-be való leképezését az S halmazon értelmezett kétváltozós (bináris) műveletnek nevezzük. $f : S \times S \to S \;((a,b) \to f(a,b))$

D.: Algebrai struktúrának nevezzük az olyan legalább kéttagú rendszert, amelynek első eleme $S(\neq \emptyset)$ halmaz, a többi pedig S-en értelmezett valamilyen algebrai művelet.

Algebrai műveletek: Egy $(S; \cdot)$ struktúrában az S halmazon értelmezett $\cdot$ műveletről azt mondjuk, hogy:

- asszociatív: $\forall a,b,c \in S$-re $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- kommutatív: $\forall a,b \in S$-re $a \cdot b = b \cdot a$
- idempotens: $\forall a \in S$-re $a \cdot a = a$
- kancellatív: $\forall a,b \in S$-re $x \cdot a = b$, $a \cdot y = b$ egyenletnek legfeljebb egy megoldása van, ha mindig van mo $\Rightarrow$ $\cdot$ invertálható
- $\exists$ neutrális elem (u): $\exists u$, $\forall a \in S$-re: $u \cdot a = a \cdot u = a$

  (szorzásnál egységelemről, összeadásnál zérusról beszélünk)

  (LEGFELJEBB 1 neutrális elem $\exists$ egy struktúrában!)
- $\exists$ zéruselem (z): $\exists z$, $\forall a \in S$-re: $z \cdot a = a \cdot z = z$

  (1 struktúrában LEGFELJEBB 1 zéruselem van!)
- $\exists$ inverz elem (a'): $\exists a'$, $\forall a \in S$-re: $a' \cdot a = a \cdot a' = u$.

  (szorzásnál: multiplikatív inverz, összeadásnál: additív inverz.)

$(S; \cdot; *)$ $\to$ S kétműveletes struktúra

- $*$ disztributív $\cdot$-ra: $\forall a,b,c \in S$-re: $a * (b \cdot c) = (a * b) \cdot (a * c)$
  $(a \cdot b) * c = (a * c) \cdot (b * c)$
- $*$ abszorbtív $\cdot$-ra: $\forall a,b \in S$-re: $a * (a \cdot b) = a$

Algebrai struktúrák:

- $(S;\cdot)$ félcsoport, ha $\cdot$ asszociatív.
- $(S;\cdot)$ csoport, ha $\cdot$ assz és invertálható (
- $(S;\cdot)$ félháló, ha $\cdot$ assz, kommutatív és idempotens.
- $(S;+)$ kommutatív csoportban (modulus) neutrális elem = zérus (jele: 0)
- $(S;+;\cdot)$ gyűrű, ha $(S;+)$ modulus $\wedge$ $(S;\cdot)$ félcsoport $\wedge$ $\cdot$ disztr. $+$-ra
- $(S;+;\cdot)$ integritástartomány, ha $(S;\cdot)$ komm, egységelemes, zérusosztómentes
- $(S;+;\cdot)$ test, ha S min kételemű $\wedge$ $(S;+)$ modulus $\wedge$ $(S\setminus\{0\};\cdot)$ komm. csoport $\wedge$ $\cdot$ disztributív $+$-ra
- $(S;\cdot;*)$ háló, ha $(S;\cdot)$ $\wedge$ $(S;*)$ félháló $\wedge$ mindegyik művelet a másikra nézve abszorbtív.

Euklideszi gyűrűk:

D.: Az R integritástartományt euklideszi gyűrűnek nevezzük, ha $\exists$ R-nek nemnegatív egész számok N halmazában olyan $^*\delta: R \to N$ $(a \to \delta a)$ leképezése, hogy:

1. $\delta a = 0 \Leftrightarrow a = 0$
2. $\delta(ab) = \delta a \cdot \delta b$
3. $\forall a,b\,(b \neq 0)$ R-beli elemhez $\exists$ $q, r\,(\in R)$ elem, amelyre $a = bq + r$, ahol $0 \leq \delta r < \delta b$. **

*: ezt a leképezést euklideszi normának nev.
**: -"- euklideszi (maradékos) osztásnak nev.
q: hányados, r: maradék

T.: Ha R euklideszi gyűrű $\Rightarrow$ $\forall$ a,b $(b \neq 0)$ R-beli elemhez található olyan x_n, y_n $(\in R)$, amelyre az $ax_n + by_n = r_n$. egyenlőség teljesül, ahol r_n az a,b $(b\neq 0)$ elempáron végrehajtott euklideszi algoritmus utolsó, zérustól különböző maradéka.

Permutációcsoport:

Egy tetszőleges H halmaz $f: H \to H$ önmagára való kölcsönösen egyértelmű leképezéseit a H halmaz permutációinak nevezzük. A $H = \{a, b, c \dots\}$ halmaz egy f permutációját úgy fogjuk megadni, h a H halmaz minden egyes x eleme alá írjuk azt az

$x' = \varphi x$ elemet, amelyet a φ permutáció az x elemhez hozzárendel.

$$\varphi = \begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix} = \begin{pmatrix} a & b & c \\ \varphi a & \varphi b & \varphi c \end{pmatrix}$$

! H-nak

$$\psi = \begin{pmatrix} a & b & c \\ a'' & b'' & c'' \end{pmatrix} = \begin{pmatrix} a & b & c \\ \psi a & \psi b & \psi c \end{pmatrix}$$

Test:

D.: $(T; +; \cdot)$ algebrai struktúra test, ha T legalább kételemű, $(T; +)$ modulus, $(T \setminus \{0\}; \cdot)$ komm. csoport $\wedge$ $\cdot$ disztributív az $+$-ra nézve.

I. T legalább kételemű
II. T-ben 2 művelet van értelmezve: $+$, $\cdot$
III. $+$ komm.
IV. $+$ asz.
V. $+$ invertálható
VI. $\cdot$ asz.
VII. $\cdot$ komm.
VIII. $T \setminus \{0\}$-ban $\cdot$ invertálható
IX. $\cdot$ az $+$-ra nézve disztributív

A test olyan kommutatív gyűrű, amelyben a 0-tól különböző elemek a szorzás szerint csoportot alkotnak.

D.: $(S; +; \cdot)$ testet a $(T; +; \cdot)$ test résztestének nev., ha:

- $(\emptyset) \subset S \subseteq T$
- $i: (S; +; \cdot) \to (T; +; \cdot)$ homomorfizmus

D.: Primtestnek nevezzük az olyan testet, amelynek nincs valódi (önmagától különböző) résztestе.

T.: Minden primtest izomorf a $\mathbb{Q}$ és a $\mathbb{Z}_p$ (p prím) testek valamelyikével.

Az egész számok gyűrűje:

A $(Z; +; \cdot)$ struktúra integritástartomány (egységelemes, zérusosztómentes, kommutatív gyűrű)

- $(Z; +; \cdot)$ - ban ismert az $a \leq b$ rendezési reláció

- a 0-nál nagyobb egész számok : pozitív egészek
- a 0-nál kisebb —"— : negatív —"—

Az $a < b$ relációra teljesülnek a következők:

a) trichotomia : $\forall\, a, b \in \mathbb{Z}$ -re

$a < b$; $a = b$; $a > b$ közül pontosan az egyik teljesül

b) izotonitás az $+$-ra nézve :

$$a < b \Rightarrow a + c < b + c$$

c) izotonitás a pozitív számmal való szorzásra nézve

$$(a < b \wedge 0 < c) \Rightarrow ac < bc$$

Ezek alapján azt mondjuk, h az egész számok gyűrűje rendezett gyűrű.