$\{1, a^4\} \subset \{1, a^2, a^4, a^6\}$

nincs szorzat alakban levő felírás, mert a metszetük nem üres.

$C_{p^2}(a)$ – nincs nem triviális direkt felbontása

$C_{100}(a) = C_{25}(a^4) \times C_4(a^{25})$

tovább nem bonthatók

$C_{30}(a) = C_{15}(a^2) \times C_2(a^{15})$

$\downarrow$

$C_3 \times C_5$

„A számokat csak prímhatványokig tudjuk felbontani"

Ábel-csoportok

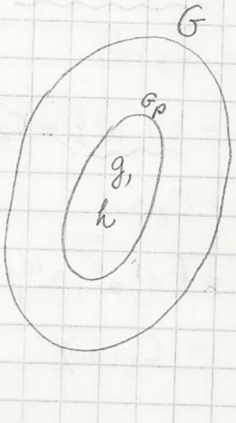
Def.: A G csoportot p-csoportnak nevezzük, ha $|G| = p^n$ (p prím)

A $g \in p$ p elemnek nevezzük, ha $o(g) = p^\alpha$.

Tétel: Az Ábel-csoportban a p elemek (amelyeknek a rendje p-nek valamely hatványa) részcsoportot alkotnak.

G Ábel csoport

$g, h \in G$ $\quad o(g) = p^\alpha$, $o(h) = p^\beta$



G_p : p elemek halmaza G-ben

Be kell látni:

G_p részcsoport

$$\left.\begin{array}{l} 1., \ 1 \in G_p \\ 2., \ g \in G_p \Rightarrow g^{-1} \in G_p \\ 3., \ g, h \in G_p \Rightarrow gh \in G_p \end{array}\right\} ?!$$

1., $1 = p^0 \qquad 1^{p^0} = 1$ ✓ igaz

2., $\exists \alpha \qquad g^{p^\alpha} = 1 \Rightarrow$

$$(g^{-1})^{p^\alpha} = (g^{p^\alpha})^{-1} = 1$$

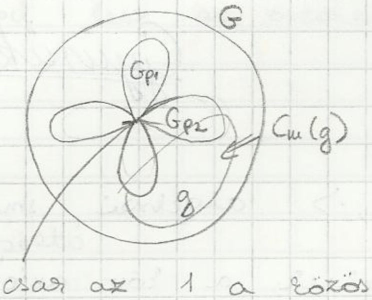
$$o(g^{-1}) = p^\alpha \Rightarrow g^{-1} \in G_p$$

3., $\alpha, \beta \qquad g^{p^\alpha} = 1 \quad h^{p^\beta} = 1 \Rightarrow (gh)^{p^{\alpha+\beta}} = 1$ ✓ igaz

mivel kommutatív $\Rightarrow (gh)^n = g^n \cdot h^n$

$$o(gh) = p^{\alpha+\beta} \Rightarrow gh \in G_p$$

$|G| = n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$



$G_{p1}, G_{p2}, \dots G_{ps}$

csak az 1 a közös elemük

$G = G_{p1} \otimes G_{p2} \otimes \dots \otimes G_{ps}$

$\downarrow$

felbomlik belső direkt szorzatra

Biz.: → nem kell.

$\forall g \in G \qquad g = g_1 g_2 \dots g_s, \quad g_i \in G_{p_i} \qquad i = 1 \dots s$

$o(g) \mid |G| = n \qquad o(g)$ osztja a csoport rendjét

$|G| \Rightarrow$ ami egyenlő n.

$o(g) = m \qquad (m \mid n)$

$\langle g \rangle = \{1, g, g^2 \dots g^{m-1}\} = C_m(g)$

$m = p_1^{\beta_1} \cdot p_2^{\beta_2} \dots p_s^{\beta_s}$

$$C_{p_1^{\beta_1}}(a^{u_1}) \otimes \ldots \otimes C_{p_s^{\beta_s}}(a^{u_s}) = C_m(g)$$

$$g = g_1 \cdot g_2 \cdot \ldots \cdot g_s$$

A tétel be van bizonyítva!

Az Ábel-tételek alaptétele:

Véges Ábel-csoport ciklikus p részcsoportok direkt szorzataként állítható elő. E részcsoportok rendje egyértelműen meghatározott.

$$\left.\begin{array}{l} C_2(a) \times C_4(b) \times C_5(c) \\ C_5 \times C_5 \times C_4 \end{array}\right\}$$ itt megengedettek

10.28. 10. előadás

Gyűrűk

Def.: $\langle R;+;\cdot\rangle$ algebrai struktúrát gyűrűnek nevezzük, ha teljesülnek a köv. axiómák. (R nem üres)

I. 1., $a+(b+c) = (a+b)+c \quad \forall a,b,c \in R$ asszociatív

2., $\exists\, 0 \in R$, $a+0=0+a=a \quad \forall a \in R$

3., $\forall a \in R \quad \exists -a$; $a+(-a) = -a+a = 0$

4., $a+b = b+a \quad \forall a,b \in R$

II. 1., $a\cdot(bc) = (ab)c \quad \forall a,b,c \in R$

2., $(a+b)\cdot c = ac+bc$

$a(b+c) = ab+ac \quad \forall a,b,c \in R$

gyűrű

i_3 $\exists\, 1 \in R \quad \forall a \in R \quad 1 \cdot a = a \cdot 1 = a$ ↑ egységelemes gyűrű

$+ \quad ab = ba \quad \forall a,b \in R$ ↑ kommutatív gyűrű

$\langle R; +\rangle$ kommutatív Ábel-csoport

+ disztributivitás kapcsolja össze az „+" és a „·"-t.

$\langle N; +; \cdot\rangle$

I/1. ✓
I/2. —
I/3. —
I/4. ✓

II/1 ✓
II/2 ✓
II/3 ✓
II/4 ✓

$\langle Z; +; \cdot\rangle$ kommutatív egységelemes gyűrű

$M_{n\times m}(\mathbb{R})$ Valós $n\times m$-es mátrixok halmaza

azonos típusúakra I/1-4 igaz

· → nincs értelmezve. ↯

$\{M_{n\times m}(\mathbb{R}) \cup M_{m\times k}(\mathbb{R})\}$ $n\times k$-s típusú lesz az eredménymátrix

$M_{n\times n}(\mathbb{R})$

$\underset{\neq 0}{\begin{pmatrix}1&0\\0&1\end{pmatrix}} \cdot \underset{\neq 0}{\begin{pmatrix}0&0\\0&1\end{pmatrix}} = \begin{pmatrix}0&0\\0&0\end{pmatrix}$ nullosztó v. zérusosztó

valós sorozatokra $\langle\langle s\rangle; +; \cdot\rangle$

I 1-4 ✓

II 1-4 ✓

valós konvergens sorozatok halmaza $\langle\langle s\rangle; +; \cdot\rangle$

Ha „+"-vagy „·" két konvergens sorozatot ⇒ a végeredmény is konvergens lesz

a $(0; 0; \ldots 0)$ is a 0-hoz konvergál ha $a_n \to a \Rightarrow -a_n \to -a$

I 1–4 ✓

az $(1, 1, 1 \ldots)$ sorozat konvergens

II 1–4 ✓

1/2, 1/3   11/3 → ezeket kellett ellenőrizni, meg hogy művelet-e

Olyan sorozatokat vizsgálunk, amelyek 0-hoz konvergálnak.

$a_n \to a$
$b_n \to b$ $a_n + b_n \to a+b$

„+": nem művelet

Def.: $R' \subseteq R$ gyűrű részhalmazát részgyűrűnek nevezzük, ha maga is gyűrű az R R' leszűkítésére nézve.

Tétel: $R' (\subseteq R) \Leftrightarrow$ részgyűrűje R-nek, ha:

i, $a+b \in R'$ $\forall a, b \in R'$

ii, $a \cdot b \in R'$ –"–

iii, $-a \in R'$ $\forall a \in R'$

iv, $0 \in R'$

Az i. iii, iv, $\Rightarrow \sim a-b \in R'$

↳ ekvivalens az előző 3 állítással

Def.: $a \neq 0 \ (\in R)$ elemet baloldali nullosztónak nevezzük, ha $\exists \ 0 \neq b \ (\in R) \Rightarrow ab = 0$

hasonlóan definiáljuk a jobboldali nullosztót

Def.: Ha $a \in R$-hez $\exists$ olyan elem, amelyet a'-gyel jelölünk, h. $aa' = a'a = 1 \Rightarrow a$-t egységnek nevezzük. (a gyűrű egységeleme)

R^* - R gyűrű egységeinek halmaza

Z^* - Z egységei : $\{1; -1\}$

$Q^* = Q \setminus \{0\}$ ⇒ nem ciklikus, de Ábel-csop.

$\langle Z^*; \cdot \rangle$ csoport-e? Igen, Ábel-csoport

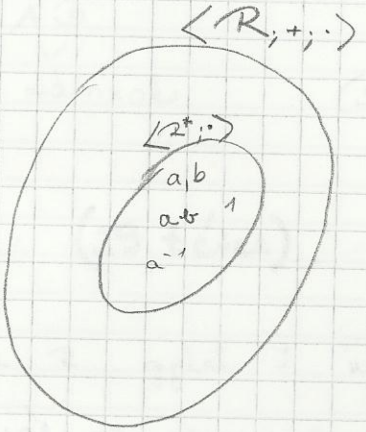
Z^* : véges csoport

Ábel-csoport

ciklikus csoport C_2 (-1) generált

Tétel: $\langle R^*; \cdot \rangle$ csoport.

(A gyűrű egységeinek halmaza multiplikatív csoportot alkot.)



R^* kisebb, mint R, mert nincs benne a 0.

Biz.: Be kell látni, h : 1, $\forall\, a,b \in R^* \Rightarrow ab \in R^*$ ✓

2, $\forall\, a \in R^* \Rightarrow a^{-1} \in R^*$ ✓

3, $1 \in R^*$ ✓

1, $a,b \in R^* \Rightarrow \begin{matrix} aa^{-1} = a^{-1}a = 1 \\ bb^{-1} = b^{-1}b = 1 \end{matrix}$ $\quad a^{-1}, b^{-1} \in R$

$(ab)^{-1} \qquad ab \cdot \boxed{b^{-1}a^{-1}} = 1 \Rightarrow (ab)^{-1} = b^{-1}a^{-1}$

2., $a^{-1}a = a \cdot a^{-1} = 1 \Rightarrow \underset{(a^{-1})^{-1}}{a^{-1}}$ inverze $= a$ $\quad (a^{-1}) \in R^*$

3., $1^{-1} = 1 \quad \Rightarrow 1 \in R^*$

Tétel: $a \in R$ nullosztó $\Rightarrow$ nem egység

$c \in R^*$ (R^*: R egységcsoportja)

c nem nullosztó

Biz.: $a \neq 0 \quad \exists\, b \neq 0 \quad (a, b \in R)$

$a^{-1}/ \quad ab = 0$

$\underbrace{a^{-1} \cdot a}_{1}b = 1b = 0$

$\underbrace{b}_{} = 0$ ↯

$c \in R^* \quad \exists\, c^{-1} \in R^*$

legyen c nullosztó $\quad b \neq 0 \quad (b \in R)$

$c^{-1} / \quad cb = 0$

$b = 0$ ↯

V. 5.

11. előadás

$2x = 3$ nincs mego. $\mathbb{Z}$-ben

$2x = 12$ nincs $\frac{1}{2}$ a $\mathbb{Z}$-ben

$\cancel{2}x = \cancel{2} \cdot 6$

Def.: Baloldali egyszerűsítési szabály: $ab = ac \Rightarrow b = c$

Jobboldali egyszerűsítési szabály: $ba = ca \Rightarrow b = c$

Tétel: $a \in R$ akkor a-val csak akkor lehet balról egyszerűsíteni, ha a nem nullosztó R-ben.

BIZ.: „$\Rightarrow$" a - nullosztó $(a \neq 0)$ $\exists\ 0 \neq b \in R$

$ab = 0$

$ab = a0$ $\quad b = 0.$ ↯ $0 \neq b \in R$

„$\Leftarrow$" Legyen $ab = ac$ $\quad a$ nem nullosztó

$a(b-c) = 0$

ha a nem nullosztó, nincs olyan nem 0 elem, hogyha megszorozzuk 0-t kapunk.

$\Downarrow$

$b - c = 0 \Rightarrow b = c$

$\cancel{A}X = \cancel{A}B$

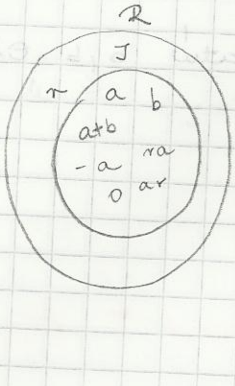
mátrixok

Ideálok: (29. tétel)

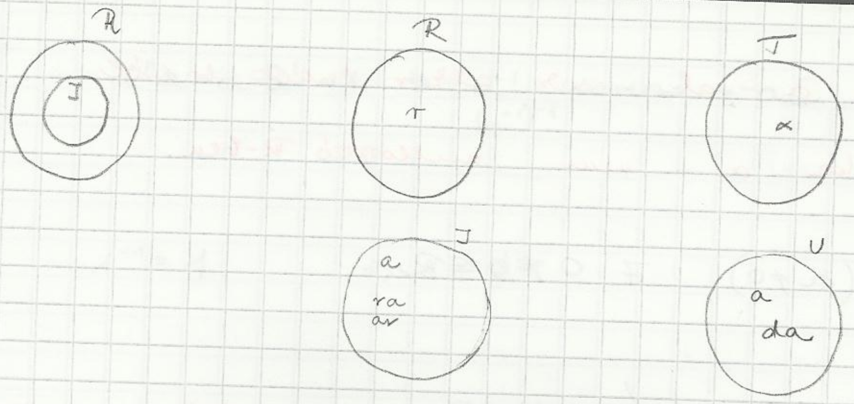
Df.: Az R gyűrű J nem üres $(\emptyset \neq J \subseteq R)$ részhalmazát ideálnak nevezzük $\forall\, a, b \in J$, $\forall\, r \in R$ esetén:

1, $\left.\begin{array}{l} a+b \in J \\ -a \in J \\ 0 \in J \end{array}\right\} a - b \in J$

2, $ra, ar \in J$



Van olyan részgyűrű, ami nem ideál.



additív csoport, Ábel-féle csop.

$R \neq \{0\}$ gyűrűben van legalább 2 tulajdonság, legalább 2 ideál: az egyik a 2, a másik a $\{0\}$, ezeket triviális ideálokat kapjuk.

$J \lhd R$

pl.: $\mathbb{Z}$-ben keressük

1, tulajdonság : páros számok halmaza ideál

Ha ra teljesül, ar nem, ⇒ azt mondjuk: balideál

$R = \mathbb{Z}$

$g = \{ n$

A páros számok halmazára teljesül, a páratlanokra nem ⇒

páratlan + páratlan = páros (0 nem páros)

Vegyük a 0-hoz konvergáló nullsorozatot.

1, ha pozitív $a, b \in \mathbb{Z}$

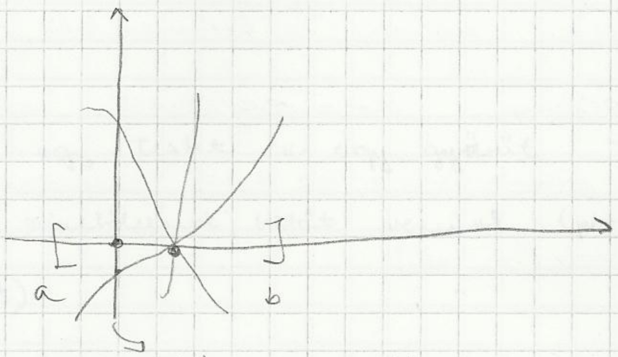
2.,

3,

Nézzük azt a sorozatot, amely 5-höz konvergál.

Nincs 5. elme

$T = \{f, \in [a,b]$ folytonos fv-ek.



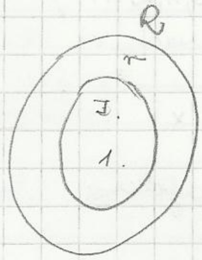
Gyüjti v. elűzi a

Ez a fgv szorzására és összeadására nézve ez gyűrű.

$F = \{f, \in \underset{\downarrow \atop [a,b]}{C[a,b]} \mid f(c) = 2;\ c \in [a,b]\}$

Tétel: Ha $1 \in J \triangleleft R \Rightarrow J = R$

BIZ.:



$1 \in J \triangleleft R$

$J \subseteq R$;

$J \supseteq R$?!

$\forall r \in R :\Rightarrow (\text{def } 2.)\ r \cdot 1 = r \in J \Rightarrow J \supseteq R \Rightarrow J = R$

Tétel: $\{J \triangleleft R,\ R^* \cap = \{\emptyset\}\} \Rightarrow J = R$

Legyen J az R egy ideálja, és J tartalmaz egységet $\Rightarrow J = R$

[egység: van inverze az elemeknek.]

$e \in I$ (e : egység) $\exists\, e^{-1} \in R$, $ee^{-1} = e^{-1}e = 1$

Az egység benne van az I-ben, $\forall$ r-rel szorozva $\Rightarrow$

az I-ben lesz. (továbbá: lsd. előző tétel)

Példák:

$R[x]$

f° : polinom foka

$R^*_{[x]} = ?$

$1 = 1x^0 \to$ egységpolinom

f-nek van inverze: $f \cdot g = 1 \cdot x^0$

f és g egymás inverzei

$(fg)^\circ = f^\circ + g^\circ$

$\parallel$

$(1x^0)^\circ$ $\quad 0 = f^\circ + g^\circ$, $f^\circ = 0$, $g^\circ = 0$

$\parallel$

0 polinom foka: nem negatív egész $(0, 1, 2 \ldots)$

$f = ax^0 = a$

Ha a polinomnak van inverze $\Rightarrow$ nulladfokú.

$f = b\,x^0$, $b \neq 0$ $\quad f^{-1} = \frac{1}{b}\, x^0$

$R^*_{[x]} = \{ f \in R[x] \mid f^\circ = 0 \}$

Hf.: $R[x]$ nullosztómentes.

2 polinom

Legyen f polinom nem 0.

változó → fgv-énél

ismeretlen → egyenleteknél

polinomoknál → határozatlan

polinom:

- Veszünk egy testet v. egy gyűrűt ⇒ innen vesszük az együtthatókat
- formális szimbólumot, betűt veszünk (pl.: x,y → határozatlannak mondjuk)
- számlázzuk azt a tulajdonságot x-re, h. x^0, $x^1 = x$, $x^2 = x \cdot x$ ⇒ FORMÁLISAN
- Veszünk egy ~~eo~~ együtthatót → így lesz monom. (pl.: ax) egytagú
- 1: annak a gyűrűnek az egyese, ahonnan az együtthatót vettük
- egymás mögé írjuk a sok monomot, közé ‚+' jelet teszünk → formálisan ⇒ polinom

A formális x helyett beteszünk egy elemet ⇒ a ‚+' jel tartalmat kapott

- megkeressük a polinom zérushelyeit
- Veggyünk 1 formális polinomot, és tegyük egyenlővé Ø-val. ⇒ algebrai egyenlet
- A megoldások a polinom gyökei → a polinom zérushelyei

• A polinom meghatározó tulajdonsága a fokszám.

$\emptyset x^{100}+3x^3+4x+1=0 \Rightarrow$ fokszáma 3.

Az x legmagasabb fokszáma, ahol az együttható nem $\emptyset$.

• Két polinom összeadása (másod- és harmadfokú)

A másodfokútól formálisan harmadfokút csinálunk. (Egyik m, a másik n : az összeg fokszáma nem nagyobb, mint max(m, n)

• Szorzás: Minden tagot, minden taggal.

$$\underbrace{ax^m \;\dots\; bx^n}_{abx^{m+n}}$$

$ax^m \cdot bx^n = 0$, ha a és b zérusosztó $\Rightarrow$ Gyűrűben

A polinomgyűrűben $T[x]$ felett nincs nullosztó.

Test felett nincs nullosztó, ott soha nem lehet.

——∘——

Legyen f polinom m-ed fokú, g polinom n-ed fokú.

$f(x) = ax^m + \dots$

$g(x) = bx^n + \dots$

Tfh. $f(x)$, $g(x)$ zérusosztó

$f(x) \cdot g(x) = 0$.

$\underline{fg}$ foka = a 0 ~~polinom~~

$(fg)^\circ$

A legmagasabb hatvány : $a_n b_n = x^{n+m}$

x^{m+n} együtthatója $\neq 0$, mert sem a, sem b $\neq 0$ $\Rightarrow$
nincs nullosztó

$f = a_n x^n + \ldots + a_0 \qquad a_n \neq 0$

$g = b_m x^m + \ldots + b_0 \qquad b_m \neq 0$

$f \cdot g = \underbrace{a_n b_m}_{\text{nem } 0} x^{n+m} + \ldots + a_0 b_0 = 0$

pl.: $(x-1)(x+1) = x^2 + x - x - 1$

$(x^2 - 2)(x^3 + x + 1) = x^5 + x^3 + x^2 - 2x^3 - 2x - 2 = x^5 - x^3 + x^2 - 2x - 2$

Fuchsból átnézni az euklideszi gyűrű → vizsgán tudni a gyűrűket
mindenkitől kérdez.

BIZ. kell a következő!