1. Bevezetés

A félév anyaga.

- *Gyűrűk és testek*
  - Ideál, faktorgyűrű, főideálgyűrű
  - Gauss-egészek, két négyzetszám tétel
  - Az alaptételes gyűrűk jellemzése
  - A számfogalom lezárása
  - Algebrai és transzcendens számok
  - Testbővítések, testek konstrukciója
  - Geometriai szerkeszthetőség, algebrai egyenletek
  - Véges testek, kódelmélet
- *Lineáris algebra*
  - Kvadratikus alak négyzetösszeg alakja
  - Euklideszi terek: merőlegesség és skaláris szorzat
  - Egybevágósági transzformációk valós és komplex fölött
  - Diagonalizálhatóság ortonormált bázisban
  - Polinommátrixok, a Jordan-alak kiszámítása

Irodalom.

- `http://www.cs.elte.hu/~ewkiss/bboard/`
  - Az előadáson látott prezentáció, és nyomtatható változata
  - A gyakorlatokon szereplő feladatsorok
  - Információk a vizsgákról, zárthelyikről
  - Tematikák, oktatási anyagok, ajánlott irodalom
- *Kiss Emil: Bevezetés az algebrába*
  - Gyűrűk és testek
  - Polinommátrixok, Jordan-alak
  - A gyakorlatokon szereplő feladatok megoldásai
- *Freud Róbert: Lineáris algebra*
  - A félév lineáris algebra anyaga
  - Feladatok megoldásokkal
- *Freud-Gyarmati: Számelmélet*
  - Gauss-egészek, két négyzetszám tétel, ideálok
- *Czédli-Szendrei-Szendrei: Absztrakt algebrai feladatok*

A számonkérés módja.

- *A gyakorlati jegy:*
  - Csak három hiányzás megengedett.
  - Két évfolyamzárthelyi: $50 - 50\%$, az előadás idejében: okt. 17. és dec. 12.
    - az elégtelen zárthelyiket ki kell javítani;
    - javító a félév végén, a gyakorlatvezető döntése alapján;
    - Ha nem sikerül: gyakorlati jegy utóvizsga.
- *A vizsgajegy:*
  - Csak érvényes gyakorlati jeggyel lehet vizsgázni.
  - *Szóbeli* vizsga, az anyag megértését is méri!
    - Mindenki két tételt húz:
    - az első egy konkrét bizonyítás;
    - a második egy téma a félévből, ahol ki kell mondani (és alkalmazni tudni) a tételeket és a definíciókat.
    - Bármelyik tétel nemtudása esetén a vizsga elégtelen.

2. Ideálok

Izomorfizmus és homomorfizmus.

Definíció
Legyenek R és S gyűrűk.
Az R összeadása $+_R$, szorzása $*_R$. Az S összeadása $+_S$, szorzása $*_S$.
A $\psi : R \to S$ leképezés *gyűrűhomomorfizmus*, ha az összeadást és a szorzást is *tartja*:
$\psi(a +_R b) = \psi(a) +_S \psi(b)$ minden $a, b \in R$-re,
$\psi(a *_R b) = \psi(a) *_S \psi(b)$ minden $a, b \in R$-re.
Ha ψ kölcsönösen egyértelmű is, akkor ψ *izomorfizmus*.

Homomorfizmusok, amik nem izomorfizmusok

(1) $R = \mathbb{Z}$, $S = \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n.

(2) $R = \mathbb{R}[x]$, $S = \mathbb{C}$, $\varphi(f) = f(i)$ (φ az i behelyettesítése).

Elemi tulajdonságok.

Láttuk korábban (2.2.44. Feladat)
Legyen $\varphi : G \to H$ csoporthomomorfizmus. Ekkor φ az *egységelemet az egységelembe* viszi, és *inverz képe a kép inverze* lesz (azaz φ az inverzképzés műveletét is tartja).

Következmény
Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor R nullelemét S nullelemébe viszi, azaz $\varphi(0) = 0$, továbbá $\varphi(-r) = -\varphi(r)$.

Példa (5.1.20. Gyakorlat)
$\varphi : \mathbb{R} \to \mathbb{R}^{2\times 2}$, $\varphi(r) = \begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix}$ gyűrűhomomorfizmus, de $\mathbb{R}$ egységelemét nem viszi $\mathbb{R}^{2\times 2}$ egységelemébe.

Homomorfizmus képe és magja.

5.1.3, 5.1.4. Definíció
Minden gyűrűhomomorfizmus csoporthomomorfizmus is az additív csoportok között, így lehet *képről* és *magról* beszélni. Mindkettő nyilván részgyűrű.

5.1.5. Tétel
Az R gyűrű egy I részhalmaza pontosan akkor magja egy R-en értelmezett homomorfizmusnak, ha részcsoport R^+-ban, és minden $a \in I$ és $r \in R$ esetén $ar, ra \in I$.

Legyen $\varphi : R \to S$ és $I = \mathrm{Ker}(\varphi) = \{r \in R : \varphi(r) = 0\}$. Ha $a \in I = \mathrm{Ker}(\varphi)$, akkor $\varphi(a) = 0$. Ezért $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0$. Azaz $ra \in I$, és hasonlóan $ar \in I$. A megfordítás *faktorgyűrű* segítségével később.

Ideálok.

5.1.6. Definíció
Egy R gyűrű egy I részhalmaza *balideál*, ha az összeadásra nézve részcsoport, és minden $a \in I$, $r \in R$ esetén $ra \in I$. Az I *jobbideál*, ha részcsoport, és minden $a \in I$, $r \in R$-re $ar \in I$. Az I (kétoldali) *ideál*, ha bal- és jobbideál is. Jele: $I \lhd R$.

Példa
A páros számok ideált alkotnak $\mathbb{Z}$-ben. Mert páros számok összege is páros, a nulla is páros, és páros szám ellentettje is páros, azaz részcsoport; továbbá páros szám minden egész számszorosa is páros.
Általában: Legyen $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n. Ennek magja az n-nel osztható számokból álló ideál. Jele: (n).
Speciálisan $(2) = (-2) =$ az összes páros szám.

Főideál.

5.1.10. Definíció
Legyen R *kommutatív* gyűrű és $s \in R$ rögzített. Álljon (s) az s összes többszöröseiből: $(s) = \{rs : r \in R\}$. Ennek neve az s által generált *főideál*.

HF: Az (s) halmaz tényleg mindig ideál.

Példa
$R = \mathbb{R}[x]$. Az $(x-1)$ az $x-1$-gyel osztható polinomokból áll. Ezek azok, melyeknek gyöke az 1 (gyöktényező kiemelhető). Ezért ha $\varphi : \mathbb{R}[x] \to \mathbb{R}$, $\varphi(f) = f(1)$ (φ az 1 behelyettesítése), akkor $\mathrm{Ker}(\varphi) = (x-1)$.

HF: Legyen $\varphi : \mathbb{R}[x] \to \mathbb{C}$, $\varphi(f) = f(i)$ (φ az i behelyettesítése).
Ekkor $\mathrm{Ker}(\varphi) = (x^2+1)$.
Segítség: ha i gyöke $f \in \mathbb{R}[x]$-nek, akkor a konjugáltja, azaz $-i$ is gyöke f-nek (4.7.7. Gyakorlat).

3. Egyszerű gyűrűk

Testek ideáljai.

5.3.2. Állítás
Egy testnek csak a triviális ideáljai vannak: (0) és önmaga.

Bizonyítás
Legyen T test és I ideálja F-nek, amely nem csak a nullából áll. Ha $0 \neq s \in I$, akkor $1 = ss^{-1} \in I$, hiszen I ideál. Tehát minden $r \in T$-re $r = 1r \in I$. Ezért $I = T$. $\square$

HF: Ferdetestnek minden balideálja és jobbideálja triviális.

5.3.1. Definíció
Az R *egyszerű* gyűrű, ha pontosan két ideálja van: (0) és R.

Főpélda (5.3.3): (Ferde)test fölötti teljes mátrixgyűrű egyszerű.

Kommutatív egyszerű gyűrűk.

Tétel (5.3.9. Következmény)
Minden kommutatív, egységelemes, egyszerű gyűrű test.

Bizonyítás
Ha R kommutatív, egységelemes, egyszerű gyűrű és $0 \neq s \in R$, akkor $s = 1s \in (s)$ miatt az (s) ideál nem (0), és így $(s) = R$. Ezért $1 \in (s)$, vagyis van olyan $r \in R$, hogy $sr = 1$. Tehát az s elem invertálható, és így R test. $\square$

Általánosítás (5.3.8. Tétel, NB)
Legyen R gyűrű, amelynek csak a két triviális balideálja van. Ekkor R vagy ferdetest, vagy olyan prímelemű gyűrű, amelyben bármely két elem szorzata nulla.

Ideálok és nullosztók.

Emlékeztető (2.2.27. Definíció)
Ha R gyűrű, $r, s \in R$ egyik sem nulla, de $rs = 0$, akkor r baloldali, s jobboldali *nullosztó*.

5.3.7. Lemma
Legyen $r \in R$ rögzített. Ekkor $\{x \in R : xr = 0\}$ balideál,
pontatlanul: az „r-hez tartozó” bal nullosztók balideált alkotnak.

Bizonyítás
Ha $xr = 0$ és $yr = 0$, akkor nyilván $(x \pm y)r = 0$.
Ha $xr = 0$ és $s \in R$, akkor pedig $(sx)r = s(xr) = s0 = 0$. □

Elnevezés: Ez az r elem bal oldali *annullátora*. Fontos szerepet játszik a balideálmentes gyűrűk leírásában.

Véges nullosztómentes gyűrű test.

5.3.5. Tétel
Minden véges, nullosztómentes gyűrű test.

Wedderburn tétele (6.7.13. Tétel, NB)
Minden véges ferdetest kommutatív.

Nehéz tétel, a nagyon szép bizonyítás benne van a jegyzetben. Így elég belátni, hogy véges nullosztómentes gyűrű *ferde*test.

Emlékeztető (2.2.8. Gyakorlat)
Nullosztómentes gyűrűben érvényes az *egyszerűsítési szabály:*
ha $ac = bc$ (vagy $ca = cb$), de $c \neq 0$, akkor $a = b$.

Bizonyítás: Ha $ac = bc$, akkor $(a - b)c = 0$. Mivel $c \neq 0$, a nullosztómentesség miatt $a - b = 0$. □

Véges nullosztómentes gyűrűk (bizonyítás).

5.3.4. Lemma
Ha R nullosztómentes, $e \in R$, és van olyan $0 \neq r \in R$, melyre $er = r$, akkor e egységelem.

Bizonyítás: Minden t-re $ter = tr$, az r-rel egyszerűsítve $te = t$. Tehát e jobboldali egységelem. Speciálisan $re = r$. Ugyanezt balról csinálva kapjuk, hogy e bal egységelem is. □

Bizonyítás (véges nullosztómentes gyűrű test)
Legyen $R = \{r_1, \ldots, r_n\}$ és $0 \neq r$. Ekkor $r_1 r, \ldots, r_n r$ a nullosztómentesség miatt csupa különböző elem. Mivel R véges, minden elemét megkapjuk. Speciálisan $r = r_i r$ esetén a Lemma miatt $e = r_i$ egységelem. Továbbá $e = r_j r$ esetén r-nek balinverze r_j. Ugyanezt a másik oldalról csinálva jobbinverzet kapunk. □