1. Főideálgyűrűk

Euklideszi gyűrű (lásd Algebra és számelmélet, 22. dia)

5.5.1. Definíció
Euklideszi gyűrű: „elvégezhető benne a maradékos osztás."
Az R szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha R nem nulla elemein értelmezve van egy nemnegatív egész értékű φ függvény úgy, hogy minden $a, b \in R$, $b \neq 0$ esetén létezik olyan $q, r \in R$, hogy $a = bq + r$, és $r = 0$ vagy $\varphi(r) < \varphi(b)$.

Példák
$\mathbb{Z}$ euklideszi: $\varphi(k) = |k|$.
$T[x]$ euklideszi, ha T test: $\varphi(f) = \mathrm{gr}(f)$.
Gauss-egészek: $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$.
Ez is euklideszi gyűrű: $\varphi(a + bi) = a^2 + b^2$.
Bizonyítás: Freud Róbert és Gyarmati Edit számelmélet könyve.

Euklideszi gyűrű főideálgyűrű

5.5.3. Tétel
Minden euklideszi gyűrű minden ideálja főideál.

Bizonyítás
Legyen I nem nulla ideál R-ben, és g a legkisebb φ-*értékű nem nulla* eleme. Belátjuk, hogy $I = (g)$.
Nyilván $(g) \subseteq I$, hiszen I tartalmazza g többszöröseit.
Legyen $f \in I$, ekkor $f = gq + r$, ahol $\varphi(r) < \varphi(g)$ vagy $r = 0$. De $r = f - gq \in I$, mert I zárt a többszörözésre és a kivonásra. Mivel $\varphi(g)$ minimális volt, így r csak nulla lehet. Tehát $f \in (g)$, azaz $I \subseteq (g)$. □

Főideálgyűrű: szokásos gyűrű, melynek minden ideálja főideál. Ezekben érvényes a *számelmélet alaptétele*.

2. Ideálok és számelmélet

Számelméleti alapfogalmak (ismétlés)

Ismétlés (3.1. Szakasz)
Szokásos gyűrű: kommutatív, nullosztómentes, egységelemes.
r *osztója* s-nek, ha van olyan t *a gyűrűben*, hogy $s = tr$.
Egység: mindent oszt. Legyen $r \in R$ *nem nulla, nem egység*.
Triviális felbontás: $r = ab$, ha valamelyik tényező egység.
r *felbonthatatlan*: nincs *nemtriviális* felbontása szorzatra (azaz minden felbontásában valamelyik tényező egység).
r *prím:* ha $r \mid ab$, akkor $r \mid a$ vagy $r \mid b$.

R alaptételes: minden nullától és egységtől különböző elem *egyértelműen* előáll felbonthatatlanok szorzataként.
Főpéldák alaptételes gyűrűre: $\mathbb{Z}$, $T[x]$ (T test), $\mathbb{Z}[x]$.
$a, b \in R$ kitüntetett közös osztója d, ha

(1) d közös osztó, azaz $d \mid a$ és $d \mid b$;

(2) d mindegyik közös osztónak többszöröse.

Az alapfogalmak összefüggései

3.1.27. Gyakorlat
Ha bármely két elemnek van kitüntetett közös osztója, akkor minden felbonthatatlan elem prím.

3.1.28. Gyakorlat
Ha minden felbonthatatlan elem prím, akkor igaz az alaptétel *egyértelműségi* állítása.

3.1.22. és 3.1.26. Gyakorlatok
Alaptételes gyűrűben

(1) bármely két elemnek van kitüntetett közös osztója;

(2) minden felbonthatatlan elem prím.

Ideálok és oszthatóság
5.1.10. Definíció: (r) az r összes többszöröséből áll: *főideál*.

5.5.4. Lemma
$r \mid s \iff (r) \supseteq (s)$. □

„Megfordul"! Például 2 kisebb, mint 4, de (2) nagyobb, mint (4).

5.5.5. Lemma
Legyen R szokásos gyűrű és $a, b \in R$. Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója. (A kitüntetett közös osztót is (a, b) jelölte számelméletben.)

Bizonyítás
Mivel $(d) = (a, b) \supseteq (a)$, ezért $d \mid a$, ugyanígy $d \mid b$. Ha $c \mid a$ és $c \mid b$, akkor $d = ra + sb$ miatt $c \mid d$. □

Euklideszi és főideálgyűrű alaptételes

Tétel (5.5.9. Következmény)
Minden főideálgyűrű (így minden euklideszi gyűrű) alaptételes.

Bizonyítás
Ha $(a,b)=(d)$, akkor d az a és b *kitüntetett közös osztója.* Ezért főideálgyűrűben (és így euklideszi gyűrűben) bármely két elemnek *van* kitüntetett közös osztója. Így érvényes az alaptétel egyértelműségi állítása.
A felbontás *létezését* nem bizonyítjuk.

$R=\mathbb{Z}[x]$ *alaptételes* gyűrű, 2 és x kitüntetett közös osztója 1, hiszen 2 osztói csak ±1, ±2, és $2\nmid x$.
$(2,x)$ azokból a polinomokból áll, melyek konstans tagja páros. Az 1 nem ilyen, tehát $(2,x)\neq(1)$, ezért $(2,x)$ *nem főideál.*
Tehát $\mathbb{Z}[x]$ nem főideálgyűrű, és így nem is euklideszi, noha alaptételes.

Példa nem alaptételes gyűrűre

3.1.34. Feladat
Legyen R az $a+bi\sqrt{5}$ alakú számokból álló gyűrű ($a,b\in\mathbb{Z}$).
A 9-nek és a $3(2+i\sqrt{5})$-nek *nincs kitüntetett közös osztója.*
A 3 *felbonthatatlan, de nem prím.*
Az alaptétel egyértelműségi állítása nem igaz:

$$9=3\cdot3=(2+i\sqrt{5})(2-i\sqrt{5}),$$

itt 3 is, $2\pm i\sqrt{5}$ is felbonthatatlan, de 3 nem egységszerese $2\pm i\sqrt{5}$-nek, így ez a 9-nek két, lényegesen különböző felbontása. Ezért ez a gyűrű *nem alaptételes.*

Az ilyen gyűrűk is hasznosak számelméleti problémák megoldásához. A kiút az, hogy a $(9,3(2+i\sqrt{5}))$ *ideál* veszi át a hiányzó kitüntetett közös osztó szerepét. Ez a témakör az *algebrai számelmélet.*

Direkt szorzat

5.1.17. Definíció
Az R és S gyűrűk *direkt szorzatának* alaphalmaza $R\times S$, ahol a műveleteket *komponensenként* végezzük:
$(r_1,s_1)+(r_2,s_2)=(r_1+r_2,s_1+s_2)$ és $(r_1,s_1)(r_2,s_2)=(r_1r_2,s_1s_2)$.

HF: Ez tényleg gyűrű. Hasonló a definíció kettőnél több tényező esetében is.
A belső jellemzés mint csoportokra (normálosztó helyett ideál):

5.1.18. Állítás
Ha I és J ideálok az R gyűrűben, a csoportelméleti $I+J$ komplexusösszeg az egész R, továbbá $I\cap J=0$, akkor $R\cong I\times J$.

A bizonyítás ötlete: Ha $I\cap J=0$, $a\in I$, $b\in J$, akkor $ab=0$.

3. Egyszerű gyűrűk

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. Ugyanígy van jobbinverze is. Ezek egyenlők (Algebra1, vagy 2.2.10. Feladat). □

Testek ideáljai

5.3.2. Állítás
Egy testnek csak a triviális ideáljai vannak: $\{0\}$ és önmaga.

Bizonyítás
Legyen T test és I ideálja T-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 $I = T$. □

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.
8.7.10, 8.7.12: A teljes mátrixgyűrű balideáljainak leírása.

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. □

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.

A faktorgyűrű mikor test
5.2.9. Állítás: Ha T test és $f \in T[x]$, akkor $T[x]/(f)$ pontosan akkor *test*, ha f *irreducibilis* T fölött.

Második, elegáns (számolásmentes) bizonyítás
Tegyük föl, hogy f irreducibilis, és legyen $T = T[x]/(f)$. Elég belátni, hogy R egységelemes, nullosztómentes és egyszerű. Nyilván $1 + (f)$ egységelem.
Ha $\big(g + (f)\big)\big(h + (f)\big)$ nulla R-ben, akkor $gh \in (f)$, azaz $f \mid gh$. Mivel $T[x]$ alaptételes, minden irreducibilis eleme prím. Ezért vagy $f \mid g$ vagy $f \mid h$. Az első esetben $g + (f)$, a másodikban $h + (f)$ lesz a nullelem R-ben. Így R nullosztómentes.

Ha $I \lhd R$, akkor álljon J azokból a $g \in T[x]$ polinomokból, melyekre $g+(f) \in I$. Ez ideál $T[x]$-ben, ezért főideál: $J = (h)$. Nyilván $(f) \subseteq J$, ezért $h \mid f$. Mivel (f) irreducibilis, vagy h egység, így $I = R$, vagy az f-nek egységszerese, és I az R nulla ideálja. □
(J az I teljes inverz képe a természetes homomorfizmusnál.)

Polinomok „nemlétező" gyökei

Példa
A z^2+1-nek nincs gyöke $\mathbb{R}$-ben, de i-vel kényelmes számolni. Ezért bevezettük $\mathbb{C}$-t, az $\mathbb{R}$ egy *testbővítését*. A bevezetés egy lehetséges módja a következő.

(1) Tudjuk, hogy $\mathbb{R}[x]/(x^2+1)$ izomorf $\mathbb{C}$-vel, és $a+bi$-nek az $a+bx+(x^2+1)$ mellékosztály felel meg. Így az $a+(x^2+1)$ alakú mellékosztályok $\mathbb{R}$-rel izomorf résztestet alkotnak, az i-nek megfelelő elem $x+(x^2+1)$.

(2) *Definiáljuk* $\mathbb{C}$-t $\mathbb{R}[x]/(x^2+1)$-nek, és igazoljuk, hogy test.

(3) *Azonosítsuk* $a \in \mathbb{R}$-et $a+(x^2+1)$-gyel, és mutassuk meg, hogy ezek az elemek $\mathbb{R}$-rel izomorf résztestet alkotnak.

(4) *Definiáljuk* i-t $x+(x^2+1)$-nek, és lássuk be, hogy ez gyöke a z^2+1 polinomnak.

Testbővítés konstrukciója

6.4.3. Tétel
Ha K test, és s egy K fölött irreducibilis polinom, akkor *létezik* olyan L test, amelyben K résztest, és amelyben az s polinomnak már *van gyöke*.

Bizonyítás
Legyen $L = K[x]/(s)$, ez test, mert s irreducibilis. A $k \mapsto k+(s)$ megfeleltetés nyilván művelettartó és injektív. Ezért a $k+(s)$ elemek ($k \in K$) a K-val izomorf résztestet alkotnak L-ben. Végezzük el a $k = k+(s)$ azonosítást (az azonosítás precíz részleteit lásd Kiss-jegyzet, 361. oldal). Legyen $\alpha = x+(s) \in L$. Be kell látni, hogy α gyöke s-nek. Ezzel a bizonyítást be is fejezzük majd.

Gyök a bővítésben

Bizonyítás (folytatás)
Legyen $s(z) = k_0 + k_1 z + \ldots + k_n z^n \in K[z]$. Az s-et $L[z]$-beli polinomnak képzeljük, hogy α-t helyettesíthessünk. Ezért s együtthatói a (k_j-vel azonosított) $k_j+(s)$ elemek. Így $\alpha = x+(s)$ miatt $s(\alpha) =$
$= \big(k_0+(s)\big) + \big(k_1+(s)\big)\big(x+(s)\big) + \ldots + \big(k_n+(s)\big)\big(x+(s)\big)^n =$
$= k_0 + k_1 x + \ldots + k_n x^n + (s) = s+(s) = (s)$, vagyis a $K[x]/(s)$ faktorgyűrű nulleleme. Ezért α tényleg gyöke az s polinomnak. □

A $\mathbb{Z}_2[x]/(x^2+x+1)$ négyelemű testben $E = 1 + (x^2+x+1)$, $0 = (x^2+x+1)$, $A = x + (x^2+x+1)$, $B = x+1+(x^2+x+1)$.
Azonosítás: $O \leftrightarrow 0$, $E \leftrightarrow 1$, $z^2+z+1 \leftrightarrow Ez^2+Ez+E$. Az $\alpha = A$ elem tényleg gyöke Ez^2+Ez+E-nek.

4. Karakterisztika, prímtest

Karakterisztika

Emlékeztető (2.2.19, 2.2.37)
Ha R gyűrű, $r \in R$ és $n \geq 0$ egész szám, akkor nr azt jelenti, hogy r-nek n példányát összeadjuk.
Ha $n < 0$, akkor nr a $(-n)r$ *ellentettje* (ami $(-n)(-r)$ is).

Ez R additív csoportjában a „hatványozás" (*többszörös*).

5.8.1. Állítás, 5.8.2. Definíció
Tegyük föl, hogy R *nullosztómentes* gyűrű. Ekkor vagy

(1) van olyan $p \in \mathbb{Z}$ prímszám, hogy $pr = 0$ minden $r \in R$-re,
ekkor R *karakterisztikája* p, vagy

(2) tetszőleges $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$ esetén $nr \neq 0$,
ekkor R *karakterisztikája* 0.

Valójában R^+ elemeinek *rendjeit* írjuk le.

Karakterisztika: bizonyítás

Bizonyítás
Tegyük föl, hogy $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$, melyre $nr = 0$. Az R^+ additív csoportban az elemrend jele $o(r)$. Tehát n „jó kitevője" (jó együtthatója) r-nek, és így $m = o(r) \mid n$. Persze $mr = 0$. Ha $s \in R$, akkor $0 = (mr)s = r(ms)$. Mivel R nullosztómentes és $r \neq 0$, innen $ms = 0$ adódik. Tehát $o(s)$ véges, és osztója $m = o(r)$-nek. Az r és s szerepét kicserélve $s \neq 0$ esetén $o(s) = o(r) = m$.
Az (1)-hez már csak azt kell megmutatni, hogy m prímszám. Tegyük föl, hogy $m = ab$, ahol a, b pozitív egészek. Ekkor

$$0 = (mr)r = (ar)(br).$$

Mivel R nullosztómentes, $ar = 0$ vagy $br = 0$. Az első esetben $m = o(r) \mid a$, vagyis $a \mid m$ miatt $a = m$. A második esetben ugyanígy kapjuk, hogy $b = m$. Ezért m tényleg prímszám. □

A Frobenius-endomorfizmus

5.8.4. Tétel
Legyen R kommutatív, p karakterisztikájú gyűrű, ahol p prím. Ekkor R-ben *tagonként lehet p-edik hatványra emelni*:

$$(r+s)^p = r^p + s^p \qquad (r, s \in R).$$

Ezért a $\psi(r) = r^p$ leképezés gyűrűhomomorfizmus R-ből R-be.
Neve: *Frobenius-endomorfizmus.* Ugyanez az állítás érvényes p hatványaira is.

Endomorfizmus: önmagába képző homomorfizmus.

ψ szorzattartása nyilvánvaló, mert R kommutatív. Az összegtartás a *binomiális tételből* következik. Elemi számelmélet: $\binom{p}{j}$ osztható p-vel, ha $0 < j < p$.
A p^k-ra emelés ψ^k (k tényezős kompozíció). □

Prímtest p karakterisztikában

5.8.7. Tétel
Legyen T egy $p > 0$ karakterisztikájú test, e az egységelem.
Ekkor $P = \{0, e, 2e, 3e, \ldots, (p-1)e\}$ $\mathbb{Z}_p$-vel izomorf résztest, amely T minden résztestének része (*legszűkebb résztest*).

A legszűkebb résztest neve: P a T *prímteste.*

Bizonyítás
Mivel $e \neq 0$ de $pe = 0$, az e elem rendje p. Ezért P részcsoport és $m \mapsto me$ izomorfizmus $\mathbb{Z}_p^+$ és P^+ között.
Ez tartja a szorzást is: $(me)(ne) = (mn)e^2 = (mn)e$.
Legszűkebb: Legyen $K \leq T$ résztest. Ekkor $K \neq \{0\}$, és így $K^\times$ részcsoportja $T^\times$-nek. Ezért T egységeleme, $e \in K$. Így $P \subseteq K$. □

Prímtest 0 karakterisztikában

5.8.7. Tétel
Legyen T egy 0 karakterisztikájú test, e az egységelem.
Ekkor $P = \{(me)/(ne) : m, n \in \mathbb{Z},\ n \neq 0\}$ egy $\mathbb{Q}$-val izomorf résztest, amely T minden résztestének része (*prímtest*).

Bizonyítás
Mivel $e \neq 0$ és a karakterisztika 0, az e elem rendje végtelen. Ellenőrizni kell, hogy $\psi : m/n \mapsto (me)/(ne)$ jóldefiniált, és izomorfizmus $\mathbb{Q}$ és P között.
Művelettartó: nyilván. Jóldefiniált: $m/n = u/v \implies (me)/(ne) = (ue)(ve)$ HF.
Továbbá $ne \neq 0$ ha $n \neq 0$, mert e rendje végtelen.
Szürjektív: nyilván. Injektív: elég, hogy $\mathrm{Ker}(\psi) = \{0\}$. Ha $(me)/(ne) = 0$ akkor $me = 0$, ezért $m = 0$ mert $o(e) = \infty$.
Legszűkebb: mint a p karakterisztikájú esetben. □

5. Algebrák test fölött

Az algebra fogalma

5.10.3. Definíció
A algebra a T test fölött, ha egyszerre gyűrű, vektortér T fölött,
és $\lambda(ab) = (\lambda a)b = a(\lambda b)$ minden $a, b \in A$ és $\lambda \in T$ esetén.

Legyen R egységelemes gyűrű, T részteste R-nek, és $1_R = 1_T$. Az R akkor algebra T fölött, ha $\lambda r = r\lambda$ ($\forall \lambda \in T$, $\forall r \in R$). (A T egy elemével, mint skalárral való szorzás az R-beli szorzás.)

Példák

- A $T[x_1, \ldots, x_n]$ polinomgyűrű a T test fölött.
- Ha $K \leq L$ testbővítés, akkor L a K fölött.
- A T test fölötti $n \times n$-es mátrixok.
- A T test fölötti V vektortér lineáris transzformációi.
- A kvaterniók ferdeteste $\mathbb{R}$ fölött.

Algebra elemének minimálpolinomja

5.10.6. Definíció
Ha A *algebra* a T test fölött, $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in T[x]$ és $b \in A$, akkor $f(b) = a_0 1_A + a_1 b + \ldots + a_n b^n$ (behelyettesítés).

Tehát f konstans tagját A egységelemével szorozzuk.
5.10.7. Gyakorlat: $f(a) + g(a) = (f+g)(a)$ és $(fg)(a) = f(a)g(a)$.

5.10.8, 5.10.11. Definíció
Az $f \in T[x]$ *jó polinomja* $b \in A$-nak, ha $f(b) = 0$. Ezek egy I ideált alkotnak, ami az $f \mapsto f(b)$ homomorfizmus magja. Ha $I = \{0\}$, akkor b *transzcendens*, különben *algebrai*. Ekkor az I főideál normált generátoreleme a $b \in A$ *minimálpolinomja*, jele m_b. Továbbá $f(b) = 0 \iff m_b \mid f$.

Bizonyítás: mint a testbővítéseknél.

A minimálpolinom irreducibilitása

5.10.9. Állítás
Véges dimenziós algebra minden eleme algebrai.

Valóban: ha $\dim_T(A) = n$, akkor $1, b, \ldots, b^n$ már összefügg:
$\lambda_0 1 + \lambda_1 b + \ldots + \lambda_n b^n = 0$. Legyen $f(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_n x^n$,
ekkor f nem 0, és b gyöke f-nek. □

5.10.12. Tétel
Legyen A nullosztómentes algebra és $b \in A$ algebrai elem. Ekkor b minimálpolinomja irreduciblis T fölött.
Ha $f \in T[x]$ normált, irreducibilis és $f(b) = 0$, akkor $f = m_b$.

Valóban: ha $m_b = gh$, akkor $0 = m_b(b) = g(b)h(b)$. Ezért vagy $g(b) = 0$ (így $m_b \mid g$ miatt h egység), vagy $h(b) = 0$ és g egység.
Megfordítva: ha $f(b) = 0$, akkor $m_b \mid f$, de mindkettő irreducibilis és normált, ezért egyenlők. □

6. A számfogalom lezárása

Frobenius tétele

5.11.6. Tétel, NB
Ha A véges dimenziós, nullosztómentes, nem nulla algebra $\mathbb{R}$ fölött, akkor A vagy a valós számtesttel, vagy a komplex számtesttel, vagy a kvaterniók ferdetestével izomorf.

Vagyis a számkört nem lehet már tovább bővíteni, ha a nullosztómentességet és az asszociativitást megtartjuk.

A Frobenius-tétel feltételei szükségesek (5.11.1. Gyakorlat)

- Ha nem $\mathbb{R}$ fölött vagyunk: $\mathbb{Q}$ véges bővítései mind nullosztómentesek és véges dimenziósak (pl. $\mathbb{Q}(\sqrt[n]{2})$).
- $\mathbb{R}[x]$ nullosztómentes, $\mathbb{R}$ fölötti, de nem véges dimenziós. Sőt, $\mathbb{R}$ egyszerű transzcendens bővítése még test is.
- $\mathbb{R}^{3\times 3}$ véges dimenziós, $\mathbb{R}$ fölötti, de nem nullosztómentes.

A polinomok azonossági tétele

5.11.5. Következmény
Az x^2+1 polinomnak a kvaterniók között végtelen sok gyöke van. Ezek pontosan azok, amelyek valós része nulla és normája 1, vagyis a $qi+rj+sk$ alakú kvaterniók, ahol $q^2+r^2+s^2=1$.
HF: Az $\alpha = a+bi+cj+dk$ minimálpolinomja $x^2-2ax+N(\alpha)$.

Valóban, ha $N(z)=1$ és $\overline{z}=-z$, akkor $z^2=-z\overline{z}=-N(z)=-1$.
Megfordítva: ha $z^2=-1$, akkor $1=N(z^2)=N(z)^2$, így $N(z)=1$. Ezért $1=z\overline{z}=-z^2$. Innen $z\neq 0$ miatt $\overline{z}=-z$. □

Hogyan lehet egy másodfokú polinomnak végtelen sok gyöke?
Magyarázat: $x^2+1=(x+i)(x-i)$ a „gyöktényezős alak”.
Ide $j\in\mathbb{K}$-t helyettesítve a bal oldal nulla lesz, de a jobb oldal nem:
$(j+i)(j-i)=j^2+ij-ji-i^2=ij-ji=2k\neq 0$.
Mivel $ij\neq ji$, nem tudjuk kihasználni, hogy $\mathbb{K}$ nullosztómentes.

7. A kvaterniók alkalmazásai

Kvaterniók és térvektorok

Tiszta kvaternió: $v=xi+yj+zk$ (valós része nulla). Azonosítsuk ezzel az $(x,y,z)^T\in\mathbb{R}^3$ vektort. Legyen $z=r+v$ ($r\in\mathbb{R}$).

- Ha $N(z)=1$, akkor $z^{-1}=\overline{z}$. Ha z tiszta is, akkor $z^{-1}=-z$.

- Ha v és w tiszta kvaterniók, akkor $vw = v \times w - \langle v, w \rangle$ (vektoriális, illetve skaláris szorzat), mert $i^2 = j^2 = k^2 = -1$, továbbá $ij = i \times j$, $ji = j \times i$, $jk = j \times k$, stb.

- Így ha $v \perp w$, akkor $vw = v \times w = -w \times v = -wv$, ahonnan $w^{-1}vw = -v$, és $w^{-1}zw = w^{-1}rw + w^{-1}vw = r - v = \overline{z}$.
  Balról zw-vel szorozva $zw\overline{z} = z^2 w$.

- Tehát ha $N(z) = 1$ és $v \perp w$, akkor $zwz^{-1} = z^2 w$.
  Speciálisan ha $z = \cos\alpha + v \sin\alpha$, ahol $N(v) = 1$, akkor $v^2 = -1$ (mert v tiszta), $z^2 = \cos(2\alpha) + v\sin(2\alpha)$, és így $zwz^{-1} = \cos(2\alpha)w + \sin(2\alpha)vw = \cos(2\alpha)w + \sin(2\alpha)(v \times w)$.
  Ha $N(w)$ is 1, akkor v, w és $v \times w$ ONB a térben. □

Kvaterniók és forgatások

Tétel
A térbeli, origón átmenő egyenesek körüli forgatások a(z 1 normájú) kvaterniókkal való konjugálások. Pontosabban:
ha v egységvektor, akkor a $z = \cos\alpha + v\sin\alpha$-val való konjugálás 2α szögű forgatás a v irányú egyenes körül.

Bizonyítás
Legyen w egy v-re merőleges egységvektor. Írjuk föl a z-vel való konjugálás mátrixát a v, w, $vw = v \times w$ ONB-ben. Nyilván $zvz^{-1} = v$ (hiszen $zv = vz$), és az iménti képletek alapján
$zwz^{-1} = \cos(2\alpha)w + \sin(2\alpha)(vw)$. A kettőt összeszorozva
$z(vw)z^{-1} = (zvz^{-1})(zwz^{-1}) = \cos(2\alpha)(vw) + \sin(2\alpha)v(vw)$,
ahol $v(vw) = v^2 w = -w$ (már láttuk, hogy $v^2 = -1$).
Ezért a megfelelő forgatás mátrixát kapjuk. □

Euler-mátrix

Az előző bizonyításban kapott mátrix:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(2\alpha) & -\sin(2\alpha) \\ 0 & \sin(2\alpha) & \cos(2\alpha) \end{pmatrix}$$

Az i, j, k bázisban, $z = r + xi + yj + zk$ esetén (*Euler-mátrix*):

$$\begin{pmatrix} r^2 + x^2 - y^2 - z^2 & -2rz + 2xy & 2ry + 2xz \\ 2rz + 2xy & r^2 - x^2 + y^2 - z^2 & -2rx + 2yz \\ -2ry + 2xz & 2rx + 2yz & r^2 - x^2 - y^2 + z^2 \end{pmatrix}$$

Előnyök:
Csak négy paraméter; numerikusan stabil; effektív.
Forgástengely folytonos változtatása (3D játékok grafikája).
Navigáció, aerodinamika, molekuláris dinamika, röntgenkristallográfia.
Számelméleti alkalmazások.

8. A kvaterniók csoportelméleti vonatkozásai

A kvaterniók mint transzformációk
A kvaternók vektortér $\mathbb{C}$ fölött (a skalárral szorzás balszorzás).
FIGYELEM: ez *NEM* algebra $\mathbb{C}$ fölött, mert $i(j1) \neq j(i1)$.

Legyen A_z a $z \in \mathbb{K}$-val való jobbszorzás $\mathbb{K}$-n: $A_z(x) = xz$. Ez összegtartó. Skalárszorostartó is az asszociativitás miatt: $A_z(\lambda x) = (\lambda x)z = \lambda(xz) = \lambda A_z(x)$ (ahol $\lambda \in \mathbb{C}$ és $x \in \mathbb{K}$). Továbbá $A_{z_1 z_2}(x) = x(z_1 z_2) = (xz_1)z_2 = A_{z_2} A_{z_1}(x)$. Azaz a $\psi : z \mapsto A_z$ leképezésre $\psi(z_1 z_2) = \psi(z_2)\psi(z_1)$.
Kellemetlen: megfordul a szorzás sorrendje. Megoldás: legyen $\psi(z) = A_{\overline{z}}$.
Erre $\psi(z_1 z_2) = \psi(z_1)\psi(z_2)$, hiszen $\overline{z_1 z_2} = \overline{z_2}\,\overline{z_1}$.
Továbbá $\psi(z_1 + z_2) = \psi(z_1) + \psi(z_2)$, azaz ψ gyűrűhomomorfizmus.
Végül ψ injektív: ha $\psi(z) = 0$, akkor $0 = \psi(z)(1) = 1\overline{z}$, így $z = 0$.
Tehát a $\mathbb{K}$ gyűrű izomorf $\mathrm{Hom}(\mathbb{C}^2)$ egy részgyűrűjével.

Ha $z = p + qi + rj + sk$, akkor $\psi(z)$ mátrixa az $(1, j)$ bázisban $\begin{pmatrix} v & w \\ -\overline{w} & \overline{v} \end{pmatrix}$ ahol $v = p + qi$ és $w = r + si$ (így vezettük be $\mathbb{K}$-t).

A speciális unitér csoport

Ha $0 \neq v, w \in \mathbb{C}^2$ hossza egyenlő, akkor pontosan egy olyan 1 determinánsú, unitér transzformáció van, ami v-t w-be viszi.

Bizonyítás
Tegyük föl, hogy van kettő: $B(v) = C(v)$. Legyen $D = B^{-1}C$, ekkor $D(v) = v$.
Ha u egy v-re merőleges egységvektor, akkor $D(u) \perp D(v) = v$, és így $D(u) \parallel u$.
A (v, u) bázisban $\det(D)$-t felírva $D(u) = u$, azaz D az identitás, és így $B = C$.
Legyen $b_1 = v/\|v\|$, $c_1 = w/\|w\|$, és (b_1, b_2), (c_1, c_2) ONB.
Előírhatósági tétel: van B, melyre $B(b_1) = c_1$ és $B(b_2) = \varepsilon c_2$.
Alkalmas $|\varepsilon| = 1$-re B unitér, 1 determinánsú és $B(v) = w$. □

Jelölje SU(2) a 2×2-es, komplex elemű, 1 determinánsú *unitér* mátrixok csoportját a szorzásra (4.1.26. Definíció).
Elnevezés: SU(2) *regulárisan* hat az egységvektorok halmazán.

Az egységkvaterniók csoportja

Tétel
Az 1 normájú kvaterniók multiplikatív csoportja izomorf SU(2)-vel.

Bizonyítás
Ha $z \in \mathbb{K}$, akkor láttuk, hogy $\psi(z) = A_{\overline{z}}$ mátrixa $\begin{pmatrix} v & w \\ -\overline{w} & \overline{v} \end{pmatrix}$, melynek determinánsa $N(z)$ és adjungáltja A_z mátrixa.
Ha $N(z) = 1$, akkor tehát $\psi(z)$ unitér és determinánsa 1.

Megfordítás: Tegyük föl, hogy A unitér, 1 determinánsú $\mathbb{K}$-n.
Legyen $z = \overline{A(1)}$, ekkor $A(1) = \overline{z} = 1\overline{z} = A_{\overline{z}}(1)$.
Ezért az imént bizonyított állítás miatt $A = A_{\overline{z}}$. □

Az SU(2)-t Spin(3) csoportnak nevezik a kvantumfizikában. Fermionok (pl. neutron) leírására használják.

Miért kétszereződik a szög?

Tétel
$\mathrm{SU}(2)/\{1,-1\} \cong \mathrm{SO}(3)$ (a térbeli forgatások csoportja).

Bizonyítás
Legyen $z = \cos\alpha + v\sin\alpha$, ahol v egységvektor.
Láttuk: $F_z : w \to zwz^{-1}$ a v irányú egyenes körüli 2α szögű forgatás.
Nyilván $\varphi : z \to F_z$ homomorfizmus, melynek magja $\{1,-1\}$. □

Algebrai magyarázat: a $zwz^{-1} = z^2w$ képlet, ha $v \perp w$.
Geometriai magyarázat: a $z \mapsto F_z$ homomorfizmus magja kételemű. Ezért SU(2) az SO(3) minden elemét kétszer „fedi le".
Tekintsük az $f : \alpha \to z$ függvényt, miközben v fix, pl. $v = i$. Ha $0 \le \alpha \le 2\pi$, akkor $f(\alpha)$ végighalad a komplex egységkörön. De $\varphi\big(f(\alpha)\big)$ kétszer halad körbe, már π-nél az identititás, és ezért kétszeres „sebességgel" halad.

9. Összefoglaló

A 17. előadás összefoglalója

Fogalmak
Főideálgyűrű. Gyűrűk direkt szorzata. Egyszerű gyűrű. Karakterisztika, prímtest, Frobenius-endomorfizmus. Test fölötti algebra, elem minimálpolinomja. Euler-mátrix.

Tételek
Euklideszi gyűrű főideálgyűrű, főideálgyűrű alaptételes. Főideálok tartalmazása és oszthatóság.
Véges nullosztómentes gyűrű test. Kommutatív, egységelemes, egyszerű gyűrű test. Egyszerű testbővítés konstrukciója faktorgyűrűként. A prímtestek szerkezete. Frobenius tétele. Kvaterniók csoportelméleti vonatkozásai.