Algebra 4

Pelikán József előadásai alapján lejegyezte Forrás Bence

2016. május 28.

Tartalomjegyzék

1. Alapvető fogalmak

Definíció. R gyűrű

Állítás. $\forall a \in R : 0 \cdot a = a \cdot 0 = 0$.

Definíció. Kommutatív gyűrű.

Állítás. $(-a)b = -ab$, $a(-b) = -ab$, $(-a)(-b) = ab$ $\forall a, b \in R$.

Definíció. Balegységelem, jobbegységelem, (kétoldali) egységelem.

Észrevétel. *Ha e balegységelem és f jobbegységelem, akkor $e = f = ef$ kétoldali egységelem.*

Jelölés. Az egységelem jelölése 1.

Állítás. *Ha egyetlen balegységelem van, az kétoldali egység is.*

Definíció. Egységelemes gyűrű. Balinverz, jobbinverz.

Állítás. *Ha egy elemnek van bal- és jobbinverze is, azok az egyetlen kétoldali inverz.*

Definíció. Egység.

Állítás. *Az egységek csoportot alkotnak a gyűrűn belüli szorzásra.*

Definíció. Test.

Definíció. R feletti polinomgyűrű: $R[x]$.

Definíció. R feletti formális hatványsorok gyűrűje: $R[[x]]$.

Állítás. $U(R[[x]]) = \left\{\sum a_j x^j : a_0 \in U(R)\right\}$.

Észrevétel. *R kommutatív $\implies$ $R[x]$ és $R[[x]]$ kommutatív.*

Definíció. $M_n(R)$ mátrixgyűrű.

Észrevétel. *Ha R egységelemes, akkor $M_n(R)$ is az.*

Definíció. Bal oldali nullosztó.

Definíció. Nullosztómentes gyűrű.

Példa. $M_n(R)$-ben van nullosztó minden $n \geq 2$-re.

Definíció. Zérógyűrű.

Definíció. Integritási tartomány.

Definíció. $\mathbb{Z}\left[\sqrt{d}\right]$.

Példa. $\mathbb{Z}\left[\sqrt{d}\right]$ egységelemes integritási tartomány minden $d \neq 0, 1$-re.

2. Részgyűrűk, ideálok, homomorfizmusok

Definíció. Részgyűrű.

Definíció. Ideál.

Definíció. Balideál, jobbideál.

Definíció. Homomorfizmus.

Definíció. $\operatorname{Ker}\varphi$.

Állítás. $\operatorname{Ker}\varphi \triangleleft R$.

Definíció. Faktorgyűrű (maradékosztály-gyűrű).

Definíció. Természetes homomorfizmus.

Definíció. Izomorfizmus.

Tétel. *Homomorfizmustétel.*

Definíció. Generált részgyűrű.

Definíció. Generált ideál.

Észrevétel. *Ideálok metszete is ideál.*

Állítás. $(I,J) = I + J$, *ahol* $I, J \triangleleft R$.

Definíció. $I \cdot J = \{\sum_{i=1}^{n} a_i b_i : a_i \in I, b_i \in J\}$.

Észrevétel. $IJ \subseteq I \cap J \subseteq I + J$.

Definíció. Főideál.

Megjegyzés. A főideál explicit alakban is felírható.

$$(a) = \left\{ na + ra + as + \sum_{i=1}^{n} r_i a s_1 : n \in \mathbb{Z}; r, s \in R; r_i, s_i \in R \right\}$$

$$(a) = \left\{ \sum_{i=1}^{n} r_i a s_1 : n \in \mathbb{Z}; r, s \in R; r_i, s_i \in R \right\}, \qquad \text{ha } 1 \in R$$

$$(a) = \{ na + ra : n \in \mathbb{Z}; r, s \in R; r_i, s_i \in R \}, \qquad \text{ha } R \text{ kommutatív}$$

$$(a) = \{ ra : n \in \mathbb{Z}; r, s \in R; r_i, s_i \in R \}, \qquad \text{ha } 1 \in R \text{ és } R \text{ kommutatív}$$

Megjegyzés. Mindezek megfogalmazhatók bal- és jobbideálokra is.

3. Modulusok

Definíció. M baloldali modulusa R-nek, ha

1. $(M,+)$ Abel-csoport
2. $(rs)m = r(sm)$
3. $(r+s)m = rm + sm$ és $r(m+n) = rm + rn$.

Ha $1 \in R$, és $1m = m$, akkor a modulus unitális.

Definíció. Részmodulus.

Definíció. Generált részmodulus.

Definíció. Homomorfizmus, homomorfizmus magja.

Tétel. *Homomorfizmustétel.*

Definíció. Jobboldali R-modulus.

Jelölés. ${}_RM$, M_R.

Példa. $\mathbb{Z}$-modulus $\leftrightarrow$ additívan írt Abel-csoport. $K[x]$: K-vektortér egy rögzített lineáris transzformációval. ${}_RR, R_R$: részmodulusai a bal-, illetve jobbideálok.

Definíció. Modulusok direkt összege: $\oplus_{\alpha\in I} M_\alpha$. Végtelen I-re a diszkrét direkt összeget tekintjük.

Definíció. $\underset{\alpha\in I}{\oplus}\, {}_RR$ szabad modulus.

Tétel (BN)**.** *Ferdetest felett minden modulus szabad. Ha minden unitális R-modulus szabad, akkor R ferdetest.*

Definíció. M egyszerű, ha csak 0 és M a részmodulusai.

4. Egyszerű gyűrűk

Definíció. R egyszerű, ha csak 0 és I az ideáljai.

Állítás. *Ferdetestnek nincs nemtriviális balideálja.*

Példa. Minden ferdetest egyszerű gyűrű.

Definíció. Gyűrűk direkt összege: $\oplus_{\alpha\in I} R_\alpha$.

Észrevétel. *Az egyes direkt összeadandók kétoldali ideálok lesznek.*

Tétel. *Ha $|R| > 1$ és $\forall a \neq 0, b \in R$-re $ax = b$ megoldható (nem feltétlenül egyértelműen), akkor R ferdetest.*

Állítás. *Ha R-ben nincs balideál, akkor ferdetest vagy prímrendű zérógyűrű.*

Következmény. *Ha R kommutatív egyszerű gyűrű, akkor test vagy prímrendű zérógyűrű.*

Állítás. *Legyen $1 \in R$. Ekkor $I \triangleleft M_n(R) \iff I = M_n(A)$, ahol $A \triangleleft R$.*

Következmény. *Ha R egyszerű, akkor $M_n(R)$ is egyszerű.*

5. Prímideál, maximális ideál, nilradikál, Jacobson-radikál

Definíció. Nilpotens elem.

Definíció. Nilradikál: $N(R) = \{a \in R : a \text{ nilpotens}\}$.

Tétel. *Ha $1 \in R$ és R kommutatív, akkor $N(R) \lhd R$.*

Megjegyzés. $N\left({}^{R}/_{N(R)}\right) = 0$.

Definíció. Legyen $1 \in R$ és R kommutatív. Ekkor a $P \lhd R$, $P \neq R$ ideál prímideál, ha $x, y \in R$, $xy \in P$ esetén $x \in P$ vagy $y \in P$ fennáll.

Megjegyzés. 0 pontosan akkor prímideál, ha R nullosztómentes.

Példa. $\mathbb{Z}$ ideáljai $(n) = n\mathbb{Z}$ alakúak ($n \geq 0$). (n) pontosan akkor prímideál, ha n prímszám vagy nulla.

Kritérium. *Egységelemes kommutatív gyűrűben $I \lhd R$ prímideál akkor és csak akkor, ha ${}^{R}/_{I}$ nullosztómentes.*

Definíció. Maximális ideál: $M \lhd_{\max} R$, ha $M \subseteq A \lhd R \implies A = R$.

Kritérium. *Egységelemes kommutatív gyűrűben $I \lhd R$, $I \neq R$ ideál akkor és csak akkor maximális, ha ${}^{R}/_{I}$ test.*

Következmény. *Minden maximális ideál prím.*

Példa. A megfordítás nem igaz: $\mathbb{Z}$-ben 0 prím, de $(0) \subset (p) \lhd \mathbb{Z}$.

Definíció. Főideálgyűrű: olyan egységelemes integritási tartomány, melyben minden ideál főideál. (PID, principal ideal domain)

Példa. $\mathbb{Z}$ és $K[x]$ főideálgyűrűk, de $K[x, y]$ nem az: (x, y) nem főideál.

Állítás. *Ha R főideálgyűrű, akkor minden nemnulla prímideálja maximális.*

Állítás. $1 \in R$, $A \lhd R$, $A \neq R \implies \exists M \lhd_{\max} R : A \subseteq M$.

Megjegyzés. Speciálisan $\forall a \notin U(R)\ \exists M \lhd_{\max} R\ a \in M$.

Tétel. *Kommutatív egységelemes gyűrűben $N(R) = \bigcap_{P \lhd R \text{ prím}} P$.*

Definíció. Jacobson-radikál: kommutatív gyűrűben $J(R) = \bigcap_{M \lhd_{\max} R} M$.

Állítás. $\forall a \in R : a \in J(R) \iff 1 - ax \in U(R)\, \forall x \in R$.

6. Artin- és noether-tulajdonságok

Minden gyűrű egységelemes, minden modulus unitális.

Definíció. ${}_{R}M$-re teljesül a minimumfeltétel (artin-modulus), ha teljesülnek a következő ekvivalens feltételek:

1. M részmodulusainak tetszőleges halmazában van minimális,
2. nem létezik $M_1 > M_2 > \ldots$ szigorúan csökkenő végtelen részsorozat,

2' ha $M_1 \geq M_2 \geq \ldots$, akkor $\exists n$: $M_n = M_{n+1} = \ldots$.

Hasonlóan M_R-re.

Definíció. ${}_RM$-re teljesül a maximumfeltétel (noether-modulus), ha teljesülnek a következő ekvivalens feltételek:

1. M részmodulusainak tetszőleges halmazában van maximális,
2. nem létezik $M_1 < M_2 < \ldots$ szigorúan növekvő végtelen részsorozat,

2'. ha $M_1 \leq M_2 \leq \ldots$, akkor $\exists n$: $M_n = M_{n+1} = \ldots$.

Hasonlóan M_R-re.

Definíció. Egy R gyűrű artin, illetve noether, ha önmaga felett vett modulusként az. Bal-artin, ha a minimumfeltétel balideálokra teljesül stb.

Megjegyzés. Minden véges gyűrű és modulus artin és noether is.

Példa. Z_∞ nem artin, de noether. Z_{p^∞} artin, de nem noether.

Tétel (Hopkins–Levitzki, BN)**.** *Ha egy egységelemes gyűrű bal-artin, akkor bal-noether is.*

Tétel (Hilbert bázistétele)**.** *Ha $1 \in R$ bal-noether, akkor $R[x]$ is bal-noether.*

Definíció. Legyen $X \subseteq K[x_1, \ldots, x_n]$. Ekkor az X által meghatározott affin algebrai halmaz $V(X) = \{(a_1, \ldots, a_n) \in K^n : f(a_1, \ldots, a_n) = 0 \ \forall f \in X\}$. $V(X)$ algebrai varietás (algebrai sokaság), ha nem bomlik fel algebrai halmazok uniójára.

Példa. Minden főideálgyűrű noether.

Tétel. *Legyen D ferdetest. $L \lhd_{\mathrm{b}} M_n(D)$ akkor és csak akkor, ha létezik olyan V altér a D feletti n dimenziós ${}_nD$ balvektortérben, hogy az L-beli mátrixok minden sora V-beli.*

Példa. $M_n(D)$ bal-artin.

Megjegyzés. Létezik bal-, de nem jobb-noether-gyűrű. Ugyanez fennáll artinra is.

7. Féligegyszerű modulusok és gyűrűk

Minden gyűrű egységelemes, minden modulus unitális.

Definíció. M féligegyszerű modulus, ha $\forall N \leq M \ \exists N^* \leq M$: $M = N \oplus N^*$, azaz minden részmodulus direkt összeadandó.

Állítás. *M féligegyszerű modulus minden részmodulusa is féligegyszerű.*

Állítás. *M féligegyszerű modulus minden faktormodulusa is féligegyszerű.*

Lemma. *Minden féligegyszerű nemnulla modulus tartalmaz egyszerű részmodulust.*

Tétel. *Legyen M baloldali R-modulus. A következők ekvivalensek:*

1. *M féligegyszerű;*
2. *$M = \oplus M_\alpha$, M egyszerű;*

3. $M = \sum M_\alpha$, M *egyszerű.*

Tétel. *A következők ekvivalensek:*

1. *minden R-modulus féligegyszerű;*
2. *minden végesen generált R-modulus féligegyszerű;*
3. *minden ciklikus (1 elem által generált) R-modulus féligegyszerű;*
4. ${}_RR$ *féligegyszerű.*

Megjegyzés. M ciklikus akkor és csak akkor, ha $M \simeq {}_RR/_L$.

Definíció. A fenti tétel feltételeinek teljesülése esetén R féligegyszerű gyűrű.

Állítás. *Ha D ferdetest, akkor $M_n(D)$ féligegyszerű gyűrű.*

Állítás. *Minden féligegyszerű gyűrű előáll minimális balideálok direkt összegeként.*

8. Csoportgyűrűk, csoportalgebrák

Definíció. Legyen G csoport, R egységelemes gyűrű. Csoportgyűrű:

$$RG = \left\{ \sum_{i=1}^{n} r_i g_i : g_1, \ldots, g_n \in G;\ r_1, \ldots, r_n \in R \right\}.$$

A formális összegekre vonatkozó műveletek értelemszerűek. Ha R test, csoportalgebra. (Kommutatív gyűrűre, illetve véges csoportra érdekes, de ez nem része a definíciónak.)

Észrevétel. *RG egységelemes: $1_R \cdot 1_G$ egységelem.*

Definíció. *A K-*algebra, ha vektortér K felett és gyűrű. (A két összeadásművelet megegyezik.)

Példa. $M_n(K)$, $K[x]$, KG K-algebrák.

Észrevétel. *Ha A egységelemes, akkor minden ideál altér.*

Tétel (Maschke)**.** *Ha G véges csoport, K test,* $\operatorname{char} K \nmid G$*, akkor KG féligegyszerű. (Igaz a megfordítás is.)*

Megjegyzés. $r \in U(R)$, $g \in G$ esetén rg ún. triviális egység RG-ben.

Definíció. Gyűrű centruma: $Z(R) = \{r \in R : rt = tr\ \forall t \in R\}$.

Észrevétel. $Z(R) \leq R$. *(De ideál szinte soha.)*

Állítás. $Z(KG) = \left\{ \sum_{i=1}^{k(G)} \alpha_j C_j : \alpha_j \in K \right\}$, *ahol* $\mathcal{C}_1, \ldots, \mathcal{C}_k$ *a konjugáltosztályok,* $C_j = \sum_{x \in \mathcal{C}_j} x$.

9. Jacobson-radikál nemkommutatív gyűrűben

A gyűrűk egységelemesek, de nem feltétlenül kommutatívak.

Definíció. (Bal-)Jacobson-radikál: a maximális balideálok metszete.

Tétel. *$a \in R$-re ekvivalensek:*

1. *$a \in J(R)$;*
2. *$\forall x \in R : (1 - xa)$-nak van balinverze;*
3. *$\forall M$ egyszerű modulusra $aM = 0$, azaz $\forall m \in M : \ am = 0$.*

Állítás. *$J(R) \triangleleft R$.*

Definíció. $\mathrm{Ann}(M) = \{r \in R : \ rM = 0\}$ az M R-beli annullátor-ideálja.

Állítás. *A fenti tétel feltételei ekvivalensek a következő 2') feltétellel: $\forall x, y \in R : \ (1 - xay) \in U(R)$.*

Következmény. *A bal-Jacobson- és a jobb-Jacobson-radikál megegyeznek.*

10. Hányadostest

Tétel. *Ha R integritási tartomány, akkor egyértelműen létezik egy olyan K test, hogy $R \leq K$ és $\forall a \in K \ \exists c, d \in R : \ a = \frac{c}{d}$.*

Definíció. K az R hányadosteste.

Példa. $\mathbb{Z}$ hányadosteste $\mathbb{Q}$, $K[x]$ hányadosteste $K(x)$, $K[[x]]$ hányadosteste a Laurent-sorok $\sum_{j=-n}^{\infty} a_j x^j$ teste.

Állítás. *Ha R tetszőleges gyűrű, akkor létezik olyan R_1 egységelemes gyűrű, hogy $R \triangleleft R_1$.*

Megjegyzés. Létezik olyan nemkommutatív nullosztómentes gyűrű, ami nem ágyazható be ferdetestbe.

11. Testbővítések

Definíció. $L|K$ testbővítés, ha $K \leq L$ testek.

Megjegyzés. Ekkor L automatikusan vektortér K felett.

Definíció. L mint K-vektortér dimenziója L felett a testbővítés foka: $(L : K) = \dim_K L$.

Példa. $(\mathbb{C} : \mathbb{Q}) = \infty$, $(\mathbb{C} : \mathbb{R}) = 2$.

Definíció. $L|K$ véges bővítés, ha $(L : K) < \infty$.

Tétel (Fokszámtétel)**.** $K \leq L \leq M \implies (M : K) = (M : L) \cdot (L : K)$. *(A végtelen eseteket is beleértve.)*

Következmény. *Prímfokú bővítésnél nincs közbülső test.*

Definíció. Ha $L|K$, $\alpha \in L$, akkor ha létezik $f \in K[x]$, amire $f(\alpha) = 0$, akkor α algebrai K felett. Ha nincs ilyen f, akkor α transzcendens K felett.

Definíció. Legyen $I = \{g(x) \in K[x] : g(\alpha) = 0\}$. I ideál $K[x]$-ben, ami főideálgyűrű, tehát $I = (p(x))$ valamely p-re. Ez konstans szorzó erejéig meghatározott, ezek közül az 1 főegyütthatójút nevezzük α kanonikus polinomjának.

Észrevétel. *$p(x)$ irreducibilis $K[x]$ felett. Ez fordítva is igaz: az 1 főegyütthatójú irreducibilis polinomok kanonikusak.*

Példa. $K = \mathbb{Q}$, $L = \mathbb{R}$, $\alpha = \sqrt{2}$-re $p(x) = x^2 - 2$.

Definíció. Ha $L|K$ és $\alpha_1, \ldots, \alpha_r \in L$, akkor $K(\alpha_1, \ldots, \alpha_r)$ a legszűkebb ezen elemeket is tartalmazó bővítés. Ha egyetlen elemről van szó, akkor $K(\alpha)$ az α adjunkciója K-hoz. (A definiált testek léteznek, mert L-beli tartalmazó résztestek metszete tartalmazó résztest.)

Állítás. *Ha $L|K$, $\alpha \in L$ algebrai elem $p(x)$ kanonikus polinommal, akkor $K(\alpha) \simeq {}^{K[x]}/_{\left(p(x)\right)}$.*

Következmény. *$(K(\alpha) : K) = \deg p$, sőt $1, \alpha, \alpha^2, \ldots, \alpha^{\deg p - 1}$ bázisa $K(\alpha)$-nak K felett.*

Definíció. Az $L|K$ bővítés algebrai, ha L minden eleme algebrai K felett.

Állítás. *Minden véges bővítés algebrai.*

Tétel. *Ha $L|K$ adott, $\alpha, \beta \in L$ algebrai elemek, akkor $\alpha + \beta$, $-\alpha$, $\alpha\beta$ és $\frac{1}{\alpha}$ is algebrai (utóbbinál feltéve, hogy $\alpha \neq 0$).*

Következmény. $K \leq K_0 = \{\alpha \in L : \alpha \text{ algebrai } K \text{ felett}\} \leq L$.

Definíció. $K = \mathbb{Q}$, $L = \mathbb{C}$ mellett a fenti K_0 test az algebrai számok teste, jele $\mathbb{A}$ vagy $\overline{\mathbb{Q}}$.

Megjegyzés. $|\mathbb{A}| = \aleph_0$.

Definíció. $L_1|K \simeq L_2|K$, ha $\exists \varphi : \ L_1 \twoheadrightarrow L_2$ izomorfizmus, amelyre $\varphi|_K = \mathrm{id}_K$.

Definíció. $L|K$ egyszerű, ha $\exists \alpha \in L : \ L = K(\alpha)$.

Állítás. *Ha $\alpha, \beta \in L$ és kanonikus polinomjaik egyeznek, akkor $K(\alpha)|K \simeq K(\beta)|K$.*

Megjegyzés. Az állítás megfordítása nem igaz: $\mathbb{Q}$ felett $\sqrt{2}$ kanonikus polinomja $x^2 - 2$, $\sqrt{2} + 1$-é $x^2 - 2x - 1$, de $\mathbb{Q}\left(\sqrt{2}\right)|\mathbb{Q} = \mathbb{Q}\left(\sqrt{2} + 1\right)|\mathbb{Q}$, tehát a két bővítés nem is csupán izomorf, de egyenlő is.

Állítás. *Ha t transzcendens K felett, akkor $K(t)|K \simeq K(x)|K$, ahol $K(x)$ a racionális törtfüggvények teste.*

Állítás. *Ha $\alpha \in K(t)$ és $\alpha \notin K$, akkor α transzcendens K felett.*

Tétel. *Legyen $f \in K[x]$. Ekkor létezik $L \geq K$, hogy $\exists \alpha \in L : \ f(\alpha) = 0$.*

Tétel (Hermite, 1873)**.** *Az e transzcendens.*

12. Az algebrai egészek gyűrűje

Definíció. $\alpha \in \mathbb{C}$ algebrai egész, ha létezik $f = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in \mathbb{Z}[x]$ polinom, hogy $f(\alpha) = 0$.

Jelölés. Az algebrai egészek halmaza Ω.

Állítás. $\Omega \cap \mathbb{Q} = \mathbb{Z}$.

Következmény. $\Omega \subsetneq \mathbb{A}$ *és* Ω *nem test.*

Tétel. Ω *gyűrű.*

Lemma. *Ha* $X = \{\alpha_1, \ldots, \alpha_n\} \subset \Omega$*, akkor létezik* S *gyűrű, hogy* $\mathbb{Z} \leq S \leq \mathbb{C}$*,* $X \subseteq S$ *és* S *mint* $\mathbb{Z}$*-modulus végesen generált.*

Lemma. *Ha* S *gyűrű,* $\mathbb{Z} \leq S \leq \mathbb{C}$*,* $X \subseteq S$ *és* S *mint* $\mathbb{Z}$*-modulus végesen generált, akkor* $S \subseteq \Omega$*.*

Állítás. Ω *hányadosteste* $\mathbb{A}$*.*

Állítás. $\alpha \in \Omega \iff \alpha$ *kanonikus polinomja egész együtthatós,* 1 *főegyütthatójú.*

13. Számelmélet integritási tartományokban

R **egységelemes integritási tartomány.**

Definíció. $a, b \in R$-re $a|b$, ha $\exists c \in R$: $b = ac$.

Észrevétel. $U(R) = \{a \in R : a|1\}$.

Definíció. Ha $a, b \in R$ és $\exists u \in U(R)$, hogy $b = au$, akkor b asszociált a-hoz. $(a \sim b)$

Állítás. *Az asszociáltság ekvivalenciareláció.*

Definíció. $a \in R$ irreducibilis, ha $a \neq 0$, $a \notin U(R)$ és $a = bc \implies b \in U(R), a \sim c$ vagy $c \in U(R), b \sim a$.

Definíció. $p \in R$ prím, ha $p \neq 0$, $p \notin U(R)$ és $p|ab \implies p|a$ vagy $p|b$.

Állítás. a *prím* $\implies$ a *irreducibilis.*

Példa. $\mathbb{Z}$-ben a megfordítás is igaz, de $\mathbb{Z}\left[\sqrt{-5}\right]$-ben nem.

Állítás. Ω*-ban nincs irreducibilis elem.*

Állítás. $(K : \Omega) = 2 \iff K = \mathbb{Q}\left(\sqrt{d}\right)$*,* $d \in \mathbb{Z}$ *négyzetmentes és* $d \neq 0, 1$*.*

Definíció. $R_d = \mathbb{Q}\left(\sqrt{d}\right) \cap \Omega$.

Állítás. $R_d = \begin{cases} \left\{a + b\sqrt{d} : a, b \in \mathbb{Z}\right\}, & \text{ha } d \equiv 2, 3 \pmod 4 \\ \left\{a + b\sqrt{d} : a, b \in \mathbb{Z} \text{ vagy } a - \frac{1}{2}, b - \frac{1}{2} \in \mathbb{Z}\right\}, & \text{ha } d \equiv 1 \pmod 4 \end{cases}$

Definíció. R_{-3} az Eisenstein-egészek (Euler-egészek) gyűrűje.

Definíció. Egy R egységelemes integritási tartomány UFD (unique factorisation domain, alaptételes gyűrű), ha igaz benne a számelmélet alaptétele.

Tétel. *R egységelemes integritási tartomány pontosan akkor UFD, ha*

1. *főideálokra teljesül a minimumfeltétel* és
2. *minden irreducibilis elem prím.*

Tétel. *Minden főideálgyűrű UFD.*

Tétel (BN)**.** *R UFD $\implies$ $R[x]$ UFD.*

Következmény. *$K[x, y]$ UFD.*

Példa (BN)*.* R UFD $\not\Longrightarrow$ $R[[x]]$ UFD.

Definíció. R egységelemes integritási tartomány euklideszi gyűrű, ha létezik $\varphi : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ és $\forall a, b \in R$, $b \neq 0$: $\exists q, r \in R$: $a = bq + r$ *és* $\varphi(r) < \varphi(q)$ vagy $r = 0$.

Tétel. *R euklideszi gyűrű $\implies$ R főideálgyűrű.*

Példa. $\mathbb{Z}$-ben $\varphi(n) = |n|$, $K[x]$-ben $\varphi(f) = \deg f$, $\mathbb{Z}[i]$-ben $\varphi(a + bi) = N(a + bi) = a^2 + b^2$.

Állítás. $R_{-2} = \mathbb{Z}\left[\sqrt{-2}\right]$.

Tétel. *Négyzetmentes $d < 0$-ra R_d euklideszi, ha $d = -1, -2, -3, -7, -11$.*

Állítás. $U(R_{-3}) = \left\{\pm 1, \pm\varepsilon, \pm\varepsilon^2\right\}$.

Állítás. *Négyzetmentes $d < 0$-ra $U(R_d) = \{\pm 1\}$, ha $d \neq -1, -3$.*

Tétel (BN)**.** *$d < 0$, R_d euklideszi $\iff$ $d = -1, -2, -3, -7, -11$.*

Tétel (BN)**.** *$d < 0$, R_d UFD $\iff$ $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$.*

Tétel (BN)**.** *$d > 0$, R_d euklideszi $\iff$ $d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$.*

Sejtés. *$d > 0$, R_d UFD végtelen sok d-re.*

Tétel (BN)**.** *$x^2 + x + p$ prímszám minden $x = 0, 1, \ldots, p - 2$-re $\iff$ $R_{-(4p-1)}$ UFD.*

Tétel. *$d \neq 0, 1$ négyzetmentesre $\mathbb{Z}[d]$-ben 2 nem prím.*

Következmény. *Ha $d \leq -3$, akkor $\mathbb{Z}[d]$ nem UFD.*

Következmény. *$d \equiv 1 \pmod 4 \implies \mathbb{Z}[d]$ nem UFD.*

Definíció. Dedekind-gyűrű: minden ideál egyértelműen előáll prímideálok szorzataként.

14. Felbontási test, normális bővítés, szeparábilitás

Definíció. L az f felbontási teste K felett, ha f lineáris faktorokra (gyöktényezőkre) bomlik L felett és $L = K(\alpha_1, \ldots, \alpha_n)$, ahol $\alpha_1, \ldots, \alpha_n$ a gyökök.

Állítás. *A felbontási test lényegében egyértelmű: ha $L_1|K$ és $L_2|K$, ahol L_1 és L_2 f felbontási testei, akkor $L_1|K \simeq L_2|K$.*

Definíció. $L|K$ normális bővítés, ha algebrai és ha $p(x) \in K[x]$ irreducibilis K felett és van gyöke L-ben, akkor lineáris faktorokra bomlik L-ben.

Tétel. *A $L|K$ véges bővítés akkor és csak akkor normális, ha létezik f, aminek L a felbontási teste K felett.*

Megjegyzés. Minden első- vagy másodfokú bővítés normális.

Példa. $\mathbb{R}$ felett $x^2 + 1$ felbontási teste $\mathbb{C}$; $\mathbb{Q}$ felett $x^2 + 1$ felbontási teste $\mathbb{Q}(i)$; $\mathbb{Q}$ felett $x^n - 1$ felbontási teste $\mathbb{Q}(\varepsilon)$, ahol ε primitív n-edik egységgyök.

Tétel. *$\Phi_n(x)$ irreducibilis $\mathbb{Z}$ felett $\forall n \geq 1$-re.*

Definíció. $\mathbb{Q}(\varepsilon)$ az n-edik körosztási test.

Megjegyzés. Legyenek $K \leq L \leq M$ véges bővítések. Ekkor

1. $M|K$ normális $\not\Longrightarrow$ $L|K$ normális;
2. $M|K$ normális $\Longrightarrow$ $M|L$ normális;
3. $L|K$ és $M|L$ normális $\not\Longrightarrow$ $M|K$ normális.

Definíció. A $p(x) \in K[x]$ irreducibilis polinom szeparábilis, ha minden gyöke egyszeres.

Definíció. Legyen $L|K$ és $\alpha \in L$ algebrai. Ekkor α szeparábilis, ha a kanonikus polinomja az.

Definíció. Az $L|K$ algebrai bővítés szeparábilis, ha $\forall \alpha \in L$ szeparábilis.

Észrevétel. *K-irreducibilis inszeparábilis polinomnak minden gyöke legalább p-szeres (a felbontási testben), ahol* $\operatorname{char} K = p$.

Definíció. K perfekt (tökéletes) test, ha minden algebrai bővítése szeparábilis, azaz $\forall p(x) \in K[x]$ irreducibilis polinom szeparábilis.

Állítás. *Ha* $\operatorname{char} K = 0$*, akkor K perfekt.*

Állítás. *A p karakterisztikájú K test akkor és csak akkor perfekt, ha K minden elemének van p-edik gyöke K-ban.*

Példa. $\mathbb{F}_p(t)$ nem perfekt, ahol t transzcendens $\mathbb{F}_p$ felett.

Megjegyzés. Legyenek $K \leq L \leq M$ véges bővítések. Ekkor

1. $M|K$ szeparábilis $\Longrightarrow$ $L|K$ szeparábilis;
2. $M|K$ szeparábilis $\Longrightarrow$ $M|L$ szeparábilis.

15. Véges testek

Tétel. *Ha F véges test, akkor $|F| = q = p^f$, ahol p prím és $f \geq 1$.*

Tétel. *Ha $q = p^f$, akkor létezik olyan F test, hogy $|F| = q$.*

Tétel. *Minden $q = p^f$-re pontosan egy q elemű test létezik.*

Tétel. *Ha $|F| = q = p^f$, akkor $(F, +) \simeq (Z_p)^f$ és $(F^*, \cdot) \simeq Z_{q-1}$.*

Tétel. *Ha K tetszőleges test és $G \leq K^*$, ahol $|G| < \infty$, akkor G ciklikus.*

Megjegyzés. Az állítás ferdetestre nem igaz: $\mathbb{H}$-ban $\{\pm 1, \pm i, \pm j, \pm k\}$ nem ciklikus.

Tétel. *Ha $|F| = p^f$, akkor* $\mathrm{Aut}(F) \simeq Z_f$.

Jelölés. Ha $|F| = q$, akkor $F = \mathrm{GF}(q)$.

Tétel (Wedderburn)**.** *Minden véges ferdetest test.*

16. Galois-csoport, Galois-bővítés

Tétel. *$L|K$ véges és szeparábilis $\implies$ egyszerű.*

Észrevétel. *Ha $\varphi : K \to L$ testek közti homomorfizmus, akkor* $\operatorname{Ker}\varphi = 0$ *vagy* $\operatorname{Ker}\varphi = K$. *Tehát minden nemtriviális homomorfizmus monomorfizmus.*

Definíció. $L|K$, $M|K$-ra $\varphi : L \to M$ K-homomorfizmus, ha $\varphi|_K = \mathrm{id}_K$.

Definíció. $L|K$-ra $\mathrm{Gal}(L|K) = \{\varphi \in \mathrm{Aut}(L) : \varphi|_K = \mathrm{id}_K\}$ a Galois-csoport.

Példa. $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt[3]{2}\right)|\mathbb{Q}\right) = \left\{\mathrm{id}_{\mathbb{Q}\left(\sqrt[3]{2}\right)}\right\}$, $\mathrm{Gal}(\mathbb{R}|\mathbb{Q}) = \{\mathrm{id}_{\mathbb{R}}\}$.

Definíció. $L|K$ Galois-bővítés, ha véges, normális és szeparábilis.

Tétel. *$L|K$ Galois-bővítés* $\implies |\mathrm{Gal}(L|K)| = (L : K)$.

Lemma (Dedekind)**.** *Ha $\lambda_1, \ldots, \lambda_n : K \rightarrowtail L$ különböző monomorfizmusok, akkor lineárisan függetlenek L felett.*

Tétel. *Legyen $G \leq \mathrm{Aut}(K)$, $|G| < \infty$. Legyen $K_0 = \{a \in K : a^g = a\} \leq K$ a fixtest. Ekkor $(K : K_0) = |G|$.*

17. Hálók

Definíció. Részbenrendezett halmaz (poset): $(H, \leq)$, ahol a reláció reflexív, tranzitív és szimmetrikus.

Példa. $(\mathcal{P}(\mathbb{R}), \leq)$, $(\mathbb{N}, |)$, $(\mathcal{P}(X), \subseteq)$.

Definíció. $a \prec b$ (b fedi a-t), ha $a < b$ és $\nexists\, x : a < x < b$.

Definíció. A $(H, \leq)$ részbenrendezett halmaz háló, ha $\forall a, b \in H$-nak van legnagyobb alsó és legkisebb felső korlátja is; ezek jele rendre $a \wedge b$ és $a \vee b$.

Állítás. $(H, \wedge, \vee)$*-on*

1. $a \vee a = a$, $a \wedge a = a$ *(idempotencia);*
2. $a \vee b = b \vee a$, $a \wedge b = b \wedge a$ *(kommutativitás);*
3. $a \vee (b \vee c) = (a \vee b) \vee c$, $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ *(asszociativitás);*
4. $(a \wedge b) \vee a = a$, $(a \vee b) \wedge a = a$ *(abszorpciós tulajdonság).*

Állítás. *A háló kétféle definíciója ekvivalens.*

Állítás. *Ha egy részbenrendezett halmazban minden részhalmaznak van szuprémuma, akkor minden részhalmaznak van infimuma is.*

Definíció. Egy háló disztributív, ha a $\wedge$ és $\vee$ műveletek disztributívak egymásra nézve.

Állítás. *A kétféle disztributivitási tulajdonság ekvivalens.*

Definíció. Egy L háló moduláris, ha $a, b, c \in L$ és $a \leq c$ esetén $a \vee (b \wedge c) = (a \vee b) \wedge c$.

Állítás. *Egy L háló akkor és csak akkor moduláris, ha $\forall a, b, c \in L$-re $a \vee (b \wedge (a \vee c)) = (a \vee b) \wedge (a \vee c)$.*

Észrevétel. *Minden L hálóban $a, b, c \in L$, $a \leq c$ esetén $a \vee (b \wedge c) \leq (a \vee b) \wedge c$.*

Állítás. *Minden disztributív háló moduláris.*

Példa. Egy G csoport összes részcsoportjainak $\mathrm{L}(G)$ hálója nem feltétlenül moduláris: $G = A_4$ ellenpéldát szolgáltat. A normálosztók moduláris hálót alkotnak, de nem feltétlenül disztributívat: $G = Z_2 \times Z_2$ ellenpélda.

Példa. A K test feletti n dimenziós $P_n(K)$ projektív tér részsokaságai moduláris hálót alkotnak. A kétdimenziós affin tér ($A_2(\mathbb{R})$) részsokaságainak hálója nem moduláris.

Példa. Modulus részmodulusai moduláris hálót alkotnak.

Állítás. *A Abel-csoport* $\implies \mathrm{L}(A)$ *moduláris.*

Definíció. Egy G csoport lokálisan T tulajdonságú, ha minden végesen generált részcsoportja T tulajdonságú.

Megjegyzés. Véges csoport lokálisan ciklikus akkor és csak akkor, ha ciklikus.

Tétel (BN)**.** $\mathrm{L}(G)$ *disztributív* $\iff$ *G lokálisan ciklikus.*

Következmény. *Minden nem-Abel-csoport nem disztributív.*

Tétel. $\mathrm{L}(G)$ *véges* $\iff$ *G véges.*

Lemma. $|G| < \infty$ *és G-nek pontosan 1 maximális részcsoportja van* $\implies G \simeq Z_{p^n}$.

Definíció. Részháló: zárt $\vee$-ra és $\wedge$-re.

Tétel. *Az L háló akkor és csak akkor moduláris, ha nincs N_5-tel izomorf részhálója.*

Tétel. *Az L háló pontosan akkor disztributív, ha nincs se N_5-tel, se M_5-tel izomorf részhálója.*

Példa. M_5 moduláris, de nem disztributív.

Definíció. Korlátos háló: van legnagyobb (minden másnál nagyobb-egyenlő) és legkisebb eleme. Ezek jele 0 és 1.

Észrevétel. *Minden véges háló korlátos. Minden háló korlátossá tehető.*

Példa. $(\mathbb{Z}, \leq)$ nem korlátos.

Definíció. L korlátos hálóban az $a \in L$ elemnek $b \in L$ komplementuma, ha $a \wedge b = 0$ és $a \vee b = 1$.

Megjegyzés. 0 és 1 mindig egymás komplementumai. Komplementum nem feltétlenül létezik (például láncban) és nem egyértelmű (például M_2-ben).

Állítás. *Disztributív hálóban ha van egy elemnek van komplementuma, akkor az egyértelmű.*

Jelölés. Ha az a elem komplementuma egyértelmű, akkor jele a'.

Definíció. Komplementumos háló: minden elemnek van komplementuma.

Definíció. Boole-algebra: korlátos disztributív komplementumos háló.

Példa. $\mathcal{P}(H)$ Boole-algebra, $A \in \mathcal{P}(H)$-ra $A' = H \setminus A$.

Példa. Ha $|H| = \aleph_0$, akkor H véges és kovéges részhalmazai megszámlálhatóan végtelen Boole-algebrát alkotnak.

Definíció (Alternatív definíció Boole-algebrára)**.** $\langle B; \wedge, \vee, ', 0, 1\rangle$ Boole-algebra, ha a korábbi axiómák mellett $1 \wedge x = x$, $0 \wedge x = 0$, $x \wedge x' = 0$, $x \vee x' = 1$ teljesül.

Definíció. Rész-Boole-algebra.

Definíció. $\mathcal{P}(H)$ rész-Boole-algebrája halmaztest.

Tétel (Stone)**.** *Minden Boole-algebra izomorf egy halmaztesttel.*

Definíció. $\mathcal{P}(H)$ részhálója halmazgyűrű.

Tétel. *Minden disztributív háló izomorf egy halmazgyűrűvel.*

Észrevétel. *Boole-algebrák $\leftrightarrow$ egységelemes Boole-gyűrűk.*

Észrevétel (De Morgan-azonosságok)**.** *Minden Boole-algebrában* $(a \vee b)' = a' \wedge b'$ *és* $(a \wedge b)' = a' \vee b'$.

Definíció. $A \subseteq L$ ideál L-ben $(A \lhd L)$, ha $a, b \in A \implies a \vee b \in A$ és $a \in A, x \in L, x \leq a \implies x \in A$ (vagy ekvivalensen $a \in A, y \in L \implies a \wedge y \in A$).

Definíció. Generált ideál, főideál.

Állítás. $(a] = \{x \in L : x \leq a\}$.

Definíció. $B \subseteq L$ duális ideál (filter, szűrő), ha $a, b \in B \implies a \wedge b \in B$ és $a \in B, x \in L, x \geq a \implies x \in B$ (vagy ekvivalensen $a \in B, y \in L \implies a \vee y \in B$).

Definíció. $P \subsetneq L$ prímideál, ha ideál és $a, b \in L, a \wedge b \in P \implies a \in b$ vagy $b \in P$.

Definíció. $P^* \subsetneq L$ duális prímideál (ultrafilter, ultraszűrő), ha duális ideál és $a, b \in L, a \vee b \in P^* \implies a \in P^*$ vagy $b \in P^*$.

Észrevétel. *Egy ideál akkor és csak akkor prímideál, ha a (halmazelméleti) komplementuma duális ideál.*

Tétel (Stone)**.** *Legyen L disztributív háló. Ekkor bármely két különböző elem elválasztható prímideállal, azaz ha $b \not\leq a$, akkor létezik P prímideál, hogy $a \in P$, $b \notin P$.*

18. Galois-elmélet, gyökjelekkel való megoldhatóság

Tétel (A Galois-elmélet alaptétele)**.** *Legyen $L|K$ Galois-bővítés. Ekkor* $\mathrm{L}(G)$ *és a bővítés közbülső testeinek hálója duálisan izomorfak.*

Következmény. *Galois-bővítésre a közbülső testek hálója véges.*

Tétel. *A közbülső testek hálója akkor és csak akkor véges, ha az $L|K$ bővítés egyszerű.*

Példa. $K = \mathbb{Q}$ felett $x^4 - 2$ felbontási teste $L = \mathbb{Q}\left(\sqrt[4]{2}, i\right)$, $\mathrm{Gal}(L|K) \simeq D_4$.

Definíció. $f \in K[x]$-re legyen a K feletti felbontási test L. Ekkor $L|K$ véges és normális. Tegyük fel, hogy $\operatorname{char} K = 0$, így a bővítés szeparábilis is. Legyen $\mathrm{Gal}_K(f) \overset{\text{def}}{=} \mathrm{Gal}(L|K)$.

Állítás. $\mathrm{Gal}_K(f)$ *tranzitív permutációcsoport.*

Definíció. $L|K$ radikálbővítés, ha $\exists \alpha_1, \ldots, \alpha_n \in L$, hogy $L = K(\alpha_1, \ldots, \alpha_n)$ és $\forall k \exists n(k) : \alpha_k^{n(k)} \in K(\alpha_1, \ldots, \alpha_{k-1})$.

Megjegyzés. Minden radikálbővítés véges. Most nullkarakterisztikában dolgozunk, így a szeparábilitás is fennáll, a normalitás viszont nem feltétlenül teljesül.

Definíció. $f \in K[x]$ megoldható gyökjelekkel, ha a felbontási teste beágyazható radikálbővítésbe, azaz ha L jelöli a felbontási testet, akkor létezik olyan $R|K$ bővítés, hogy $K \leq L \leq R$.

Tétel (BN)**.** $f \in K[x]$ *akkor és csak akkor oldható meg gyökjelekkel, ha* $\mathrm{Gal}_K(f)$ *feloldható.*

Tétel. $x^5 - 6x + 3 \in \mathbb{Q}[x]$ *nem oldható meg gyökjelekkel.*

Definíció. K algebrailag zárt, ha $\forall f \in K[x], \deg f \geq 1\ \exists \alpha \in K : f(\alpha) = 0$. Ekvivalens megfogalmazások: minden $f \in K[x]$ gyöktényezőkre bomlik K felett; ha $L|K$ algebrai bővítés, akkor $L = K$.

Definíció. L a K test algebrai lezártja, ha $L|K$ algebrai bővítés és L algebrailag zárt.

Tétel (BN)**.** *Minden testnek létezik algebrai lezártja. Ha L_1 és L_2 a K algebrai lezártjai, akkor $L_1|K \simeq L_2|K$. A (lényegében egyértelmű) algebrai egész jelölést $\overline{K}$.*

Példa. $\overline{\mathbb{Q}} = \mathbb{A}$, $\overline{\mathbb{R}} = \mathbb{C}$. $\overline{\mathbb{F}_p} = \overline{\mathbb{F}_{p^n}}$.

Tétel (Az algebra alaptétele)**.** $\mathbb{C}$ *algebrailag zárt.*

19. Geometriai szerkeszthetőség

Tétel (Kockakettőzés, BN)**.** $\sqrt[3]{2}$ *nem szerkeszthető meg.*

Tétel (Szögharmadolás, BN)**.** $\cos 20°$ *nem szerkeszthető meg.*

Tétel (Körnégyszögesítés, BN)**.** $\sqrt{\pi}$ *nem algebrai.*

Tétel (BN)**.** *Szabályos n-szög akkor és csak akkor szerkeszthető, ha $n = 2^\alpha \cdot p_1 \ldots p_k$, ahol $\alpha \geq 0$ és $p_1, \ldots, p_k$ különböző Fermat-prímek.*