ABSZTRAKT ALGEBRA

vázlat az előadáshoz[†]

2019 tavaszi félév, OT

1. Alapvető algebrai konstrukciók

Algebrai struktúrák

1.1. Definíció. Tetszőleges A nemüres halmaz és $n \in \mathbb{N}_0$ esetén A-n értelmezett n-változós ***műveleten*** egy $f\colon A^n \to A$ leképezést értünk. (Ha $n = 0$, akkor f az A halmaz egy elemének kijelölését jelenti.)

1.2. Definíció. ***Algebrai struktúrán*** vagy röviden ***algebrán*** egy műveletekkel „felszerelt" nemüres halmazt értünk. Formálisan: $\mathbb{A} = (A; F)$ algebrai struktúra, ha A egy nemüres halmaz, F pedig A-n értelmezett műveletek egy halmaza. Az A halmazt az $\mathbb{A}$ algebra ***alaphalmazának*** vagy ***tartóhalmazának*** nevezzük.

1.3. Példa. Csoport: $(G; \cdot)$ vagy $\left(G; \cdot, 1, ^{-1}\right)$, gyűrű: $(R; +, \cdot)$ vagy $(R; +, 0, -, \cdot)$, egységelemes gyűrű: $(R; +, 0, -, \cdot, 1)$.

1.4. Megjegyzés. Ha a műveletek világosak a szövegkörnyezetből, akkor az algebrát és a tartóhalmazát nem mindig különböztetjük meg élesen egymástól.

1.5. Definíció. Ha f egy kétváltozós művelet az A halmazon, akkor $f(x, y)$ helyett általában azt írjuk, hogy $x * y$ (más szimbólumot is írhatunk x és y közé). Ilyenkor az $\mathbb{A} = (A; *)$ algebrát ***grupoidnak*** nevezzük.

1.6. Definíció. Az $\mathbb{A} = (A; *)$ és $\mathbb{B} = (B; \oplus)$ grupoidok ***izomorfak*** (jelölés: $\mathbb{A} \cong \mathbb{B}$), ha létezik olyan $\varphi\colon A \to B$ bijekció, amelyre

$$\forall a_1, a_2 \in A\colon\ (a_1 * a_2)\,\varphi = (a_1\varphi) \oplus (a_2\varphi)\,.$$

Ekkor a φ leképezést ***izomorfizmusnak*** nevezzük. Tetszőleges algebrák izomorfizmusa hasonlóan definiálható (lásd az 1.32. Definíciót).

1.7. Megjegyzés. Az izomorfizmus szemléletes jelentése az, hogy $\mathbb{A}$ és $\mathbb{B}$ szerkezete ugyanaz, csak „máshogy hívják" az elemeiket. Ezért izomorf algebrákat nem mindig érdemes (időnként nem is lehet!) megkülönböztetni (Steinitz-elv).

Részalgebra, generálás

1.8. Definíció. A $B \subseteq A$ részhalmaz ***zárt az $f\colon A^n \to A$ műveletre***, ha minden $b_1, \dots, b_n \in B$ esetén $f(b_1, \dots, b_n) \in B$. (Ha $n = 0$, akkor ez azt jelenti, hogy B tartalmazza az f által kijelölt elemet). Ha B zárt az $\mathbb{A} = (A; F)$ algebra minden műveletére (azaz minden $f \in F$-re), akkor egyszerűen csak ***zárt részhalmaznak*** nevezzük. Ha B nemüres zárt halmaz az $\mathbb{A} = (A; F)$ algebrában, akkor az F-beli műveletek megszorításaival egy $\mathbb{B}$ algebrát alkot, amelyet $\mathbb{A}$ ***részalgebrájának*** nevezünk. Jelölés: $\mathbb{B} \leq \mathbb{A}$.

1.9. Megjegyzés. Az üres halmaz zárt minden legalább egyváltozós műveletre, de a nullaváltozósokra nem.

1.10. Példa. A G csoportban $H \subseteq G$ ***részcsoportot*** alkot, ha részalgebrája a $\left(G; \cdot, 1, ^{-1}\right)$ algebrának. (Figyelem: a $(G; \cdot)$ algebra részalgebrái csak részfélcsoportok!) Hasonlóképpen az R gyűrű ***részgyűrűi*** az $(R; +, 0, -, \cdot)$ algebra részalgebrái. (Miért nem lehet a résztesteket ilyen módon definiálni?).

1.11. Állítás. Zárt részhalmazok metszete is zárt: ha B_i $(i \in I)$ zárt részhalmazok egy családja az $\mathbb{A}$ algebrában (lehet végtelen sok halmaz is), akkor a $\bigcap_{i\in I} B_i$ halmaz is zárt.

1.12. Definíció. Az $\mathbb{A}$ algebrában a nemüres $T \subseteq A$ halmaz által ***generált részalgebra***, más szóval T ***generátuma***, az a részalgebrája $\mathbb{A}$-nak, amelynek tartóhalmaza az T-et tartalmazó legszűkebb zárt halmaz. Jelölés: az T által generált részalgebrát (vagy annak tartóhalmazát) $[T]$ jelöli. Ha $[T] = A$, akkor azt mondjuk, hogy T ***generátorrendszere*** $\mathbb{A}$-nak.

1.13. Megjegyzés. Az 1.11. Állítás garantálja, hogy valóban létezik a H-t tartalmazó zárt halmazok között egy legszűkebb, nevezetesen az T-et tartalmazó összes zárt halmazok metszete:

$$[T] = \bigcap_{T \subseteq \mathbb{B} \leq \mathbb{A}} B.$$

[†]A természetes számok halmazát $\mathbb{N}$, a nemnegatív egész számok halmazát $\mathbb{N}_0$ jelöli, azaz $\mathbb{N} = \{1, 2, 3, \dots\}$ és $\mathbb{N}_0 = \{0, 1, 2, \dots\}$.

1.14. Megjegyzés. Ha F-ben nincsenek nullaváltozós műveletek, akkor az üres halmazt tartalmazó legszűkebb zárt halmaz maga az üres halmaz, de ez nem alkot részalgebrát. Ha F-ben vannak nullaváltozós műveletek, akkor viszont a $[\emptyset]$ részalgebra értelmezhető (megegyezik a nullaváltozós műveletek szerint kijelölt elemek által generált részalgebrával).

1.15. Állítás. Tetszőleges $\mathbb{A} = (A; F)$ algebra és $T \subseteq A$ esetén $[T]$ azon elemek halmaza, amelyek megkaphatóak T elemeiből kiindulva az F-beli műveletek véges számú alkalmazásával.

1.16. Definíció. Az $\mathbb{A}$ algebra összes zárt részhalmazai a tartalmazásra nézve egy $(\mathrm{Sub}(\mathbb{A}); \subseteq)$ részbenrendezett halmazt alkotnak, melyet $\mathbb{A}$ ***részalgebrahálójának*** nevezünk. A $B_1, B_2 \in \mathrm{Sub}(\mathbb{A})$ zárt részhalmazok legnagyobb közös alsó korlátja $B_1 \wedge B_2 := B_1 \cap B_2$, legkisebb közös felső korlátja pedig $B_1 \vee B_2 := [B_1 \cup B_2]$.

1.17. Megjegyzés. Ha F-ben nincsenek nullaváltozós műveletek, akkor $\mathrm{Sub}(\mathbb{A})$ legkisebb eleme $\emptyset$, ami nem részalgebra (tehát ekkor kicsit félrevezető a részalgebraháló elnevezés). Ha F-ben vannak nullaváltozós műveletek, akkor $\mathrm{Sub}(\mathbb{A})$ legkisebb eleme $[\emptyset]$. A legnagyobb elem pedig mindig maga A.

1.18. Definíció. Tetszőleges K test esetén K legszűkebb részteste $K_0 := [\{0, 1\}]$, amit K ***prímtestének*** nevezünk.

1.19. Definíció. A K test multiplikatív egységelemének additív rendjét K ***karakterisztikájának*** nevezzük, amennyiben ez a rend véges: $\mathrm{char}\, K := o_{(K;+)}(1)$. Ha 1 additív rendje végtelen, akkor $\mathrm{char}\, K := 0$.

1.20. Tétel. Test karakterisztikája mindig nulla vagy prímszám. Ha $\mathrm{char}\, K = 0$, akkor $K_0 \cong \mathbb{Q}$, ha pedig $\mathrm{char}\, K = p$, akkor $K_0 \cong \mathbb{Z}_p$.

1.21. Definíció. Ha L egy test és K egy részteste L-nek, akkor azt mondjuk, hogy L ***bővítése*** K-nak. Jelölés: $L \mid K$.

1.22. Tétel. Ha $L \mid K$ egy testbővítés és $\alpha \in L$, akkor a $K \cup \{\alpha\}$ halmaz által generált részgyűrűt $K[\alpha]$, a $K \cup \{\alpha\}$ halmaz által generált résztestet $K(\alpha)$ jelöli. Ezek éppen a K feletti polinomok, illetve a K feletti racionális törtek α helyen felvett értékeiből állnak:

$$K[\alpha] = \{f(\alpha) : f \in K[x]\}, \qquad K(\alpha) = \{t(\alpha) : t \in K(x)\} = \left\{\frac{f(\alpha)}{g(\alpha)} : f, g \in K[x], g(\alpha) \neq 0\right\}.$$

1.23. Definíció. Ha az $L \mid K$ testbővítéshez van olyan $\alpha \in L$ elem, amelyre $L = K(\alpha)$, akkor azt mondjuk, hogy $L \mid K$ ***egyszerű testbővítés***.

Kongruencia, faktoralgebra, homomorfizmus

1.24. Definíció. Legyen $\mathbb{A} = (A; F)$ egy algebra, és legyen ρ egy ekvivalenciareláció az A halmazon. Azt mondjuk, hogy ρ ***kongruenciarelációja*** (vagy röviden ***kongruenciája***) az $\mathbb{A}$ algebrának, ha minden $f \in F$ (n-változós) művelet és tetszőleges $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n \in A$ elemek esetén

$$(a_1 \rho b_1 \text{ és } a_2 \rho b_2 \text{ és } \ldots \text{ és } a_n \rho b_n) \implies f(a_1, a_2, \ldots, a_n)\, \rho f(b_1, b_2, \ldots, b_n).$$

1.25. Definíció. Legyen $\mathbb{A} = (A; F)$ egy algebra, és legyen $\mathcal{C}$ egy osztályozás az A halmazon. Azt mondjuk, hogy $\mathcal{C}$ ***kompatibilis osztályozás*** az $\mathbb{A}$ algebrán, ha minden $f \in F$ (n-változós) művelet és tetszőleges $C_1, C_2, \ldots, C_n \in \mathcal{C}$ osztályok esetén létezik egy olyan (egyértelműen meghatározott) $D \in \mathcal{C}$ osztály, amelyre

$$\{f(c_1, c_2, \ldots, c_n) : c_1 \in C_1,\ c_2 \in C_2,\ \ldots, c_n \in C_n\} \subseteq D.$$

1.26. Állítás. Tetszőleges $\mathbb{A}$ algebra és tetszőleges A-n értelmezett ρ ekvivalanciareláció esetén ρ akkor és csak akkor kongruenciája $\mathbb{A}$-nak, ha a hozzá tartozó A/ρ osztályozás kompatibilis osztályozása $\mathbb{A}$-nak.

1.27. Példa. Az egész számok gyűrűjén (vagy bármely integritástartományon) az $a \rho b \iff m \mid a - b$ képlettel definiált reláció mindig kongruencia, és a megfelelő osztályok a modulo m maradékosztályok.

1.28. Definíció. Legyen ρ kongruenciarelációja az $\mathbb{A}$ algebrának. Minden $f \in F$ (n-változós) művelet és tetszőleges $C_1, C_2, \ldots, C_n \in A/\rho$ osztályok esetén jelölje $f^{\mathbb{A}/\rho}(C_1, C_2, \ldots, C_n)$ azt a $D \in A/\rho$ osztályt, amelyre $f(c_1, c_2, \ldots, c_n) \in D$ minden $c_i \in C_i$ esetén. Ekkor az A/ρ halmaz az $f^{\mathbb{A}/\rho}$ ($f \in F$) műveletekkel egy algebrát alkot, amelyet az $\mathbb{A}$ algebra ρ szerinti ***faktoralgebrájának*** nevezzük. Jelölés: $\mathbb{A}/\rho = \left(A/\rho; \left\{f^{\mathbb{A}/\rho} : f \in F\right\}\right)$.

1.29. Megjegyzés. Az $\{f(c_1, c_2, \ldots, c_n) : c_1 \in C_1,\ c_2 \in C_2,\ \ldots, c_n \in C_n\}$ halmazt szokás $f(C_1, C_2, \ldots, C_n)$-nel jelölni (***komplexusművelet***). Ez általában nem egyezik meg az $f^{\mathbb{A}/\rho}(C_1, C_2, \ldots, C_n)$ halmazzal (de mindig részhalmaza neki). Ezért félreértést okozhat, ha elhagyjuk a felső indexet az $f^{\mathbb{A}/\rho}(C_1, C_2, \ldots, C_n)$ jelölésben.

1.30. Definíció. Az $\mathbb{A}$ és $\mathbb{B}$ algebrák ***azonos típusúak***, ha műveleteik kölcsönösen egyértelműen megfeleltethetőek egymásnak úgy, hogy az egymásnak megfelelő műveletek változószáma ugyanannyi. Ennek érzékeltetésére jelölje most F a műveleti jelek halmazát (nem pedig magukat a műveleteket, mint eddig), és tetszőleges $f \in F$ műveleti jelre legyen $f^{\mathbb{A}}$ és $f^{\mathbb{B}}$ a megfelelő művelet az $\mathbb{A}$ és a $\mathbb{B}$ algebrában. Ekkor tehát $f^{\mathbb{A}} \colon A^n \to A$ és $f^{\mathbb{B}} \colon B^n \to B$, ahol az n változószámot az f műveleti jel írja elő. Így tehát $\mathbb{A} = \left(A; \left\{f^{\mathbb{A}} : f \in F\right\}\right)$ és $\mathbb{B} = \left(B; \left\{f^{\mathbb{B}} : f \in F\right\}\right)$.

1.31. Megjegyzés. A felső indexeket nagyon gyakran lehagyjuk, ha a szövegkörnyezetből kiderül, hogy melyik algebra műveletéről van szó (például a csoport műveletét általában csak $\cdot$ jelöli).

1.32. Definíció. Legyenek $\mathbb{A}$ és $\mathbb{B}$ azonos típusú algebrák. Azt mondjuk, hogy a $\varphi \colon A \to B$ leképezés ***homomorfizmus*** $\mathbb{A}$-ból $\mathbb{B}$-be, ha minden (n-változós) $f \in F$ műveleti jel és tetszőleges $a_1, a_2, \ldots, a_n \in A$ elemek esetén

$$f^{\mathbb{A}}(a_1, a_2, \ldots, a_n)\,\varphi = f^{\mathbb{B}}(a_1\varphi, a_2\varphi, \ldots, a_n\varphi).$$

Ha φ szürjektív, akkor $\mathbb{B}$ ***homomorf képe*** $\mathbb{A}$-nak. Az injektív homomorfizmust ***beágyazásnak***, a bijektív homomorfizmust ***izomorfizmusnak*** nevezzük, az $\mathbb{A} \to \mathbb{A}$ izomorfizmusokat pedig $\mathbb{A}$ ***automorfizmusainak*** nevezzük. Ha létezik $\mathbb{A} \to \mathbb{A}$ izomorfizmus, akkor $\mathbb{A}$ és $\mathbb{B}$ ***izomorf*** algebrák (jelölés: $\mathbb{A} \cong \mathbb{B}$).

1.33. Állítás. Homomorfizmusok (izomorfizmusok) szorzata is homomorfizmus (izomorfizmus), továbbá izomorfizmus inverze izomorfizmus.

1.34. Következmény. Egy $\mathbb{A}$ algebra összes automorfizmusai csoportot alkotnak; ezt $\mathbb{A}$ ***automorfizmuscsoportjának*** nevezzük. Jelölés: $\mathrm{Aut}(\mathbb{A})$.

1.35. Állítás. Ha $\varphi \colon \mathbb{A} \to \mathbb{B}$ homomorfizmus, akkor $A\varphi$ (azaz φ értékkészlete) részalgebrát alkot $\mathbb{B}$-ben. Sőt, tetszőleges $T \subseteq A$ esetén $[T]\,\varphi = [T\varphi]$.

1.36. Állítás. Ha ρ kongruenciája az $\mathbb{A}$ algebrának, akkor az $\mathbb{A}/\rho$ faktoralgebra homomorf képe $\mathbb{A}$-nak az alábbi ***természetes homomorfizmus*** mellett:

$$\nu \colon \mathbb{A} \to \mathbb{A}/\rho,\ a \mapsto a/\rho.$$

1.37. Definíció. A $\varphi \colon \mathbb{A} \to \mathbb{B}$ homomorfizmus ***magján*** az alábbi $\ker\varphi$ relációt értjük:

$$\ker\varphi := \{(a_1, a_2) : a_1\varphi = a_2\varphi\} \subseteq A \times A.$$

1.38. Tétel (homomorfiatétel). Ha $\varphi \colon \mathbb{A} \to \mathbb{B}$ szürjektív homomorfizmus, akkor $\ker\varphi$ kongruenciája az $\mathbb{A}$ algebrának, és $\mathbb{A}/\ker\varphi \cong \mathbb{B}$.

1.39. Megjegyzés. Ha $\varphi \colon \mathbb{A} \to \mathbb{B}$ (nem feltétlenül szürjektív) homomorfizmus, akkor a homomorfiatétel szerint $\mathbb{A}/\ker\varphi \cong \mathbb{A}\varphi \leq \mathbb{B}$. Tehát a $\varphi \colon \mathbb{A} \to \mathbb{B}$ homomorfizmusok megtalálásához $\mathbb{A}$ faktoralgebrái és $\mathbb{B}$ részalgebrái között kell izomorfiumusokat keresnünk.

1.40. Megjegyzés. A homomorfiatételt és a természetes homomorfizmust összefoglalva elmondhatjuk, hogy a kongruenciák ugyanazok, mint a homomorfizmusok magjai, és a faktoralgebrák ugyanazok, mint a homomorf képek (izomorfia erejéig).

Csoportok kongruenciái: normálosztó, faktorcsoport, konjugálás

1.41. Állítás. Tetszőleges G csoport és $\rho \subseteq G \times G$ ekvivalenciareláció esetén ρ akkor és csak akkor kongruenciája a $(G; \cdot)$ algebrának, ha ρ kongruenciája a $\left(G; \cdot, 1, {}^{-1}\right)$ algebrának. Hasonlóan, csoporthomomorfizmus egységelemet egységelembe, inverzet inverzbe visz.

1.42. Tétel. Legyen ρ kongruenciája a G csoportnak, és legyen N az egységelem osztálya: $N = 1/\rho = \{a \in G : 1\rho a\}$. Ekkor $N \leq G$, továbbá minden $g \in G$ esetén $g^{-1}Ng \subseteq N$. A ρ relációt az N halmaz egyértelműen meghatározza: minden $a, b \in G$ esetén $a\rho b \iff a^{-1}b \in N \iff ab^{-1} \in N \iff aN = bN \iff Na = Nb$.

1.43. Tétel. Bármely G csoport bármely N részcsoportjára ekvivalensek az alábbiak:

(1) $\forall g \in G \colon g^{-1}Ng \subseteq N$;
(2) $\forall g \in G \colon g^{-1}Ng = N$;
(3) $\forall g \in G \colon gN = Ng$ (vagyis az N szerinti bal oldali és jobb oldali mellékosztályozás ugyanaz).

1.44. Definíció. Az előző tételben leírt tulajdonságokkal rendelkező részcsoportokat ***normális részcsoportoknak*** vagy ***normálosztóknak*** nevezzük. Jelölés: $N \lhd G$.

1.45. Tétel. Csoport kompatibilis osztályozásai éppen a normálosztók szerinti mellékosztályozások.

1.46. Definíció. Az $N \lhd G$ normálosztóhoz (tartozó kongruenciához) tartozó faktoralgebrát G/N jelöli, és ezt a G csoport N normálosztó szerinti ***faktorcsoportjának*** nevezzük.

1.47. Tétel. A G/N faktorcsoport valóban csoport. A faktorcsoportbeli szorzás így fest: $aN \cdot bN = abN$; a faktorcsoport egységeleme: $1N = N$; a faktorcsoportbeli inverz: $(aN)^{-1} = a^{-1}N$.

1.48. Megjegyzés. Az 1.29. Megjegyzésben említettük, hogy a faktoralgebra műveletei általában nem egyeznek meg a komplexusműveletekkel (utóbbi adhat szűkebbb halmazt is, mint az előbbi). Csoportoknál szerencsére megegyezik a kettő: az aN és bN mellékosztályok komplexusszorzata „teljesen kitölti" az abN mellékosztályt.

1.49. Példa. A legszűkebb normálosztó szerinti faktorcsoport $G/\{1\} \cong G$, a legbővebb normálosztó szerinti faktorcsoport pedig $G/G \cong \{1\}$. Minden 2 indexű részcsoport normálosztó (ilyenkor a faktorcsoport izomorf $\mathbb{Z}_2$-vel). Abel-csoportban minden részcsoport normálosztó.

1.50. Definíció. Tetszőleges G csoport és $g \in G$ elem esetén a $\varkappa_g \colon G \to G$, $x \mapsto g^{-1}xg$ leképezést g-vel való ***konjugálásnak*** nevezzük. Ha a $b \in G$ elem megkapható az $a \in G$ elemből egy alkalmas $g \in G$ elemmel való konjugálással, akkor azt mondjuk, hogy b ***konjugáltja*** a-nak; ezt a tényt $a \sim b$ jelöli. Tehát $a \sim b \iff \exists g \in G \colon b = g^{-1}ag$.

1.51. Állítás. A $\varkappa_g$ leképezés automorfizmusa G-nek. Az ilyen automorfizmusokat ***belső automorfizmusoknak*** nevezzük. A belső automorfizmusok részcsoportot alkotnak az $\mathrm{Aut}(G)$ csoportban.

1.52. Állítás. A $\sim$ konjugáltsági reláció ekvivalenciareláció.

1.53. Definíció. A konjugáltsági relációhoz tartozó ekvivalenciaosztályokat ***konjugáltosztályoknak*** nevezzük. Az $a \in G$ elemet tartalmazó konjugáltsági osztály: $K_G(a) = \{b \in G : a \sim b\} = \{g^{-1}ag : g \in G\}$.

1.54. Tétel. Az S_n szimmetrikus csoportban két permutáció pontosan akkor konjugált, ha azonos a ciklusszerkezetük (azaz létezik olyan bijekció a ciklusaik között, hogy az egymásnak megfelelő ciklusok egyforma hosszúak).

1.55. Tétel. Egy $N \leq G$ részcsoport akkor és csak akkor normálosztó, ha előáll konjugáltsági osztályok egyesítéseként. Egy $T \subseteq G$ részhalmazt tartalmazó legszűkebb normálosztó nem más, mint $\left[\bigcup_{g \in G} g^{-1}Tg\right]$, vagyis a T konjugáltjai által generált részcsoport. Ezt nevezzük a T által ***generált normálosztónak***.

1.56. Tétel. Normálosztók metszete is normálosztó. Ha $N_1, N_2 \lhd G$, akkor $N_1N_2 = N_2N_1 \lhd G$.

1.57. Megjegyzés. Egy csoport összes normálosztói részbenrendezett halmazt alkotnak a tartalmazásra nézve, amelyet a csoport ***normálosztóhálójának*** nevezünk. Az N_1, N_2 normálosztók legnagyobb közös alsó korlátja $N_1 \wedge N_2 = N_1 \cap N_2$, legkisebb közös felső korlátja pedig $N_1 \vee N_2 = N_1N_2$.

1.58. Definíció. A G csoportot ***egyszerű csoportnak*** nevezzük, ha $|G| \geq 2$ és G-nek csak két normálosztója van: $\{1\}$ és G.

1.59. Tétel. Az Abel-csoportok között pontosan a prímrendű ciklikus csoportok egyszerűek.

1.60. Tétel. Ha $n \geq 5$, akkor az A_n alternáló csoport egyszerű.

1.61. Tétel. Ha $n \geq 5$, akkor az S_n szimmetrikus csoport egyetlen valódi nemtriviális normálosztója A_n.

1.62. Definíció. A $\varphi \colon G \to H$ ***csoporthomomorfizmus magján*** a $\operatorname{Ker}\varphi = \{g \in G : g\varphi = 1_H\} \lhd G$ normálosztót értjük.

1.63. Megjegyzés. Homomorfizmus magját már definiáltuk korábban (lásd az 1.37. Definíciót). Csoportoknál a magot, mint ekvivalenciarelációt az 1.42. Tétel szerint meghatározza az egységelem ekvivalenciaosztálya. Ezért szokás csoportok esetén magon egyszerűen csak ezt az osztályt érteni: $\operatorname{Ker}\varphi = 1/\ker\varphi$.

1.64. Tétel (csoportelméleti homomorfiatétel). Ha $\varphi \colon G \to H$ szürjektív csoporthomomorfizmus, akkor $\operatorname{Ker}\varphi$ normálosztója G-nek és $G/\operatorname{Ker}\varphi \cong H$.

Gyűrűk kongruenciái: ideál, faktorgyűrű

1.65. Tétel. Legyen ρ kongruenciája az R gyűrűnek, és legyen I az additív egységelem osztálya: $I = 0/\rho = \{a \in R : 0\rho a\}$. Ekkor $I \leq R$, továbbá minden $r \in R$ esetén $rI, Ir \subseteq I$. A ρ relációt az I halmaz egyértelműen meghatározza: minden $a, b \in R$ esetén $a\rho b \iff a - b \in I$.

1.66. Definíció. Ha az $I \leq R$ részgyűrűre $RI, IR \subseteq I$, akkor azt mondjuk, hogy I ***ideálja*** az R gyűrűnek. Jelölés: $I \lhd R$. (Az $RI, IR \subseteq I$ tulajdonságot *szívó tulajdonságnak* hívják, mert ez azt fejezi ki, hogy I magába „szippantja" a szorzatokat: ha egy szorzat valamelyik tényezője I-ben van, akkor a szorzat is I-be esik, még akkor is, ha a másik tényező I-n kívül van. Ez nyilván erősebb tulajdonság, mint a szorzásra való zártság.)

1.67. Tétel. Gyűrű kompatibilis osztályozásai éppen az ideálok (mint additív részcsoportok) szerinti mellékosztályozások.

1.68. Definíció. Az $I \lhd R$ ideálhoz (tartozó kongruenciához) tartozó faktoralgebrát R/I jelöli, és ezt az R gyűrű I ideál szerinti ***faktorgyűrűjének*** nevezzük.

1.69. Tétel. Az R/I faktorgyűrű valóban gyűrű. A faktorgyűrűbeli összeadás és szorzás így festenek: $(a+I)+(b+I) = (a+b)+I$ és $(a+I)\cdot(b+I) = a\cdot b+I$; a faktorgyűrű addív egységeleme: $0+I=I$; a faktorgyűrűbeli additív inverz: $-(a+I) = (-a)+I$. Ha R egységelemes gyűrű, akkor R/I is az, és a multiplikatív egységeleme $1+I$.

1.70. Megjegyzés. Az 1.48. Megjegyzés szerint a faktorgyűrűbeli összeadás megegyezik a komplexusösszeggel, viszont az $(a+I)(b+I) \subseteq ab+I$ tartalmazás lehet valódi (lásd az 1.29. Megjegyzést).

1.71. Példa. A legszűkebb ideál szerinti faktorgyűrű $R/\{0\} \cong R$, a legbővebb ideál szerinti faktorgyűrű pedig $R/R \cong \{0\}$.

1.72. Tétel. Tetszőleges R egységelemes gyűrű esetén egy $T \subseteq R$ részhalmazt tartalmazó legszűkebb ideál nem más, mint az RTR halmaz által generált részcsoport, vagyis az összes $r_1t_1r_1' + \dots + r_nt_nr_n'$ alakú véges összegek halmaza, ahol $n \in \mathbb{N}$, $t_i \in T$, $r_i, r_i' \in R$. Ezt nevezzük a T által ***generált ideálnak***, és $\langle T\rangle$-vel jelöljük.

1.73. Definíció. Az egyetlen elemmel generált ideálokat ***főideáloknak*** nevezzük. Az a elem által generált főideált $\langle a\rangle$ jelöli.

1.74. Következmény. Ha R kommutatív egységelemes gyűrű, akkor az $a \in R$ elem által generált főideál: $\langle a\rangle = Ra = \{ra : r \in R\}$.

1.75. Példa. Bármely $m \in \mathbb{Z}$ esetén $\langle m\rangle$ éppen m többszöröseiből áll; az ehhez az ideálhoz tartozó kongruencia a modulo m kongruencia, a megfelelő faktorgyűrű pedig $\mathbb{Z}/\langle m\rangle = \mathbb{Z}_m$.

1.76. Tétel. Ideálok metszete és összege is ideál: ha $I_1, I_2 \lhd R$, akkor $I_1 \cap I_2 \lhd R$ és $I_1 + I_2 \lhd R$.

1.77. Megjegyzés. Egy gyűrű összes ideáljai részbenrendezett halmazt alkotnak a tartalmazásra nézve, amelyet a gyűrű ***ideálhálójának*** nevezünk. Az I_1, I_2 ideálok legnagyobb közös alsó korlátja $I_1 \wedge I_2 = I_1 \cap I_2$, legkisebb közös felső korlátja pedig $I_1 \vee I_2 = I_1 + I_2$.

1.78. Definíció. Az R gyűrűt ***egyszerű gyűrűnek*** nevezzük, ha $|R| \geq 2$ és R-nek csak két ideálja van: $\{0\}$ és R.

1.79. Tétel. A kommutatív egységelemes gyűrűk között pontosan a testek egyszerűek.

1.80. Tétel. Tetszőleges K test és $n \in \mathbb{N}$ esetén a $K^{n\times n}$ mátrixgyűrű egyszerű.

1.81. Tétel (Wedderburn). Ha R *véges* egységelemes egyszerű gyűrű, akkor van olyan K véges test és n természetes szám, hogy $R \cong K^{n\times n}$.

1.82. Definíció. A $\varphi\colon R \to S$ ***gyűrűhomomorfizmus magján*** a $\operatorname{Ker}\varphi = \{r \in R : r\varphi = 0_S\} \lhd R$ ideált értjük.

1.83. Megjegyzés. A mag fogalmával kapcsolatban itt is az a kettősség figyelhető meg, mint csoportok esetén (lásd az 1.63. Megjegyzést). Minden gyűrűhomomorfizmus egyúttal homomorfizmus a két gyűrű additív csoportja között is, és a „csoportelméleti mag” megegyezik a „gyűrűelméleti maggal”.

1.84. Tétel (gyűrűelméleti homomorfiatétel). Ha $\varphi\colon R \to S$ szürjektív gyűrűhomomorfizmus, akkor $\operatorname{Ker}\varphi$ ideálja R-nek és $R/\operatorname{Ker}\varphi \cong S$.

Direkt szorzat

1.85. Definíció. Legyenek $\mathbb{A}_1, \dots, \mathbb{A}_k$ azonos típusú algebrák (F művelethalmazzal). Minden (n-változós) $f \in F$ műveletre (pontosabban műveleti jelre) értelmezzük az $f^{\mathbb{A}_1\times\dots\times\mathbb{A}_k}$ műveletet az $A_1 \times \dots \times A_k$ halmazon a következőképp:

$$f^{\mathbb{A}_1\times\dots\times\mathbb{A}_k}\big((a_1^{(1)},\dots,a_k^{(1)}),\dots,(a_1^{(n)},\dots,a_k^{(n)})\big) = \big(f^{\mathbb{A}_1}(a_1^{(1)},\dots,a_1^{(n)}),\dots,f^{\mathbb{A}_k}(a_k^{(1)},\dots,a_k^{(n)})\big) \qquad (a_i^{(j)} \in A_i).$$

Ekkor az $A_1 \times \dots \times A_k$ halmaz az $f^{\mathbb{A}_1\times\dots\times\mathbb{A}_k}$ ($f \in F$) műveletekkel egy algebrát alkot, amelyet az $\mathbb{A}_1, \dots, \mathbb{A}_k$ algebrák ***(külső) direkt szorzatának*** nevezünk. Jelölés: $\mathbb{A}_1 \times \dots \times \mathbb{A}_k = \big(A_1 \times \dots \times A_k; \{f^{\mathbb{A}_1\times\dots\times\mathbb{A}_k} : f \in F\}\big)$.

1.86. Megjegyzés. Végtelen sok algebra direkt szorzata hasonlóan definiálható.

1.87. Példa. Ha $\mathbb{A}_1 = (A_1; *_1)$ és $\mathbb{A}_2 = (A_2; *_2)$ grupoidok, akkor direkt szorzatuk $\mathbb{A}_1 \times \mathbb{A}_2 = (A_1 \times A_2; *)$, ahol a $*$ művelet az alábbi módon értelmezzük:

$$(a_1, a_2) * (a_1', a_2') = (a_1 *_1 a_1', a_2 *_2 a_2') \qquad (a_1, a_1' \in A_1,\ a_2, a_2' \in A_2).$$

1.88. Definíció. Az $\mathbb{A}$ algebra ***direkt felbontható***, ha léteznek olyan legalább kételemű $\mathbb{A}_1, \mathbb{A}_2$ algebrák, amelyekre $\mathbb{A} \cong \mathbb{A}_1 \times \mathbb{A}_2$.

1.89. Állítás. Az $\mathbb{A}_1 \times \cdots \times \mathbb{A}_k$ direkt szorzatnak mindegyik $\mathbb{A}_i$ tényező homomorf képe.

1.90. Tétel. Tetszőleges G és $G_1, \ldots, G_k$ csoportok esetén $G \cong G_1 \times \cdots \times G_k$ akkor és csak akkor teljesül, ha léteznek olyan $N_1, \ldots, N_k \leq G$ részcsoportok, amelyekre

(a) $N_i \cong G_i$ $(i = 1, \ldots, k)$;
(b) G minden eleme egyértelműen felírható $n_1 \cdot \ldots \cdot n_k$ alakban, ahol $n_i \in N_i$ $(i = 1, \ldots, k)$;
(c) minden $1 \leq i < j \leq k$ és $n_i \in N_i$, $n_j \in N_j$ esetén $n_i \cdot n_j = n_j \cdot n_i$.

1.91. Tétel. Tetszőleges G és $G_1, \ldots, G_k$ csoportok esetén $G \cong G_1 \times \cdots \times G_k$ akkor és csak akkor teljesül, ha léteznek olyan $N_1, \ldots, N_k \lhd G$ normálosztók, amelyekre

(a) $N_i \cong G_i$ $(i = 1, \ldots, k)$;
(b) $G = N_1 \cdot \ldots \cdot N_k$;
(c) $N_i \cap (N_1 \cdot \ldots \cdot N_{i-1} \cdot N_{i+1} \cdot \ldots \cdot N_k) = \{1\}$ minden $1 \leq i \leq k$ esetén.

1.92. Definíció. Ha az előző tétel feltételei teljesülnek, akkor azt mondjuk, hogy a G csoport az $N_1, \ldots, N_k$ normálosztóinak ***(belső) direkt szorzata***.

1.93. Tétel. Tetszőleges R és $R_1, \ldots, R_k$ gyűrűk esetén $R \cong R_1 \times \cdots \times R_k$ akkor és csak akkor teljesül, ha léteznek olyan $I_1, \ldots, I_k \leq R$ részgyűrűk, amelyekre

(a) $I_i \cong R_i$ $(i = 1, \ldots, k)$;
(b) R minden eleme egyértelműen felírható $a_1 + \cdots + a_k$ alakban, ahol $a_i \in I_i$ $(i = 1, \ldots, k)$;
(c) minden $1 \leq i < j \leq k$ és $a_i \in I_i$, $a_j \in I_j$ esetén $a_i \cdot a_j = a_j \cdot a_i = 0$.

1.94. Tétel. Tetszőleges R és $R_1, \ldots, R_k$ gyűrűk esetén $R \cong R_1 \times \cdots \times R_k$ akkor és csak akkor teljesül, ha léteznek olyan $I_1, \ldots, I_k \leq R$ ideálok, amelyekre

(a) $I_i \cong R_i$ $(i = 1, \ldots, k)$;
(b) $R = I_1 + \cdots + I_k$;
(c) $I_i \cap (I_1 + \cdots + I_{i-1} + I_{i+1} + \cdots + I_k) = \{0\}$ minden $1 \leq i \leq k$ esetén.

1.95. Definíció. Ha az előző tétel feltételei teljesülnek, akkor azt mondjuk, hogy az R gyűrű az $I_1, \ldots, I_k$ ideáljainak ***(belső) direkt összege***.

1.96. Tétel. Két véges ciklikus csoport direkt szorzata akkor és csak akkor ciklikus, ha a két csoport elemszáma relatív prím: $C_n \times C_m \cong C_{nm} \iff n \perp m$. Következésképp minden véges ciklikus csoport előáll prímhatványrendű ciklikus csoportok direkt szorzataként. A prímhatványrendű ciklikus csoportok már direkt felbonthatatlanok.

1.97. Tétel (a véges Abel-csoportok alaptétele). Minden véges Abel-csoport előáll prímhatványrendű ciklikus csoportok direkt szorzataként. Ez az előállítás a tényezők sorrendjétől (és izomorfiától) eltekintve egyértelmű.

1.98. Tétel. Ha n és m relatív prím, akkor a $\mathbb{Z}_n \times \mathbb{Z}_m$ és $\mathbb{Z}_{nm}$ gyűrűk izomorfak. Következésképp, ha n prímhatványtényezős felbontása $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, akkor $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}$. A $\mathbb{Z}_{p^\alpha}$ alakú gyűrűk már direkt felbonthatatlanok.

2. Csoporthatások, Sylow-tételek

Csoporthatás, pálya, stabilizátor

2.1. Definíció. Legyen $G = (G; \cdot, 1, ^{-1})$ egy csoport és Ω egy nemüres halmaz. Minden $g \in G$ és $\omega \in \Omega$ esetén jelöljünk ki egy $\omega \bullet g \in \Omega$ elemet (vagyis egy $\Omega \times G \to \Omega$ leképezést adunk meg) úgy, hogy

(a) $\forall g, h \in G \ \ \forall \omega \in \Omega \colon (\omega \bullet g) \bullet h = \omega \bullet (gh)$;
(b) $\forall \omega \in \Omega \colon \omega \bullet 1 = \omega$.

Ekkor azt mondjuk, hogy a G csoport (jobbról) ***hat*** az Ω halmazon.

2.2. Megjegyzés. Tekintsük a G csoport hatását az Ω halmazon a fenti definíció szerint. Tetszőleges $g \in G$ esetén legyen $\pi_g \colon \Omega \to \Omega$, $\omega \mapsto \omega \bullet g$ a g elem által indukált leképezés az Ω halmazon. A csoporthatás definíciójából levezethető, hogy π_g permutációja Ω-nak (hiszen van inverze, mégpedig $\pi_{g^{-1}}$), és $\pi_{gh} = \pi_g \pi_h$ minden $g, h \in G$ esetén. Tehát a $\varphi \colon G \to S_\Omega$, $g \mapsto \pi_g$ leképezés csoporthomomorfizmus. Fordítva, minden $\varphi \colon G \to S_\Omega$ homomorfizmus megfelel egy csoporthatásnak. Ennek megfelelően beszélhetünk a ***hatás magjáról***: a magban azok a $g \in G$ elemek vannak, amelyekre $\omega \bullet g = \omega$ minden $\omega \in \Omega$ esetén. Ha $\ker \varphi = \{1\}$ (azaz φ injektív homomorfizmus), akkor azt mondjuk, hogy a hatás ***hű***.

2.3. Példa. Az S_n csoport természetes módon hat az $\{1, \ldots, n\}$ halmazon. A D_n csoport hat a szabályos n-szög csúcsain (oldalain), ezeket megszámozva pedig az $\{1, \ldots, n\}$ halmazon is. A kocka forgáscsoportja hat a kocka csúcsainak (éleinek, lapjainak) halmazán. Az $\mathbb{R}^n$ halmazon hat az $\mathbb{R}^*$ csoport (skalárral való szorzás) és a $\mathrm{GL}_n(\mathbb{R})$ csoport (lineáris transzformációk).

2.4. Példa. Tetszőleges G csoport hat saját magán (vagyis az $\Omega = G$ halmazon) jobbszorzásokkal: $\omega \bullet g = \omega g$. Ez a hatás hű, és ebből a tényből következik a Cayley-féle reprezentációs tétel.

2.5. Példa. Tetszőleges G csoport hat saját magán (vagyis az $\Omega = G$ halmazon) konjugálásokkal: $\omega \bullet g = g^{-1}\omega g$. Ennek a hatásnak a magja mindazon elemekből áll, melyek a csoport összes elemével felcserélhetőek. Ezt a részcsoportot (ami normálosztó is, hiszen egy homomorfizmus magja) a csoport ***centrumának*** nevezzük. Jelölés: $Z(G) = \{g \in G : ag = ga \text{ minden } a \in G \text{ esetén}\}$.

2.6. Állítás. Ha a G csoport hat az Ω halmazon, akkor az $\alpha \sim \beta \iff \exists g \in G\colon \alpha \bullet g = \beta$ képlettel definiált $\sim$ reláció ekvivalenciareláció az Ω halmazon.

2.7. Definíció. A fenti állításban szereplő ekvivalenciarelációhoz tartozó ekvivalenciaosztályokat a csoporthatás ***pályáinak*** nevezzük.

2.8. Definíció. Tetszőleges $g \in G$ és $\omega \in \Omega$ esetén ω ***stabilizátora*** az ω-t fixen hagyó csoportelemek halmaza: $\mathrm{Stab}(\omega) = \{g \in G : \omega \bullet g = \omega\}$.

2.9. Tétel. Hasson a G csoport az Ω halmazon.

(1) A stabilizátorok részcsoportok: $\mathrm{Stab}(\omega) \leq G$ minden $\omega \in \Omega$ esetén.
(2) Azonos pályán lévő elemek stabilizátorai konjugáltak: $\mathrm{Stab}(\omega \bullet g) = g^{-1}\,\mathrm{Stab}(\omega)g$ minden $\omega \in \Omega$ és $g \in G$ esetén.
(3) Két csoportelem akkor és csak akkor esik ugyanabba a $\mathrm{Stab}(\omega)$ szerinti jobb oldali mellékosztályba, ha „ugyanoda viszik" az ω elemet: $\omega \bullet g = \omega \bullet h \iff \mathrm{Stab}(\omega)g = \mathrm{Stab}(\omega)h$ minden $\omega \in \Omega$ és $g, h \in G$ esetén.
(4) A pálya mérete megegyezik a stabilizátor indexével: $|\{\omega \bullet g : g \in G\}| = [G : \mathrm{Stab}(\omega)]$ minden $\omega \in \Omega$ esetén. Következésképp, ha G véges, akkor minden pálya mérete osztója G rendjének.

2.10. Tétel (Pólya–Redfield-módszer). Hasson a G véges csoport a véges Ω halmazon, és minden $g \in G$ esetén jelölje $c(g)$ a π_g permutáció ciklusainak számát (a fixpontokat is beleértve). Színezzük ki az Ω halmazt k színnel úgy, hogy két színezést nem tekintünk lényegesen különbözőnek, ha valamely G-beli elem egymásba viszi őket. Ekkor a lényegesen különböző színezések száma

$$\frac{1}{|G|}\sum_{g\in G} k^{c(g)}.$$

2.11. Példa. Legyen p prímszám és színezzük a szabályos p-szög csúcsait k színnel úgy, hogy a forgatással egymásba vihető színezéseket nem különböztetjük meg. Ekkor a lényegesen különböző színezések száma $\frac{1}{p}\left(k^p + (p-1)\,k\right) = k + \frac{1}{p}\left(k^p - k\right)$. Ebből következik, hogy $p \mid k^p - k$ (kis Fermat-tétel).

2.12. Példa. A kocka lapjait $\frac{1}{24}\left(k^6 + 3k^4 + 12k^3 + 8k^2\right)$ különböző módon lehet k színnel színezni, ha az egymásba forgatható színezéseket nem különböztetjük meg.

Sylow-tételek, kis elemszámú csoportok

2.13. Tétel (Cauchy tétele). Ha a p prímszám osztja a véges G csoport rendjét, akkor G-ben van p-edrendű elem.

2.14. Tétel (Sylow-tételek). Legyen a p prímszám kitevője a véges G csoport elemszámában k azaz $|G| = p^k \cdot m$, ahol $p \nmid m$. A G csoport p^k rendű részcsoportjait ***Sylow-részcsoportoknak*** nevezzük.

(1) Minden $i \leq k$ esetén van G-nak p^i rendű részcsoportja. Ha $i < k$, akkor minden p^i rendű részcsoport benne van egy p^{i+1} rendű részcsoportban.
(2) Létezik p-Sylow részcsoport, és minden p-hatvány rendű részcsoport benne van egy p-Sylow részcsoportban.
(3) A p-Sylow részcsoprtok egymás konjugáltjai.
(4) Jelölje n_p a p-Sylow részcsoportok számát. Ekkor $n_p \equiv 1 \pmod p$ és $n_p \mid m$.

2.15. Következmény. A G-beli p-Sylow részcsoportok izomorfak egymással. Akkor és csak akkor van normális p-Sylow részcsoport, ha csak egyetlen p-Sylow részcsoport van.

2.16. Tétel. Ha p prímszám, akkor minden p^2 rendű csoport Abel-csoport. Következésképp izomorfia erejéig csak kétféle p^2 rendű csoport létezik: $\mathbb{Z}_{p^2}$ és $\mathbb{Z}_p \times \mathbb{Z}_p$.

2.17. Tétel. Ha p prímszám, akkor izomorfia erejéig csak kétféle $2p$ rendű csoport létezik: $\mathbb{Z}_{2p}$ és D_p. (A $p = 2$ esetben $D_2 \cong V$ értendő.)

2.18. Következmény. A legfeljebb 11 rendű csoportok izomorfia erejéig a következők: $\mathbb{Z}_2$; $\mathbb{Z}_3$; $\mathbb{Z}_4, \mathbb{Z}_2^2$; $\mathbb{Z}_5$; $\mathbb{Z}_6, D_3$; $\mathbb{Z}_7$; $\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2^3, D_4, Q$; $\mathbb{Z}_9, \mathbb{Z}_3^2$; $\mathbb{Z}_{10}, D_5$; $\mathbb{Z}_{11}$.

3. Integritástartományok

Hányadostest

3.1. Tétel. Legyen $R = (R, +, 0, -, \cdot, 1)$ integritástartomány, és értelmezzük az $R \times (R \setminus \{0\})$ halmazon a $\oplus$ és $\odot$ műveleteket, valamint a $\sim$ relációt a következőképpen:

$$(a,b) \oplus (c,d) := (ad + bc, bd), \qquad (a,b) \sim (c,d) \overset{\text{def}}{\iff} ad = bc.$$
$$(a,b) \odot (c,d) := (ac, bd),$$

Ekkor $\sim$ ekvivalenciareláció, ami kompatibilis a $\oplus$ és $\odot$ műveletekkel, vagyis kongruenciája az $(R \times (R \setminus \{0\}); \oplus, \odot)$ algebrának; legyen Q_R a megfelelő faktoralgebra. A Q_R algebra a következő tulajdonságokkal rendelkezik:

(1) Q_R test, amelyben az $\overline{(a,1)}$ alakú elemek egy R-rel izomorf részgyűrűt alkotnak;
(2) Q_R minden eleme előáll „két R-beli elem hányadosaként", azaz $\overline{(a,1)} \odot \overline{(b,1)}^{-1}$ alakban;
(3) ha K egy tetszőleges test, ami részgyűrűként tartalmazza R-et (vagy egy R-rel izomorf gyűrűt), akkor K-nak van Q_R-rel izomorf részteste.

3.2. Definíció. A fent megkonstruált Q_R testet az R integritástartomány ***hányadostestének*** nevezzük.

3.3. Példa. Az egész számok gyűrűjének hányadosteste a racionális számok teste: $Q_{\mathbb{Z}} \cong \mathbb{Q}$. Egy T test feletti polinomgyűrű hányadosteste a T feletti racionális törtek teste: $Q_{T[x]} \cong T(x)$.

3.4. Megjegyzés. A tételben szereplő harmadik tulajdonság így is megfogalmazható: ha K egy test, és $\varphi\colon R \to K$ beágyazás (azaz injektív gyűrűhomomorfizmus), akkor $\widehat{\varphi}\colon Q_R \to K$, $\overline{(a,1)} \odot \overline{(b,1)}^{-1} \mapsto (a\varphi)(b\varphi)^{-1}$ is beágyazás. Ha az $\overline{(a,1)} \in Q_R$ elemet azonosítjuk az $a \in R$ elemmel, azaz R-et Q_R részgyűrűjének tekintjük (a tételbeli első tulajdonság miatt ezt megtehetjük), akkor $\widehat{\varphi}$ kiterjesztése φ-nek: $\overline{(a,1)}\widehat{\varphi} = a\varphi = \overline{(a,1)}\varphi$. Tehát R bármely testebe történő beágyazása kiterjed Q_R-nek ugyanabba a testbe történő beágyazásává.

3.5. Következmény. Minden integritástartomány beágyazható testbe. Izomorfia erejéig egyetlen olyan minimális K test létezik, amibe R beágyazható (a minimalitás azt jelenti, hogy K-nak egyetlen valódi résztestébe sem ágyazható be R). Ez a K test izomorf R hányadostestével.

Gauss-gyűrűk

A következőkben $R = (R, +, 0, -, \cdot, 1)$ mindig tetszőleges integritástartományt jelöl.

3.6. Definíció. Azt mondjuk, hogy az $a \in R$ elem ***osztója*** a $b \in R$ elemnek, ha létezik olyan $c \in R$, amelyre $b = ac$. Jelölés: $a \mid b$.

3.7. Definíció. Azt mondjuk, hogy az a és b elemek ***asszociáltak***, ha $a \mid b$ és $b \mid a$. Jelölés: $a \sim b$.

3.8. Definíció. Az $u \in R$ elemet ***egységnek*** nevezzük, ha $u \mid 1$ (azaz $u \sim 1$). Az egységek halmazát R^* jelöli.

3.9. Állítás. Az oszthatósági és asszociáltsági reláció, valamint az egységek minden integritástartományban rendelkeznek a szokásos tulajdonságokkal. Így például $(R^*; \cdot)$ csoportot, és két elem akkor és csak akkor asszociált, ha egymástól csupán egység tényezőben különböznek. Az oszthatóság reflexív és tranzitív, valamint „asszociáltság erejéig" antiszimmetrikus. Tehát ha az oszthatósági relációt az asszociáltsági osztályok halmazán értelmezzük, akkor egy $(R/\sim; |)$ részbenrendezett halmazt kapunk, amelynek legkisebb eleme $1/\sim = R^*$, legnagyobb eleme pedig $0/\sim = \{0\}$.

3.10. Definíció. A $d \in R$ elemet az a és b elemek ***legnagyobb közös osztójának*** nevezzük, ha kielégíti a következő két feltételt:

(1) $d \mid a$ és $d \mid b$;
(2) $\forall k \in R : (k \mid a \text{ és } k \mid b) \implies k \mid d$.

A $t \in R$ elem ***legkisebb közös többszöröse*** a-nak és b-nek, ha kielégíti a következő két feltételt:

(1) $a \mid t$ és $b \mid t$;
(2) $\forall k \in R : (a \mid k \text{ és } b \mid k) \implies t \mid k$.

3.11. Állítás. A legnagyobb közös osztó és a legkisebb közös többszörös asszociáltság erejéig egyértelműen meghatározott, és a szokásos tulajdonságokkal rendelkezik (ha létezik egyáltalán). Az $(R/\sim; |)$ részbenrendezett halmazban $a/\sim$ és $b\sim$ legnagyobb közös alsó korlátja $\operatorname{lnko}(a,b)\sim$, legkisebb közös felső korlátjuk pedig $\operatorname{lkkt}(a,b)\sim$ (amennyiben létezik $\operatorname{lnko}(a,b)$ és $\operatorname{lkkt}(a,b)$).

3.12. Definíció. Azt mondjuk, hogy a $p \in R$ elem ***irreducibilis***, ha nem nulla és nem egység, és csak úgy bontható két elem szorzatára, hogy az egyik tényező asszociált p-hez. (Ekkor a másik tényező szükségképpen egység; ilyenkor ***triviális faktorizációról*** beszélünk.) Formálisan:

$$p \not\sim 0, 1 \quad \text{és} \quad \forall a, b \in R : p = ab \implies (p \sim a \text{ vagy } p \sim b)\,.$$

3.13. Definíció. Azt mondjuk, hogy a $p \in R$ elem ***prím***, ha nem nulla és nem egység, és valahányszor osztója egy szorzatnak, mindannyiszor osztója a szorzat egyik tényezőjének. Formálisan:

$$p \not\sim 0, 1 \quad \text{és} \quad \forall a, b \in R : p \mid ab \implies (p \mid a \text{ vagy } p \mid b)\,.$$

3.14. Tétel. Minden integritástartományban a prím elemek irreducibilisek.

3.15. Tétel. Ha az R integritástartományban bármely két elemnek létezik legnagyobb közös osztója, akkor R-ben minden irreducibilis elem prím.

3.16. Példa. A $\mathbb{Z}[\sqrt{-5}] = \left\{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\right\}$ integritástartományban az $a = 6$ és $b = 2 + 2\sqrt{-5}$ elemeknek nem létezik legnagyobb közös osztója. (Asszociáltság erejéig három közös osztójuk van: 1, 2 és $1 + \sqrt{-5}$, de ezek között nincs legnagyobb az oszthatóság szerinti részbenrendezésben.) A $\mathbb{Z}[\sqrt{-5}]$ gyűrűben 2 irreducibilis, de nem prím: $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$, de $2 \nmid 1 + \sqrt{-5}$ és $2 \nmid 1 - \sqrt{-5}$.

3.17. Definíció. ***Gauss-gyűrűnek*** nevezzük az olyan integritástartományokat, amelyekben minden a nullától és az egységektől különböző elem irreducibilis elemek szorzatára bomlik, és ez a felbontás a tényezők sorrendjétől és asszociáltságtól eltekintve egyértelmű. Tehát az R integritástartomány Gauss-gyűrű, ha minden $a \in R$ $(a \neq 0, a \not\sim 1)$ esetén léteznek olyan $p_1, \ldots, p_n \in R$ irreducibilis elemek, amelyekre $a = p_1 \cdot \ldots \cdot p_n$; továbbá amennyiben $a = q_1 \cdot \ldots \cdot q_m$ egy másik irreducibilis faktorizáció, akkor $n = m$, és létezik olyan $\pi \in S_n$, amelyre $p_i \sim q_{i\pi}$ $(i = 1, \ldots, n)$.

3.18. Példa. Az egész számok gyűrűje, a Gauss-egészek gyűrűje, és bármely test feletti polinomgyűrű Gauss-gyűrű. (A testek is Gauss-gyűrűk: a definíció üresen teljesül rájuk.)

3.19. Tétel. Legyen R Gauss-gyűrű, és legyen $a, b \in R$ irreducibilis felbontása $a \sim p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}$ és $b \sim p_1^{\beta_1} \cdot \ldots \cdot p_n^{\beta_n}$. (Az α_i, β_i kitevők nemnegatív egész számok; ha valamelyik p_i csak a vagy csak b felbontásában szerepel, akkor a másikban 0 kitevővel vesszük.) Ekkor teljesülnek az alábbiak:

(1) $a \mid b \iff \alpha_i \leq \beta_i$ $(i = 1, \ldots, n)$;
(2) $\operatorname{lnko}(a, b) \sim p_1^{\min(\alpha_1, \beta_1)} \cdot \ldots \cdot p_n^{\min(\alpha_n, \beta_n)}$;
(3) $\operatorname{lkkt}(a, b) \sim p_1^{\max(\alpha_1, \beta_1)} \cdot \ldots \cdot p_n^{\max(\alpha_n, \beta_n)}$.

3.20. Definíció. Az $(A; \leq)$ részbenrendezett halmaz teljesíti a ***leszállólánc-feltételt***, ha A-ban nem létezik végtelen szigorúan csökkenő sorozat, azaz nem léteznek olyan $a_1, a_2, \ldots \in A$ elemek, amelyekre $a_1 > a_2 > \cdots$. Másképpen fogalmazva, minden csökkenő sorozat előbb-utóbb stabilizálódik: ha $a_1 \geq a_2 \geq \cdots$, akkor $a_k = a_{k+1} = \cdots$ valamely k természetes számra. Hasonlóan definiálható a ***felszállólánc-feltétel*** is.

3.21. Tétel. Tetszőleges R integritástartomány esetén ekvivalensek az alábbiak:

(1) R Gauss-gyűrű;
(2) az $(R/\!\sim; |)$ részbenrendezett halmaz teljesíti a leszállólánc-feltételt, és R-ben bármely két elemnek létezik legnagyobb közös osztója;
(3) az $(R/\!\sim; |)$ részbenrendezett halmaz teljesíti a leszállólánc-feltételt, és R-ben minden irreducibilis elem prím.

3.22. Tétel. Ha R Gauss-gyűrű, akkor $R[x]$ is az.

3.23. Következmény. Ha K test, akkor $K[x]$ és $K[x, y] \cong K[x][y]$ Gauss-gyűrűk (és hasonlóan $K[x_1, \ldots, x_n]$ is minden n természetes számra). Az egész együtthatós polinomok $\mathbb{Z}[x]$ gyűrűje is Gauss-gyűrű.

Főideálgyűrűk

3.24. Állítás. Bármely $a, b \in R$ esetén érvényesek az alábbi ekvivalenciák:

(1) $a \mid b \iff \langle a \rangle \supseteq \langle b \rangle$;
(2) $a \sim b \iff \langle a \rangle = \langle b \rangle$;
(3) $a \sim 1 \iff \langle a \rangle = R$.

3.25. Következmény. Az $a, b \in R$ elemeknek a $d \in R$ elem akkor és csak akkor legnagyobb közös osztója, ha $\langle d \rangle$ a legszűkebb olyan főideál, ami tartalmazza $\langle a \rangle$-t is és $\langle b \rangle$-t is.

3.26. Megjegyzés. A legszűkebb ideál (nemcsak a főideálok, hanem az összes ideálok között), ami tartalmazza $\langle a \rangle$-t és $\langle b \rangle$-t is, nem más, mint $\langle a \rangle + \langle b \rangle$ (ez az ideálhálóbeli egyesítés, lásd az 1.76. Tételt és az 1.77. Megjegyzést). Csakhogy $\langle a \rangle + \langle b \rangle$ nem biztos, hogy főideál, és az sem biztos, hogy létezik $\operatorname{lnko}(a, b)$.

3.27. Definíció. Az R integritástartományt ***főideálgyűrűnek*** nevezzük, ha minden ideálja főideál, azaz minden $I \lhd R$ ideálhoz létezik olyan $a \in R$ elem, amelyre $I = \langle a \rangle$.

3.28. Állítás. Főideálgyűrűben bármely két elemnek létezik legnagyobb közös osztója (és így legkisebb közös többszöröse is), és az előáll a két elem „lineáris kombinációjaként": $\forall a, b \in R\ \exists x, y \in R$: $ax + by \sim \operatorname{lnko}(a, b)$.

3.29. Következmény. Főideálgyűrűben az $ax + by = c$ „diofantoszi egyenletnek" akkor és csak akkor van megoldása, ha $\operatorname{lnko}(a, b) \mid c$. Az általános megoldás ugyanúgy kapható meg egy partikuláris megoldásból, mint az egész számok gyűrűjében.

3.30. Definíció. Az R integritástartományt ***euklideszi gyűrűnek*** nevezzük, ha létezik olyan $\|\cdot\| : R \to \mathbb{N}_0$, $a \mapsto \|a\|$ leképezés (úgynevezett ***euklideszi norma***), amire teljesülnek az alábbiak tetszőleges $a \in R$ és $b \in R \setminus \{0\}$ esetén:

(a) $\|a\| = 0 \iff a = 0$;

(b) $a \mid b \implies \|a\| \leq \|b\|$;

(c) $\exists q, r \in R : a = bq + r$ és $\|r\| < \|b\|$.

3.31. Tétel. Minden euklideszi gyűrű főideálgyűrű.

3.32. Megjegyzés. A tétel megfordítása nem igaz: létezik olyan főideálgyűrű, amely nem euklideszi. Ilyen például a $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$ gyűrű, ahol $\omega = \frac{1+\sqrt{19}i}{2}$.

3.33. Következmény. Az egész számok gyűrűje, minden test feletti polinomgyűrű, valamint a Gauss-egészek gyűrűje főideálgyűrű.

3.34. Tétel. Minden főideálgyűrű Gauss-gyűrű.

3.35. Megjegyzés. A tétel megfordítása nem igaz: létezik olyan Gauss-gyűrű, ami nem főideálgyűrű. Ilyenek például a $\mathbb{Z}[x]$ és $K[x, y]$ gyűrűk (tetszőleges K test esetén).

3.36. Következmény. Az egész számok gyűrűje, minden test feletti polinomgyűrű, valamint a Gauss-egészek gyűrűje Gauss-gyűrű.

3.37. Tétel. Ha R főideálgyűrű és $m \in R \setminus \{0\}$, akkor az $R/\langle m \rangle$ faktorgyűrű akkor és csak akkor test, ha m irreducibilis.

4. Testbővítések, Galois-elmélet

Testbővítések fajtái

4.1. Definíció. Ha a K test részteste az L testnek, akkor azt mondjuk, hogy L ***testbővítése*** K-nak, és ezt így jelöljük: $L \mid K$ (lásd az 1.21. Definíciót). Az $L_1 \mid K$ és $L_2 \mid K$ testbővítések ***izomorfak***, ha létezik olyan $\varphi\colon L_1 \to L_2$ izomorfizmus, amelynek K-ra való megszorítása identikus (azaz $a\varphi = a$ minden $a \in K$ esetén).

A továbbiakban – hacsak mást nem mondunk – $L \mid K$ mindig egy tetszőleges testbővítést jelöl.

4.2. Definíció. Tetszőleges $\vartheta \in L$ esetén jelölje I_ϑ mindazon $f \in K[x]$ polinomok halmazát, amelyeknek ϑ gyöke: $I_\vartheta = \{f \in K[x] : f(\vartheta) = 0\}$. Ha $I_\vartheta = \{0\}$, akkor azt mondjuk, hogy ϑ ***transzcendens*** K felett, ellenkező esetben pedig azt mondjuk, hogy ϑ ***algebrai*** K felett. Könnyen ellenőrizhető, hogy $I_\vartheta \lhd K[x]$ (HF), és mivel $K[x]$ főideálgyűrű, I_ϑ főideál. Ezért, ha ϑ algebrai K felett, akkor létezik egy olyan egyértelműen meghatározott $m_{\vartheta,K} \in K[x]$ főpolinom, amelyre $I_\vartheta = \langle m_{\vartheta,K} \rangle$. Ekkor tehát minden $f \in K[x]$ esetén $f(\vartheta) = 0 \iff m_{\vartheta,K} \mid f$. Az $m_{\vartheta,K}$ polinomot a ϑ elem K feletti ***minimálpolinomjának***, $m_{\vartheta,K}$ gyökeit pedig a ϑ elem K feletti ***konjugáltjainak*** nevezzük. Ha L minden eleme algebrai K felett, akkor azt mondjuk, hogy $L \mid K$ ***algebrai testbővítés***, ellenkező esetben pedig ***transzcendens testbővítésről*** beszélünk.

4.3. Példa. A $\mathbb{C} \mid \mathbb{Q}$ testbővítés algebrai elemeit ***algebrai számoknak***, transzcendens elemeit pedig ***transzcendens számoknak*** nevezzük.

4.4. Állítás. Bármely $\vartheta \in L$ algebrai elem esetén $m_{\vartheta,K}$ irreducibilis K felett. Fordítva, ha $f \in K[x]$ irreducibilis K felett és $f(\vartheta) = 0$, akkor $f \sim m_{\vartheta,K}$.

4.5. Definíció. Tetszőleges $T \subseteq L$ halmaz esetén $K[T]$ jelöli a $K \cup T$ halmaz által generált részgyűrűt, és $K(T)$ jelöli a $K \cup T$ halmaz által generált résztestet L-ben. Ha $T = \{\vartheta\}$ egyelemű halmaz, akkor egyszerűen csak $K[\vartheta]$-t és $K(\vartheta)$-t írunk. A $K(\vartheta) \mid K$ alakú testbővítéseket ***egyszerű testbővítéseknek*** nevezzük (lásd az 1.23. Definíciót és az 1.22. Tételt), és azt mondjuk, hogy $K(\vartheta)$ a ϑ elem K-hoz történő ***adjungálásával*** keletkezik.

4.6. Definíció. Ha $L \mid K$ egy testbővítés, akkor L vektortertet alkot K felett. Ha ez a vektortér véges dimenziós, akkor azt mondjuk, hogy $L \mid K$ ***végesfokú testbővítés***, és a $\dim_K L$ dimenziót az $L \mid K$ bővítés ***fokszámának*** nevezzük. Jelölés: $[L : K] = \dim_K L$.

4.7. Tétel. Legyen $m \in K[x]$ irreducibilis n-edfokú polinom, és legyen $L = K[x] / \langle m \rangle$. Ekkor L test, amelyben a konstans polinomok modulo m maradékosztályai egy K-val izomorf résztestet alkotnak ($K \to L$, $a \mapsto a + \langle m \rangle$ beágyazás), tehát tekinthetjük úgy, hogy L bővítése K-nak. Ha az $x + \langle m \rangle \in L$ elemet α-val jelöljük, akkor L minden eleme egyértelműen előáll $a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$ $(a_{n-1}, \ldots, a_1, a_0 \in K)$ alakban. Következésképp $L = K[\alpha] = K(\alpha)$ és $[L : K] = n$. Az α elem gyöke az m polinomnak, tehát $m_{\alpha,K} \sim m$.

4.8. Tétel. Legyen $L = K(\vartheta)$ egyszerű algebrai bővítése K-nak, és legyen az $m = m_{\vartheta,K}$ polinom fokszáma n. Ekkor az $L \mid K$ bővítés izomorf a $K[x] / \langle m \rangle \mid K$ bővítéssel, és így $[L : K] = n$.

4.9. Tétel. A $K(x) \mid K$ bővítés egyszerű transzcendens bővítés. Fordítva, ha $L = K(\vartheta)$ egyszerű transzcendens bővítése K-nak, akkor az $L \mid K$ bővítés izomorf a $K(x) \mid K$ bővítéssel, és $[L : K] = \infty$.

4.10. Tétel. Legyenek $L \mid K$ és $M \mid L$ végesfokú testbővítések (tehát $K \le L \le M$), és legyen $\alpha_1, \ldots, \alpha_\ell$ bázisa az ${}_KL$ vektortérnek, $\beta_1, \ldots, \beta_m$ pedig legyen egy bázisa az ${}_LM$ vektortérnek. Ekkor $\alpha_i\beta_j$ $(i = 1, \ldots, \ell,\ j = 1, \ldots, m)$ bázisa az ${}_KM$ vektortérnek. Következésképp $[M : K] = [M : L] \cdot [L : K] = m \cdot \ell$.

4.11. Tétel. Minden végesfokú bővítés algebrai. Nulla karakterisztikájú testek (pl. számtestek) esetén minden végesfokú bővítés egyszerű algebrai bővítés: ha $\operatorname{char} K = 0$ és $[L : K] < \infty$, akkor létezik olyan $\vartheta \in L$ ***primitív elem***, amelyre $L = K(\vartheta)$.

4.12. Tétel. Minden testbővítésben az algebrai elemek résztestet alkotnak. Így például az algebrai számok is testet alkotnak (lásd a 4.3. Példát).

4.13. Definíció. Ha egy L testre teljesülnek az alábbi (egymással ekvivalens) feltételek, akkor azt mondjuk, hogy L ***algebrailag zárt***.

(1) Minden nemkonstans L feletti polinomnak van gyöke L-ben.

(2) Minden nemkonstans L feletti polinom elsőfokú polinomok szorzatára bomlik az $L[x]$ polinomgyűrűben.

(3) A L test felett csak az elsőfokú polinomok irreducibilisek.

Azt mondjuk, hogy L ***algebrai lezártja*** K-nak, ha L algebrailag zárt, és $L \mid K$ algebrai bővítés (jelölés: $L = \overline{K}$).

4.14. Tétel. Minden K testnek létezik algebrai lezártja, és az K feletti izomorfia erejéig egyértelmű (vagyis ha L_1 és L_2 is algebrai lezártja K-nak, akkor van olyan $\varphi\colon L_1 \to L_2$ izomorfizmus, amelynek K-ra való megszorítása identikus).

4.15. Megjegyzés. Algebrailag zárt testnek nincs valódi algebrai bővítése, tehát $\overline{K}$ maximális algebrai bővítése K-nak. Másrészt, $\overline{K}$ valódi résztestei már nem lesznek algebrailag zártak, tehát $\overline{K}$ minimális algebrailag zárt bővítése K-nak. Meg lehet mutatni, hogy ezen két tulajdonság bármelyike jellemzi az algebrai lezártat.

4.16. Példa. Az algebra alaptétele szerint a komplex számok teste algebrailag zárt. Mivel $\mathbb{C} \mid \mathbb{R}$ algebrai (miért?), $\overline{\mathbb{R}} = \mathbb{C}$. Ebben nem az a „pláne”, hogy $\mathbb{R}$-nek van algebrai lezártja, hanem az, hogy az algebrai lezárt mindössze másodfokú bővítés: elég az $x^2 + 1$ polinom egy gyökét adjungálni, és máris minden polinomnak lesz gyöke. A racionális számok testével más a helyzet: $\overline{\mathbb{Q}}$ nem más, mint az algebrai számok teste (lásd a 4.3. Példát), és $\overline{\mathbb{Q}} \mid \mathbb{Q}$ végtelen fokú bővítés (miért?).

Felbontási test, véges testek

4.17. Definíció. Azt mondjuk, hogy L ***felbontási teste*** a nemkonstans $f \in K[x]$ polinomnak (K felett), ha f elsőfokú polinomok szorzatára bomlik az $L[x]$ polinomgyűrűben, és az L testet K felett generálják f gyökei. Formálisan: léteznek olyan $\alpha_1, \ldots, \alpha_n \in L$ (nem feltétlenül különböző) elemek, hogy

(a) $f \sim (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$ és

(b) $L = K(\alpha_1, \ldots, \alpha_n)$.

4.18. Megjegyzés. A (b) feltétel azt jelenti, hogy f nem bontható lineáris tényezők szorzatára L semmilyen valódi résztestében, vagyis a K testet „épp csak annyira” bővítettük ki, amennyire szükséges.

4.19. Tétel. Minden polinomnak létezik felbontási teste, és az az alaptest feletti izomorfia erejéig egyértelmű. Az egyértelműség precízebben így fogalmazható meg: ha L_1 és L_2 is K feletti felbontási teste az $f \in K[x]$ polinomnak, akkor létezik olyan $\varphi\colon L_1 \to L_2$ izomorfizmus, melynek K-ra való megszorítása identikus.

4.20. Megjegyzés. Ha adott a K test $\overline{K}$ algebrai lezártja, akkor könnyen megkaphatjuk egy $f \in K[x]$ polinom felbontási testét: mivel $\overline{K}$ algebrailag zárt, f elsőfokú polinomok szorzatára bomlik $\overline{K}$ felett, azaz $f \sim (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$ alkalmas $\alpha_1, \ldots, \alpha_n \in \overline{K}$ elemekkel. Ekkor f felbontási teste $K(\alpha_1, \ldots, \alpha_n)$.

4.21. Tétel. Véges test elemszáma mindig prímhatvány.

4.22. Lemma. Tetszőleges p prímszám és $1 \leq k \leq p-1$ esetén $\binom{p}{k}$ osztható p-vel.

4.23. Következmény. Ha az L test karakterisztikája p (prímszám), akkor minden $n \in \mathbb{N}$ és $a, b \in L$ esetén

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

4.24. Tétel. Minden p^n prímhatvány esetén létezik, mégpedig izomorfia erejéig egyetlen p^n-elemű test, amelyet $\mathrm{GF}(p^n)$ jelöl (itt GF az angol „Galois field" kifejezés rövidítése).

4.25. Példa. Minden p prímszámra $\mathrm{GF}(p) \cong \mathbb{Z}_p$. A két legkisebb véges test, ami nem prímtest: $\mathrm{GF}(4) \cong \mathbb{Z}_2[x] / \langle x^2+1 \rangle$ és $\mathrm{GF}(8) \cong \mathbb{Z}_2[x] / \langle x^3+x+1 \rangle \cong \mathbb{Z}_2[x] / \langle x^3+x^2+1 \rangle$.

4.26. Tétel. Véges test multiplikatív csoportja ciklikus: $(\mathrm{GF}(p^n)^*; \cdot) \cong (\mathbb{Z}_{p^n-1}; \cdot)$.

4.27. Megjegyzés. Az $n=1$ esetben a fenti tétel azzal ekvivalens, hogy létezik primitív gyök modulo p.

4.28. Következmény. Minden p prímszám és n természetes szám esetén létezik n-edfokú irreducibilis polinom $\mathbb{Z}_p$ felett.

4.29. Tétel. A $\mathrm{GF}(p^n)$ testnek minden $d \mid n$ estén létezik egy és csak egy p^d-elemű részteste (és ezeken kívül más részteste nincs).

Geometriai szerkeszthetőség

Legyen adott a síkon egy legalább kételemű H ponthalmaz, amelyből kiindulva egy bizonyos pontot kell megszerkesztenünk a szokásos euklideszi szerkesztési lépésekkel (ez a ***szerkesztési feladat***). Válasszunk tetszőlegesen $O, E \in H$ pontokat, és vegyük fel a síkon a valós és a képzetes tengelyt úgy, hogy O feleljen meg a 0-nak és E az 1-nek. Így a sík minden pontja egy komplex számnak felel meg, ezért ezentúl a szerkesztési feladatra úgy gondolunk, hogy adott komplex számokból kell egy kívánt komplex számot megszerkeszteni. A H halmazba tartozó (pontoknak megfelelő) komplex számok és konjugáltjaik által generált K számtestet a szerkesztési feladat ***alaptestének*** nevezzük. Meg lehet mutatni, hogy az alaptest nem függ az O és E pontok megválasztásától. A következőkben K mindig a szerkesztés alaptestét jelenti.

4.30. Definíció. Az α komplex számot K feletti ***négyzetgyökmennyiségnek*** nevezzük, ha α megkapható K elemeiből a négy alapművelet és négyzetgyökvonás véges számú alkalmazásával.

4.31. Definíció. Az $L \mid K$ testbővítés ***egyszerű négyzetgyökbővítés***, ha $L = K(\sqrt{a})$ valamely $a \in K$ elemre. Az $L \mid K$ testbővítés ***négyzetgyökbővítés***, ha megkapható véges sok egyszerű négyzetgyökbővítés egymásutánjaként:

$$K = T_0 \leq T_1 \leq \cdots \leq T_\ell = L, \quad \text{ahol minden } i\text{-re } T_{i+1} = T_i(\sqrt{a_i}) \text{ és } a_i \in T_i.$$

4.32. Állítás. Négyzetgyökbővítés foka mindig kettőhatvány. (Fordítva ez általában nem igaz, de *normális* testbővítésekre igen; lásd a 4.54. Definíciót.)

4.33. Tétel. Tetszőleges α komplex számra az alábbiak ekvivalensek:

(1) α megszerkeszthető (K-ból);

(2) α négyzetgyökmennyiség K felett;

(3) α benne van K valamely négyzetgyökbővítésében.

4.34. Következmény. Ha α megszerkeszthető, akkor α algebrai K felett, és $m_{\alpha,K}$ foka kettőhatvány.

4.35. Megjegyzés. A fenti következmény megfordítása nem igaz; például az x^4+7x+7 polinom gyökei nem szerkeszthetőek meg a $K=\mathbb{Q}$ alaptestből.

4.36. Tétel. Az α komplex szám akkor és csak akkor szerkeszthető meg a K alaptestből kiindulva, ha α algebrai K felett, és $m_{\alpha,K}$ *felbontási testének* foka kettőhatvány.

4.37. Definíció. Az n-edik ***körosztási polinom*** az a Φ_n polinom, amelynek gyökei éppen a primitív n-edik egységgyökök (mindegyik egyszeres gyök):

$$\Phi_n = \prod_{\substack{\varepsilon \in \mathbb{C}^* \\ o(\varepsilon)=n}} (x-\varepsilon) = \prod_{\substack{k=1,\ldots,n \\ \mathrm{lnko}(k,n)=1}} (x-\varepsilon_k).$$

4.38. Tétel. A körosztási polinomok egész együtthatósak, és irreducibilisek $\mathbb{Q}$ felett.

4.39. Következmény. Ha ε primitív n-edik egységgyök, akkor $m_{\varepsilon,\mathbb{Q}} = \Phi_n$.

4.40. Lemma. Ha szerkeszthető szabályos n-szög, akkor minden $d \mid n$ esetén szerkeszthető szabályos d-szög is, és minden $k \geq 0$ esetén szerkeszthető szabályos $2^k n$-szög is. Ha szerkeszthető szabályos n-szög és m-szög, akkor szerkeszthető szabályos $\mathrm{lkkt}(n,m)$-szög is.

4.41. Tétel (Gauss–Wantzel-tétel). A szabályos n-szög akkor és csak akkor szerkeszthető, ha az n prímfelbontásában fellépő páratlan prímek mind Fermat-prímek, és mindegyik első hatványon lép fel, azaz $n = 2^k \cdot p_1 \cdot \ldots \cdot p_t$, ahol $k \in \mathbb{N}_0$ és $p_1, \ldots, p_t$ páronként különböző Fermat-prímek.

Galois-kapcsolatok és fogalomhálók

4.42. Definíció. Az U halmazon értelmezett ***lezárási operátoron*** olyan $\mathcal{P}(U) \to \mathcal{P}(U)$, $A \mapsto \overline{A}$ leképezést értünk, amely rendelkezik az alábbi három tulajdonsággal:

(a) *monoton*: $A \subseteq B \implies \overline{A} \subseteq \overline{B}$ minden $A, B \subseteq U$ esetén;

(b) *extenzív*: $\overline{A} \supseteq A$ minden $A \subseteq U$ esetén;

(c) *idempotens*: $\overline{\overline{A}} = \overline{A}$ minden $A \subseteq U$ esetén.

Ha $\overline{A} = A$, akkor azt mondjuk, hogy A ***zárt halmaz***.

4.43. Állítás. Tetszőleges lezárási operátor esetén érvényesek az alábbiak (minden $A, B \subseteq U$ esetén):

(1) A zárt $\iff \exists B \subseteq U : A = \overline{B}$;

(2) A, B zárt $\implies A \cap B$ is zárt;

(3) $\overline{A \cup B}$ az a legszűkebb zárt halmaz, ami tartalmazza A-t és B-t;

(4) a zárt halmazok hálót alkotnak, amelyben $A \wedge B = A \cap B$ és $A \vee B = \overline{A \cup B}$.

4.44. Példa.

(1) Ha $\mathbb{A} = (A; F)$ egy algebra, akkor $\mathcal{P}(A) \to \mathcal{P}(A)$, $T \mapsto [T]$ lezárási operátor az A halmazon, és a zárt halmazok hálója nem más, mint $\mathbb{A}$ részalgebrahálója (lásd az 1.16. Definíciót). Ennek a példának speciális esetei a részcsoporthálók, normálosztóhálók, részgyűrűhálók, ideálhálók, résztesthálók.

(2) Legyen U a sík (vagy a tér) pontjainak halmaza, és legyen $\overline{A}$ az A halmaz konvex burka. Ez egy lezárási operátor, amelynél a zárt halmazok éppen a konvex halmazok.

(3) A sík (vagy a tér) pontjainak halmazán a topológiai lezárás (torlódási pontok hozzávétele) is lezárási operátor; itt a zárt halmazok éppen a zárt halmazok(!).

Legyen adott objektumok egy G halmaza (németül Gegenstand) és tulajdonságok (attribútumok) egy M halmaza (németül Merkmal). Minden $g \in G$ és $m \in M$ esetén meg van határozva, hogy g rendelkezik-e az m tulajdonsággal. Ezt egy $I \subseteq G \times M$ megfeleltetés írja le: $(g, m) \in I$ (vagy egyszerűbb jelöléssel gIm) akkor és csak akkor teljesül, ha g rendelkezik az m tulajdonsággal. A (G, M, I) hármast ***kontextusnak*** nevezzük.

Tetszőleges $X \subseteq G$ és $Y \subseteq M$ esetén legyen

$$X' = \alpha(X) = \{m \in M \mid \forall g \in X : gIm\} \subseteq M,$$
$$Y' = \beta(Y) = \{g \in G \mid \forall m \in Y : gIm\} \subseteq G.$$

Tehát $\alpha(X)$ mindazon tulajdonságok halmaza, amelyekkel X minden eleme rendelkezik, $\beta(Y)$ pedig mindazon objektumok halmaza, amelyek rendelkeznek az összes Y-beli tulajdonsággal. Az egyszerűség kedvéért az $X' = \alpha(X)$ és $Y' = \beta(Y)$ jelölést használjuk; a szövegkörnyezetből (remélhetőleg) kiderül, hogy melyik vessző jelent alfát és melyik bétát. (Pl. ha $X \subseteq G$, akkor $X''' = \alpha(\beta(\alpha(X)))$ és ha ha $Y \subseteq M$, akkor $Y''' = \beta(\alpha(\beta(Y)))$.) Így tehát definiáltunk egy $\alpha\colon \mathcal{P}(G) \to \mathcal{P}(M)$, $X \mapsto X'$ és egy $\beta\colon \mathcal{P}(M) \to \mathcal{P}(G)$, $Y \mapsto Y'$ leképezést; ezt a leképezéspárt nevezzük ***Galois-kapcsolatnak***.

4.45. Állítás. Tetszőleges $X, X_1, X_2 \subseteq G$ és $Y, Y_1, Y_2 \subseteq M$ esetén teljesülnek az alábbiak:

(1) $X_1 \subseteq X_2 \implies X_1' \supseteq X_2'$ és $Y_1 \subseteq Y_2 \implies Y_1' \supseteq Y_2'$;

(2) $X'' \supseteq X$ és $Y'' \supseteq Y$;

(3) $X''' = X'$ és $Y''' = Y'$.

4.46. Következmény. A „kettővessző” operátorok: $\mathcal{P}(G) \to \mathcal{P}(G)$, $X \mapsto X''$ illetve $\mathcal{P}(M) \to \mathcal{P}(M)$, $Y \mapsto Y''$, lezárási operátorok G-n illetve M-en. A megfelelő zárt halmazokat ***Galois-zárt*** halmazoknak nevezzük.

4.47. Állítás. Tetszőleges $X \subseteq G$ és $Y \subseteq M$ esetén

$$X \text{ Galois-zárt} \iff \exists Y \subseteq M\colon X = Y';$$
$$Y \text{ Galois-zárt} \iff \exists X \subseteq G\colon Y = X'.$$

4.48. Tétel. Legyen L_G a G halmaz Galois-zárt részhalmazainak hálója, L_M pedig az M halmaz Galois-zárt részhalmazainak hálója. Ekkor $\varphi\colon L_G \to L_M$, $X \mapsto X'$ és $\psi\colon L_M \to L_G$, $Y \mapsto Y'$ rendezésfordító bijekciók (egymás inverzei). Következésképp L_G izomorf L_M duálisával („fejreállítottjával”).

4.49. Megjegyzés. Mivel L_G és L_M duálisan izomorfak, lehet őket egy Hasse-diagramon ábrázolni úgy, hogy L_G Hasse-diagramjában az $X \in L_G$ halmazt jelképező ponthoz az (X, Y) címkét írjuk, ahol $Y = X'$ (ekkor persze $Y' = X$). Az ilyen (X, Y) párt ***fogalomnak*** nevezzük; X a fogalom *terjedelme* (azon objektumok halmaza, amelyek az adott fogalomhoz tartoznak), Y pedig a fogalom *tartalma* (a fogalomra jellemző tulajdonságok összessége). A fogalmak halmazán L_G-ből (és L_M duálisából) adódik rendezés: $(X_1, Y_1) \leq (X_2, Y_2) \iff X_1 \subseteq X_2 \,(\iff Y_1 \supseteq Y_2)$; így kapjuk a (G, M, I) kontextushoz tartozó ***fogalomhálót***.

4.50. Példa. Legyen G rögzített típusú algebrák halmaza (pl. grupoidok), M pedig a típusnak megfelelő azonosságok halmaza, és jelentse I azt, hogy az adott algebra teljesíti az adott azonosságot. (Például $(\mathbb{Z}_6, xy = yx) \in I$ és $\left(V, x^2 = y^2\right) \in I$, de $(S_3, xy = yx) \notin I$.) Ekkor egy X algebrahalmazra X' mindazon azonosságokat tartalmazza, amelyeket X minden eleme kielégít, egy Y azonosséghalmaz esetén pedig Y' az Y-beli azonosságokat kielégítő összes algebrák halmaza. Például $\{(xy)\,z = x\,(yz)\,, xy = yx\}'$ a kommutatív félcsportok halmaza, $\{(xy)\,z = x\,(yz)\,, xy = yx\}''$ pedig az összes olyan azonosságot tartalmazza, ami teljesül minden kommutatív félcsoporton, vagyis az asszociativitás és a kommutativitás következményeit (pl. $(xy)\,(xz) = x\,(z\,(yx))$). Könnyű belátni, hogy minden azonosság „öröklődik" részalgebrákra, faktoralgebrákra és direkt szorzatokra, tehát Y' mindig zárt erre a három konstrukcióra. *Birkhoff tétele* szerint ennek a megfordítása is igaz: ha egy X algebraosztály zárt a részalgebra, faktoralgebra és direkt szorzat képzésére, akkor definiálható azonosságokkal, azaz Galois-zárt (előáll $X = Y'$ alakban). Az ilyen algebraosztályokat nevezzük *varietásoknak*. Tehát ebben a kontextusban a zárt algebraosztályok éppen a varietások, a zárt azonosséghalmazokat pedig bizonyos logikai dedukciós lépésekre való zártsággal lehet jellemezni (ezeket *azonosságelméleteknek* nevezzük).

Galois-elmélet

A továbbiakban az egyszerűség kedvéért feltesszük, hogy minden szóba kerülő test számtest, és minden bővítés végesfokú.

4.51. Definíció. Az $L \mid K$ testbővítés ***Galois-csoportja*** azon $L \to L$ automorfizmusok csoportja, melyek pontonként fixen hagyják K-t (vagyis az $L \mid K$ bővítést saját magára képező izomorfizmusok csoportja; lásd a 4.1. Definíciót):

$$\mathrm{Gal}\,(L \mid K) = \mathrm{Aut}_K L = \{\sigma \colon L \to L \text{ izomorfizmus, } \sigma|_K = \mathrm{id}_K\}\,.$$

4.52. Definíció. Az $L \mid K$ testbővítés ***közbülső testein*** olyan E testeket értünk, amelyekre $K \leq E \leq L$ teljesül. A közbülső testek halmazát $\mathrm{Sub}\,(L \mid K)$ jelöli.

4.53. Tétel. Tetszőleges $L \mid K$ végesfokú bővítés esetén ekvivalensek az alábbiak:

(1) Ha $f \in K\,[x]$ irreducibilis polinom és f-nek van gyöke L-ben, akkor f elsőfokú polinomok szorzatára bomlik L felett (azaz f „minden gyöke" L-ben van).

(2) Ha egy szám L-ben van, akkor minden konjugáltja (a 4.2. Definíció értelmében) is L-ben van (azaz L zárt a „konjugálásra").

(3) Van olyan K feletti polinom, amelynek felbontási teste éppen L.

4.54. Definíció. A fenti ekvivalens tulajdonságokkal rendelkező testbővítéseket ***normális bővítéseknek*** nevezzük.

4.55. Állítás. Minden $L \mid K$ testbővítés kiterjeszthető normális bővítéssé: létezik olyan $N \geq L$ test, amelyre $N \mid K$ normális bővítés. Az ilyen N testek között van egy legszűkebb; ezt nevezzük $L \mid K$ ***normális lezártjának***.

4.56. Definíció. Egy $f \in K\,[x]$ polinom ***Galois-csoportján*** a K feletti felbontási testének a Galois-csoportját értjük: $\mathrm{Gal}\,(f) = \mathrm{Gal}\,(N \mid K)$, ahol N az f polinom K feletti felbontási teste.

4.57. Tétel. Tetszőleges $N \mid K$ normális bővítés és $\alpha, \beta \in N$ esetén α és β akkor és csak akkor vannak a $\mathrm{Gal}\,(N \mid K)$ csoport hatása szerint ugyanazon a pályán (lásd a 2.7. Definíciót), ha egymás konjugáltjai K felett:

$$\exists \sigma \in \mathrm{Gal}\,(N \mid K) : \alpha\sigma = \beta \iff m_{\alpha,K} = m_{\beta,K}.$$

4.58. Tétel. Normális bővítés Galois-csoportjának rendje megegyezik a bővítés fokszámával: ha $N \mid K$ normális bővítés, akkor $|\mathrm{Gal}\,(N \mid K)| = [N : K]$.

4.59. Tétel. Legyen az n-edfokú $f \in K\,[x]$ polinom felbontási teste N, gyökeinek halmaza pedig Gy. Tegyül fel, hogy f minden gyöke egyszeres (vagyis $|Gy| = n$). Ekkor minden $\sigma \in \mathrm{Gal}\,(N \mid K)$ esetén $Gy\sigma = Gy$, így van értelme megszorítani a σ automorfizmust a Gy halmazra. A $\varphi \colon \mathrm{Gal}\,(N \mid K) \to S_{Gy}$, $\sigma \mapsto \sigma|_{Gy}$ leképezés beágyazza a $\mathrm{Gal}\,(N \mid K)$ csoportot az S_{Gy} csoportba, azaz $\mathrm{Gal}\,(f)$ izomorf S_n egy részcsoportjával.

4.60. Tétel (a Galois-elmélet főtétele). Legyen $N \mid K$ normális testbővítés és $G = \mathrm{Gal}(N \mid K) = \mathrm{Aut}_K N$. Tekintsük az $I = \{(\alpha, \sigma) : \alpha\sigma = \alpha\} \subseteq N \times G$ „illeszkedési reláció" által indukált Galois-kapcsolatot:

$$\mathcal{P}(N) \to \mathcal{P}(G), \quad E \mapsto \{\sigma \in G \mid \forall \alpha \in E : \alpha\sigma = \alpha\} = E' = \mathrm{Gal}(N \mid E);$$
$$\mathcal{P}(G) \to \mathcal{P}(N), \quad H \mapsto \{\alpha \in N \mid \forall \sigma \in H : \alpha\sigma = \alpha\} = H' = \mathrm{Fix}(H).$$

Ekkor teljesülnek az alábbiak:

(I) Az N halmaz Galois-zárt részhalmazai éppen a közbülső testek:

$$\forall E \subseteq N : \ E'' = E \iff K \leq E \leq N \quad (\text{azaz } E \in \mathrm{Sub}(N \mid K)).$$

(II) A G halmaz Galois-zárt részhalmazai éppen a részcsoportok:

$$\forall H \subseteq G : \ H'' = H \iff H \leq G \quad (\text{azaz } H \in \mathrm{Sub}\, G).$$

(III) A $\mathrm{Sub}(N \mid K)$ és $\mathrm{Sub}\, G$ hálók között duális izomorfizmust létesítenek az

$$E \mapsto E' = \mathrm{Gal}(N \mid E) \quad \text{és} \quad H \mapsto H' = \mathrm{Fix}(H)$$

leképezések (amelyek egymás inverzei).

(IV) Ha $E \in \mathrm{Sub}(N \mid K)$ és $H \in \mathrm{Sub}\, G$ egymásnak megfelelő résztest és részcsoport, azaz

$$E = H' = \mathrm{Fix}(H) \quad \text{és} \quad H = E' = \mathrm{Gal}(N \mid E),$$

akkor

(a) $[N : E] = |H|$ és $[E : K] = [G : H]$;

(b) $N \mid E$ normális;

(c) $E \mid K$ normális $\iff H \triangleleft G$, és ha ez teljesül, akkor $\mathrm{Gal}(E \mid K) \cong G/H$, azaz

$$\mathrm{Gal}(E \mid K) \cong \mathrm{Gal}(N \mid K) \,/\, \mathrm{Gal}(N \mid E).$$

Gyökjelekkel való megoldhatóság

4.61. Definíció. Az α komplex számot K feletti ***gyökmennyiségnek*** nevezzük, ha α megkapható K elemeiből a négy alapművelet és pozitív egész kitevős gyökvonások véges számú alkalmazásával.

4.62. Definíció. Az $L \mid K$ testbővítés ***egyszerű radikálbővítés***, ha $L = K(\sqrt[n]{a})$ valamely $a \in K$ elemre és n természetes számra. Az $L \mid K$ testbővítés ***radikálbővítés***, ha megkapható véges sok egyszerű radikálbővítés egymásutánjaként:

$$K = T_0 \leq T_1 \leq \cdots \leq T_\ell = L, \quad \text{ahol minden } i\text{-re } T_{i+1} = T_i(\sqrt[n_i]{a_i}) \text{ és } a_i \in T_i,\ n_i \in \mathbb{N}.$$

4.63. Tétel. Tetszőleges α komplex számra az alábbiak ekvivalensek:

(1) α gyökmennyiség K felett;

(2) α benne van K valamely radikálbővítésében;

(3) α benne van K valamely normális radikálbővítésében.

4.64. Következmény. Ha α gyökmennyiség K felett, akkor α algebrai K felett.

4.65. Definíció. A G csoport ***feloldható***, ha létezik olyan $\{1\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{\ell-1} \triangleleft G_\ell = G$ *normállánc*, amelynek minden G_{i+1}/G_i faktora Abel-csoport.

4.66. Példa. Minden Abel-csoport feloldható. A diédercsoportok, valamint az S_3 és S_4 szimmetrikus csoportok feloldhatóak, de $n \geq 5$ esetén S_n már nem feloldható.

4.67. Tétel. Tetszőleges $f \in K[x]$ polinomra ekvivalensek az alábbiak:

(1) f-nek van olyan gyöke, ami gyökmennyiség K felett;

(2) f minden gyöke gyökmennyiség K felett;

(3) f Galois-csoportja feloldható.

4.68. Tétel. Az $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$ polinom Galois-csoportja S_5. Következésképp f gyökei nem gyökmennyiségek $\mathbb{Q}$ felett (vagyis az $x^5 - 4x + 2 = 0$ egyenlet „nem oldható meg gyökjelekkel").

4.69. Tétel (Ruffini–Abel-tétel). Az általános n-edfokú egyenletnek nincs megoldóképlete, azaz nem létezik olyan, az $a_{n-1}, \ldots, a_1, a_0$ szimbólumokból a négy alapművelet és gyökvonások véges számú alkalmazásával felírható képlet, ami minden $a_{n-1}, \ldots, a_1, a_0 \in \mathbb{C}$ komplex értékekre az $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$ egyenlet egy megoldását adja.

4.70. Tétel (a casus irreducibilis tétele). Ha az $f \in \mathbb{Q}[x]$ polinom irreducibilis $\mathbb{Q}$ felett és minden gyöke valós, akkor f gyökei nem fejezhetőek ki $\mathbb{Q}$ feletti *valós* gyökkifejezéssel (azaz nem létezik olyan $L \mid \mathbb{Q}$ radikálbővítés, ami tartalmazza f egyik (minden) gyökét, és $L \subseteq \mathbb{R}$).