Direkt limesz, inverz limesz, végtelen Galois-bővítések

Az alábbi jegyzetben a direkt limeszt, az inverz limeszt, testek algebrai lezártjának létezését, ill. a végtelen Galois-csoportokat tekintjük át. Nem minden bizonyítás szerepelt előadáson (vagy gyakorlaton), ezeket természetesen nem kell tudni. Az algebrai lezárt konstrukciója lényegében megegyezik Pelikán József [1] internetes Algebra jegyzetében szereplő konstrukcióval.

1. Direkt limesz

Legyen I egy (általában végtelen) részbenrendezett halmaz, melyben bármely két elemnek van közös felső korlátja (azaz *I jobb filtrált*). Ekkor természetesen bármely véges sok elemnek is van közös felső korlátja.

1.1. Definíció. *Legyenek az A_i halmazok az I részbenrendezett halmazzal indexelve, és minden $i \leq j$-re legyen adva egy $f_{ji} \colon A_i \to A_j$ függvény az alábbi tulajdonságokkal: (1) $f_{ii} = \mathrm{id}_{A_i}$ minden $i \in I$-re; (2) ha $i \leq j \leq k \in I$, akkor $f_{ki} = f_{kj} \circ f_{ji}$. Az $(A_i)_{i\in I}$ halmazrendszert ekkor* direkt rendszer*nek nevezzük. Az $(A_i)_{i\in I}$ direkt rendszer* direkt limesz*én a*

$$\varinjlim_{i\in I} A_i := \dot{\bigcup} A_i / \sim \ ,$$

ahol $\sim$ a következő ekvivalenciareláció a $\dot{\bigcup}_{i\in I} A_i$ diszjunkt unión: $a_i \sim a_j$ ($a_i \in A_i$, $a_j \in A_j$, $i, j \in I$) akkor és csak akkor, ha van olyan $k \in I$, melyre $i \leq k$, $j \leq k$ és $f_{ki}(a_i) = f_{kj}(a_j) \in A_k$. Az $a_i \in A_i$ osztályát a $\varinjlim A_i$ direkt limeszben $[a_i]$-vel jelöljük. A direkt limeszt időnként injektív limesznek, vagy kolimesznek is nevezik.

1.2. Megjegyzés. *Ha az A_i halmazok topologikus terek, és az f_{ji} leképezések folytonosak, akkor a $\varinjlim_{i\in I} A_i$ is egy topologikus tér lesz (a diszjunkt unión vett ekvivalenciareláció szerinti faktortértopológiával). Ez a topológia $\varinjlim_{i\in I} A_i$-n a* direkt limesz topológia*, mely nem más, mint a legfinomabb olyan topológia, melyre nézve az $A_i \hookrightarrow \dot{\bigcup} A_i \twoheadrightarrow \varinjlim A_i$ leképezések mind folytonosak.*

1.3. Állítás. *Ha az A_i halmazok csoportok, és az f_{ji} leképezések csoporthomomorfizmusok, akkor $\varinjlim A_i$ is csoport az $[a_i] \cdot [a_j] := [f_{ki}(a_i) \cdot f_{ji}(a_i)]$ művelettel, ahol $k \in I$ tetszőleges közös felső korlátja $i, j \in I$-nek.*

Bizonyítás. A jóldefiniáltság abból következik, hogy $[a_i] = [f_{ki}(a_i)]$, és ha $a_i \sim a_{i'}$ (melyet egy $i, i' \leq k_1 \in I$ index bizonyít), $a_j \sim a_{j'}$ (melyet egy $j, j' \leq k_2 \in I$ index bizonyít) és k, k' egy-egy közös felső korlátja i, j-nek, illetve i', j'-nek rendre, akkor vehetünk egy $k_0 \in I$ közös felső korlátot az $i, j, k, i', j', k', k_1, k_2 \in I$ elemeknek. Ekkor (többször használva, hogy az f-ek homomorfizmusok, és jól viselkednek a kompozícióra)

$$\begin{aligned} f_{k_0k}(f_{ki}(a_i)f_{kj}(a_j)) = f_{k_0k} \circ f_{ki}(a_i) f_{k_0k} \circ f_{kj}(a_j) = \\ = f_{k_0i}(a_i) f_{k_0j}(a_j) = f_{k_0k_1} \circ f_{k_1i}(a_i) f_{k_0k_2} \circ f_{k_2j}(a_j) = \\ = f_{k_0k_1} \circ f_{k_1i'}(a_{i'}) f_{k_0k_2} \circ f_{k_2j'}(a_{j'}) = f_{k_0i'}(a_{i'}) f_{k_0j'}(a_{j'}) = f_{k_0k'}(f_{k'i'}(a_{i'}) f_{k'j'}(a_{j'})) \ . \end{aligned}$$

Az asszociativitás egy hasonló számolás és $[a_i]^{-1} = [a_i^{-1}]$. □

A fenti bizonyítás azt is mutatja, hogy ha az A_i-ken tetszőleges műveletek vannak adva, amiket az f_{ji} leképezések megtartanak, akkor a direkt limeszen is értelmezhetők ugyanezek a műveletek. Sőt, ha vannak azonosságaink, melyek az összes A_i-ben teljesülnek, akkor azok az azonosságok a direkt limeszben is teljesülni fognak. Tehát gyűrűk, modulusok, vektorterek direkt limesze is gyűrű, modulus, vektortér. Sőt, ha feltesszük, hogy a leképezések mindig testhomomorfizmusok, melyek az 1-et az 1-be viszik (speciálisan injektívek), akkor testek direkt limesze is test lesz, hiszen minden nem 0 elemnek lesz inverze.

1.4. Példa. *Ha $I = \mathbb{Z}^{>0}$ az oszthatóságra nézve, és $\mu_n \leq \mathbb{C}^\times$ jelöli az n-edik egységgyökök csoportját, és $n \mid m$ esetén $f_{mn} \colon \mu_n \to \mu_m$ a természetes tartalmazás, akkor $\varinjlim_n \mu_n \cong \mu_\infty$ az összes komplex egységgyök csoportja.*

1.5. Állítás. *A direkt limesz funktor egzakt (Abel-csoportokon).*

Mielőtt belekezdenénk a fenti állítás bizonyításába, először azt kell megmondanunk, mitől is lesz a „direkt limesz” egy funktor, és melyik kategóriából melyikbe képez. Rögzítsünk egy I jobb filtrált részbenrendezett halmazt, és tekintsük ezzel a részbenrendezett halmazzal indexelt Abel-csoportok direkt rendszereit, mint objektumokat. Egy $(A_i, f_{ji})_{i\leq j\in I}$ és egy $(B_i, g_{ji})_{i\leq j\in I}$ direkt rendszer között egy $\varphi = (\varphi_i)_{i\in I}$ morfizmus alatt $\varphi_i \colon A_i \to B_i$ $(i \in I)$ Abel-csoport homomorfizmusok egy rendszerét értjük, melyekre minden $i \leq j \in I$ esetén a

$$\begin{array}{ccc} A_i & \xrightarrow{\varphi_i} & B_i \\ {\scriptstyle f_{ji}}\downarrow & & \downarrow{\scriptstyle g_{ji}} \\ A_j & \xrightarrow{\varphi_j} & B_j \end{array}$$

diagram kommutatív. Vegyük észre, hogy direkt rendszerek közti leképezések magja és képe (sőt, komagja) is direkt rendszer, ezért van értelme direkt rendszerek egzakt sorozatáról beszélni. Továbbá ha φ egy morfizmus az $(A_i)_{i\in I}$ és a $(B_i)_{i\in I}$ direkt rendszer között, akkor φ indukál egy $\varinjlim \varphi_i \colon \varinjlim A_i \to \varinjlim B_i$ Abel-csoport homomorfizmust a direkt limeszek között. Tehát $\varinjlim_{i\in I}$ valóban egy funktor, mégpedig az I-vel indexelt Abel-csoportokból álló direkt rendszerek kategóriájából az Abel-csoportok kategóriájába, és van értelme arról beszélni, hogy egzakt sorozatot egzaktba visz-e.

Bizonyítás. Azt kell belátnunk, hogy ha $(A_i, f_{ji})_{i\leq j\in I} \xrightarrow{\alpha} (B_i, g_{ji})_{i\leq j\in I} \xrightarrow{\beta} (C_i, h_{ji})_{i\leq j\in I}$ direkt rendszerek egy egzakt sorozata, akkor $\varinjlim A_i \xrightarrow{\varinjlim \alpha_i} \varinjlim B_i \xrightarrow{\varinjlim \beta_i} \varinjlim C_i$ is egzakt. Az, hogy $\varinjlim \beta_i \circ \varinjlim \alpha_i = \varinjlim(\beta_i \circ \alpha_i) = \varinjlim 0 = 0$ (vagyis $\mathrm{Im}(\varinjlim \alpha_i) \subseteq \mathrm{Ker}(\varinjlim \beta_i)$), világos. Másrészt legyen $b = [b_i] \in \mathrm{Ker}(\beta) \subseteq \varinjlim B_i$. Ez azt jelenti, hogy $(\varinjlim \beta_i)(b) = [\beta_i(b_i)] = [0] = 0$ $\varinjlim C_i$-ben. A $\sim$ ekvivalenciareláció definíciója szerint ez azt jelenti, hogy van olyan $k \geq i \in I$, melyre $h_{ki}(\beta_i(b_i)) = h_{ki}(0) = 0 \in C_k$. Node $0 = h_{ki}(\beta_i(b_i)) = \beta_k(g_{ki}(b_i))$, azaz $g_{ki}(b_i) \in \mathrm{Ker}(\beta_k) = \mathrm{Im}(\alpha_k)$ (a direkt rendszerek közti sorozat egzaktsága miatt). Ekkor van olyan $a_k \in A_k$, melyre $\alpha_k(a_k) = g_{ki}(b_i)$, azaz $b = [b_i] = [g_{ki}(b_i)] = [\alpha_k(a_k)] = \varinjlim \alpha_i([a_k]) \in \mathrm{Im}(\varinjlim \alpha_i)$. Tehát $\mathrm{Ker}(\varinjlim \beta_i) \subseteq \mathrm{Im}(\varinjlim \alpha_i)$, mivel $b \in \mathrm{Ker}(\varinjlim \beta_i)$ tetszőleges volt. □

2. Inverz limesz

2.1. Definíció. *Legyenek az A_i halmazok ismét egy részben rendezett I halmazzal indexelve (melyben bármely két elemnek van felső korlátja, de ez itt a definícióhoz nem szükséges, csak* *a későbbi állításokhoz). Az $(A_i)_{i\in I}$ halmazok egy* inverz rendszer*t alkotnak, ha minden $i \le j \in I$-re adva van egy $f_{ij}\colon A_j \to A_i$ függvény, melyre* (1) $f_{ii} = \mathrm{id}_{A_i}$; (2) $i \le j \le k$ *esetén* $f_{ij} \circ f_{jk} = f_{ik}$. *Az A_i halmazok inverz limesze a*

$$\varprojlim_{i\in I} A_i := \{(a_i)_{i\in I} \in \prod_{i\in I} A_i \mid f_{ij}(a_j) = a_i \text{ minden } i \le j \in I\text{-re}\}$$

halmaz. Az inverz limeszt időnként projektív limesznek vagy egyszerűen csak limesznek is nevezik.

2.2. Megjegyzés. *Ha az A_i halmazok topologikus terek, és az f_{ij} $(i \le j \in I)$ leképezések folytonosak, akkor a $\varprojlim A_i$ halmazon értelmezhetjük a szorzattopológia altértopológiáját, melyre nézve egy topologikus tér lesz. Ez a topológia nem más, mint a legdurvább olyan topológia, melyre nézve a $\varprojlim_{i\in I} A_i \hookrightarrow \prod_{i\in I} A_i \to A_j$ leképezések folytonosak minden $j \in I$-re. Másrészt az is világos, hogy ha az A_i halmazok csoportok (gyűrűk, modulusok, stb.) és az f_{ij} leképezések homomorfizmusok, akkor a $\varprojlim A_i$ részcsoportja (részgyűrűje, részmodulusa, stb.) lesz a direkt szorzatnak.*

2.3. Példa. *A p-adikus egészek gyűrűje felírható inverz limeszként: $\mathbb{Z}_p \cong \varprojlim_{n\ge 1} \mathbb{Z}/(p^n)$. Hasonlóan egy R (kommutatív) gyűrű feletti formálos hatványsorok gyűrűje is: $R[[x]] \cong \varprojlim_{n\ge 1} R[x]/(x^n)$.*

2.4. Állítás. *Nemüres, kompakt, Hausdorff A_i $(i \in I)$ halmazok (folytonos összekötő leképezésekkel vett) inverz limesze nemüres, kompakt, és Hausdorff.*

Bizonyítás. Hausdorff terekt direkt szorzata is Hausdorff, ezek részhalmaza is az. Másrészt Tyihonov tétele szerint kompakt halmazok szorzata is kompakt. Belátjuk, hogy ha az eredeti A_i halmazok Hausdorffak, akkor $\varprojlim A_i$ egy zárt része $\prod A_i$-nek, speciálisan kompakt. Valóban, minden $i \le j \in I$ pár esetén a $B_{i,j} := \{(a_i)_{i\in I} \in \prod_{i\in I} A_i \mid f_{ij}(a_j) \ne a_i\}$ halmaz nyílt $\prod A_i$-ben, hiszen A_i Hausdorff, ezért $(a_i)_{i\in I} \in B_{ij}$ esetén a_i-nek és $f_{ij}(a_j)$-nek van egymástól diszjunkt $a_i \in V_i$, $f_{ij}(a_j) \in U_j$ környezetei. Ekkor $V_j := f_{ij}^{-1}(U_j) \subseteq A_j$ is nyílt, tehát $V_i \times V_j \times \prod_{k\in I, i\ne k\ne j} A_j \subseteq B_{ij}$, azaz B_{ij} nyílt. Továbbá ha $\varprojlim A_i$ üres lenne, az azt jelentené, hogy a B_{ij} $(i \le j \in I)$ lefednék a kompakt $\prod A_i$ halmazt, tehát ennek létezne véges részfedése, azaz $i_1 \le j_1, \dots, i_n \le j_n \in I$ n darab pár, melyre $\bigcup_{k=1}^n B_{i_k j_k} = \prod A_i$. Node ennek a $2n$ darab indexnek van egy $t \in I$ közös felső korlátja, és tetszőleges $a_t \in A_t$-re az $a_{i_k} := f_{i_k t}(a_t)$, $a_{j_k} := f_{j_k t}(a_t)$, $a_s \in A_s$ tetszőleges $(s \ne i_1, j_1, \dots, i_n, j_n \in I)$ esetén $(a_i)_{i\in I} \in \prod A_i$ nincs benne egyik $B_{i_k j_k}$-ban sem $(k = 1, \dots, n)$, ami ellentmondás. □

Vegyük észre, hogy a fenti állítás a Kőnig-lemma messzemenő általánosítása, mely – ezen a nyelven – azt mondja ki, hogy véges nemüres halmazok inverz limesze nemüres. Valóban, minden véges halmaz kompakt a diszkrét topológiában, és minden leképezés folytonos két diszkrét tér között.

A direkt limeszhez hasonlóan adott I részbenrendezett halmazra az inverz limesz is funktor: az Abel-csoport inverz rendszereinek kategóriájából az Abel-csoportok kategóriájába.

2.5. Állítás. *Abel-csoportokon az inverz limesz balegzakt, de általában nem jobb egzakt.*

Bizonyítás. Legyen $0 \to A_i \overset{\alpha_i}{\to} B_i \overset{\beta_i}{\to} C_i$ Abel-csoportok inverz rendszerének egy egzakt sorozata (tehát a

$$\begin{tikzcd}
0 \arrow[r] & A_j \arrow[r, "\alpha_j"] \arrow[d, "f_{ij}"'] & B_j \arrow[r, "\beta_j"] \arrow[d, "g_{ij}"'] & C_j \arrow[d, "h_{ij}"] \\
0 \arrow[r] & A_i \arrow[r, "\alpha_i"] & B_i \arrow[r, "\beta_i"] & C_i
\end{tikzcd}$$

diagramok minden $i \leq j \in I$ esetén kommutatívak). Az, hogy $\varprojlim \alpha_i$ injektív, abból következik, hogy a $\prod \alpha_i \colon \prod A_i \to \prod B_i$ leképezés is injektív. A $(\varprojlim \beta_i) \circ (\varprojlim \alpha_i) = \varprojlim(\beta_i \circ \alpha_i) = \varprojlim 0 = 0$, szintén világos. Másrészt, ha $(b_i)_{i \in I} \in \varprojlim B_i \subseteq \prod B_i$ benne van $\mathrm{Ker}(\varprojlim \beta_i)$-ben, akkor minden $i \in I$-re $\beta_i(b_i) = 0$, azaz $b_i \in \mathrm{Ker}(\beta_i) = \mathrm{Im}(\alpha_i)$, így van olyan $a_i \in A_i$, melyre $\alpha_i(a_i) = b_i$. Ráadásul α_i injektív, ezért ez az a_i egyértelmű is, sőt, $\alpha_i(f_{ij}(a_j)) = g_{ij}(\alpha_j(a_j)) = g_{ij}(b_j) = b_i = \alpha_i(a_i)$ és α_i injektivitása miatt $f_{ij}(a_j) = a_i$, azaz $(a_i)_{i \in I}$ benne van $\varprojlim A_i$-ben. $\square$

2.6. Példa. *Az inverz limesz általában nem egzakt: A $0 \to p^n\mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/(p^n) \to 0$ sorozat minden n-re egzakt, és kompatibilis a természetes leképezésekkel, viszont $\varprojlim_n p^n\mathbb{Z} = 0$, $\varprojlim \mathbb{Z} = \mathbb{Z}$, és $\varprojlim \mathbb{Z}/(p^n) = \mathbb{Z}_p$, és a $0 \to 0 \to \mathbb{Z} \to \mathbb{Z}_p \to 0$ sorozat nem egzakt.*

Variációk egy témára:

2.7. Következmény. *Kompakt Hausdorff Abel-csoportokon az inverz limesz egzakt.*

Bizonyítás. Azt kell belátnunk, hogy anélkül, hogy feltennénk, hogy az $\alpha_i \colon A_i \to B_i$ leképezések injektívek, következik az egzaktság $\varprojlim B_i$-nél. A fenti bizonyításban ezt ott használtuk ki, hogy mivel a_i egyértelmű volt, ezért az $(a_i)_{i \in I}$ sorozat szükségképpen kompatibilis az A_i-k közötti összekötőleképezésekkel. Viszont most az A_i-k kompaktak, ezért az $\alpha_i^{-1}(b_i) \subset A_i$ részhalmazok is kompaktak, nemüresek, és Hausdorffak (zárt őse zárt, kompaktnak zárt része kompakt). Ráadásul ezen halmazok is inverz rendszert alkotnak, tehát inverz limeszük nemüres a 2.4-es állítás miatt. Ez pedig azt bizonyítja, hogy a $(b_i)_{i \in I}$ elem benne van $\varprojlim \alpha_i$ képében. $\square$

2.8. Következmény. *Legyen $0 \to A_i \overset{\alpha_i}{\to} B_i \overset{\beta_i}{\to} C_i \to 0$ Abel-csoportok inverz rendszerének egy egzakt sorozata, és tegyük fel, hogy $I = \mathbb{N}$ a szokásos $\leq$ részbenrendezéssel. Tegyük fel, hogy az $(A_i)_{i \in I}$ inverz rendszer teljesíti a Mittag-Leffler feltételt: Minden $i \in \mathbb{N}$-re van olyan $i \leq m = m(i) \in \mathbb{N}$ index, melyre minden $j \geq m$-re $\mathrm{Im}(f_{im}) = \mathrm{Im}(f_{ij})$ (azaz valamilyen indextől kezdve a képterek stabilizálódnak). Ekkor a $0 \to \varprojlim A_i \to \varprojlim B_i \to \varprojlim C_i \to 0$ sorozat is egzakt. Speciálisan ha az $f_{ij} \colon A_j \to A_i$ leképezések minden $i \leq j \in I$-re szürjektívek, akkor a Mittag-Leffler feltétel triviálisan teljesül $m = i$-vel.*

Bizonyítás. Az általános eset bizonyítását az olvasóra hagyjuk. Ha az f_{ij} leképezések szürjektívek, akkor be kell látnunk, hogy a $\varprojlim \beta_i \colon \varprojlim B_i \to \varprojlim C_i$ leképezés szürjektív. Legyen $(c_i)_{i \in I} \in \varprojlim C_i$. Ekkor a $D_i := \beta_i^{-1}(c_i) \subseteq B_i$ halmazok $\mathrm{Ker}(\beta_i) = \mathrm{Im}(\alpha_i)$-szerinti mellékosztályok, melyekre $g_{ij}(D_j) \subseteq D_i$. Belátjuk, hogy itt egyenlőség van, azaz $g_{ij} \colon D_j \to D_i$ is szürjektív. Legyen $d_i \in D_i$, vegyünk egy tetszőleges $d'_j \in D_j$-t. Ekkor $g_{ij}(d'_j) \in D_i$, azaz $d_i - g_{ij}(d'_j) \in \mathrm{Im}(\alpha_i)$. Mivel α_i injektív, ezért egyértelműen létezik egy $a_i \in A_i$, melyre $\alpha_i(a_i) = d_i - g_{ij}(d'_j)$. Másrészt $f_{ij} \colon A_j \to A_i$ szürjektív, azaz van olyan $a_j \in A_j$, melyre $f_{ij}(a_j) = a_i$. Ekkor viszont $d_i = \alpha_i(a_i) + g_{ij}(d'_j) = \alpha_i(f_{ij}(a_j)) + g_{ij}(d'_j) = g_{ij}(\alpha_j(a_j) + d'_j) \in$

$g_{ij}(D_j)$, hiszen $\alpha_j(a_j)+d'_j$ ugyanabban az $\mathrm{Im}(\alpha_j)$-szerinti mellékosztályban van, mint d'_j, azaz D_j-ben van. Tehát rekurzívan meg tudjuk konstruálni a $\varprojlim D_i$ halmaz egy elemét: ha $d_i \in D_i$ már megvan, akkor vesszük egy tetszőleges ősképét D_{i+1}-ben, és így tovább. □

Az alábbi példában megmutatjuk, hogyan lehet a fenti Mittag-Leffler feltételt alkalmazni.

2.9. Feladat. *Igazoljuk, hogy* $\mathbb{Z}[[x]]/(x-p) \cong \mathbb{Z}_p$*.*

Megoldás. Írjuk a $\mathbb{Z}[[x]]$ formális hatványsorgyűrűt $\mathbb{Z}[[x]] \cong \mathbb{Z}[x]/(x^n)$ alakba. Vegyük észre, hogy az $x-p$-vel való szorzás injektív a $\mathbb{Z}[x]/(x^n)$ gyűrűn. Valóban, ha valamely $f(x) \in \mathbb{Z}[x]$-re $f(x)(x-p)$ osztható x^n-nel, akkor $f(x)$ is osztható x^n, mivel x^n-nek és $x-p$-nek nincs közös irreducibilis osztója, és $\mathbb{Z}[x]$-ben igaz a számelmélet alaptétele. Tehát minden $n \geq 1$-re kapunk egy

$$0 \to \mathbb{Z}[x]/(x^n) \overset{(x-p)\cdot}{\to} \mathbb{Z}[x]/(x^n) \to \mathbb{Z}[x]/(x^n, x-p) \to 0$$

rövid egzakt sorozatot. Ráadásul ezek a rövid egzakt sorozatok kompatibilisek a $\mathbb{Z}[x]/(x^{n+1}) \twoheadrightarrow \mathbb{Z}[x]/(x^n)$ természetes szürjektív faktorleképezésekkel, azaz a

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}[x]/(x^{n+1}) \arrow[r, "(x-p)\cdot"] \arrow[d] & \mathbb{Z}[x]/(x^{n+1}) \arrow[r] \arrow[d] & \mathbb{Z}[x]/(x^{n+1}, x-p) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathbb{Z}[x]/(x^n) \arrow[r, "(x-p)\cdot"] & \mathbb{Z}[x]/(x^n) \arrow[r] & \mathbb{Z}[x]/(x^n, x-p) \arrow[r] & 0
\end{tikzcd}$$

diagram kommutatív minden $n \geq 1$-re. Vegyük észre, hogy $\mathbb{Z}[x]/(x^n, x-p) \cong \mathbb{Z}[x]/(p^n, x-p) \cong \mathbb{Z}/(p^n)$, ráadásul a természetes $\mathbb{Z}[x]/(x^{n+1}, x-p) \to \mathbb{Z}[x]/(x^n, x-p)$ faktorleképezés ennél az izomorfizmusnál a $\mathbb{Z}/(p^{n+1}) \to \mathbb{Z}/(p^n)$ természetes faktorleképezést indukálja. Így a 2.8-as Következmény szerint a

$$0 \to \varprojlim \mathbb{Z}[x]/(x^n) \overset{(x-p)\cdot}{\to} \varprojlim \mathbb{Z}[x]/(x^n) \to \varprojlim \mathbb{Z}/(p^n) \to 0$$

sorozat is egzakt, azaz $\mathbb{Z}_p \cong \mathbb{Z}[[x]]/(x-p)$. □

3. Algebrai lezárt létezése, végtelen Galois-bővítések

3.1. Lemma. *Legyenek* $f_1(x), \ldots, f_n(x) \in K[x]$ *nemkonstans polinomok. Ekkor van olyan* $K \leq L$ *véges bővítése* K*-nak, melyben mindegyik* f_i *(*$i = 1, \ldots, n$*) polinomnak van gyöke.*

Bizonyítás. Indukció n szerint. Ha $n = 1$, akkor vesszük f_1-nek egy g_1 irreducibilis osztóját, és az $L_1 := K[x]/(g_1(x))$ testet, melyben g_1-nek és így f_1-nek van gyöke. □

A következő bizonyítás megegyezik Pelikán József Algebra [1] jegyzetében található bizonyítással, de az olvasó kényelmének kedvéért megismételjük.

3.2. Tétel. *Minden* K *testnek izomorfia erejéig egyértelműen létezik algebrai lezártja, azaz olyan* $K \leq \overline{K}$ *test, mely algebrai bővítése* K*-nak és algebrailag zárt.*

Bizonyítás. Létezés: Legyen $S := \{f(x) \in K[x] \mid f \text{ nem konstans }\}$ a K feletti nemkonstans polinomok halmaza, és $R := K[x_f \mid f \in S]$ sokváltozós polinomgyűrű (minden $f \in S$ polinomra veszünk egy-egy x_f változót). Legyen továbbá $I := (f(x_f) \mid f \in S) \lhd R$ az $f(x_f)$ polinomok által generált ideál. Azt állítjuk, hogy $I \neq R$. Valóban, tegyük fel indirekten, hogy $1 \in I$, azaz van olyan $g_1, \dots, g_n \in R$ és $f_1, \dots, f_n \in S$, melyekre

$$1 = g_1 f_1(x_{f_1}) + \cdots + g_n f_n(x_{f_n}) \ . \tag{1}$$

A 3.1-es Lemma szerint van olyan $K \leq L$ véges bővítés és $\alpha_1, \dots, \alpha_n \in L$ elemek, melyekre $f_i(\alpha_i) = 0$ $(i = 1, \dots, n)$. Az (1)-es egyenletbe x_{f_i} helyére α_i-t helyettesítve, a többi változó helyére pedig tetszőleges (pl. 0) számokat írva egy olyan $R \to L$ gyűrűhomomorfizmust kapunk, ami a bal oldalt 1-be, a jobb oldalt pedig 0-ba viszi. Ez ellentmondás, tehát $I \neq R$.

Így van I-t tartalmazó $M \lhd R$ maximális ideál R-ben Krull tétele szerint (itt kihasználjuk a Zorn lemmát). Ekkor $K_1 := R/M$ test. Vegyük észre, hogy K_1-et generálják az $x_f + M \in K_1$ elemek K felett ($f \in S$), hiszen R-et is generálják az x_f elemek. Viszont az $x_f + M$ elemek algebraiak K fölött, hiszen $f(x_f + M) = 0$. Tehát K_1 egy olyan algebrai bővítése K-nak, melyben minden K feletti nemkonstans polinomnak van gyöke. Vegyük észre, hogy K_1 nem feltétlenül algebrailag zárt, hiszen előfordulhat, hogy egyes K_1-beli polinomoknak nincs gyökük K_1-ben, sőt, az is, hogy egy $f \in K[x]$ polinomnak csak egyetlen gyöke van K_1-ben, nem az összes. Viszont K helyett K_1-gyel elismételhetjük a fenti konstrukciót, mellyel kapunk egy $K \leq K_1 \leq K_2$ algebrai bővítést, melyben minden K_1 feletti polinomnak van gyöke. És így tovább, legyen $\overline{K} := \bigcup_{n=1}^{\infty} K_n$ felszálló unió. Ekkor a $\overline{K}$ testnek minden eleme algebrai K felett (hiszen algebrai bővítések egymásutánja is algebrai), továbbá $\overline{K}$ már algebrailag zárt: ha $g(x) \in \overline{K}[x]$ nemkonstans, akkor van olyan $n \geq 1$, melyre g minden együtthatója benne van K_n-ben, azaz g-nek van gyöke $K_{n+1} \subset \overline{K}$-ban.

Egyértelműség: Legyen F egy másik algebrai lezártja K-nak. A Zorn-lemma segítségével megadunk egy $\overline{K} \to F$ izomorfizmust. Legyen $\mathcal{H}$ az (L, φ) rendezett párok halmaza, ahol $K \leq L \leq \overline{K}$ egy közbülső test, $\varphi \colon L \to F$ pedig egy K-homomorfizmus. Értelmezzük $\mathcal{H}$-n a következő részbenrendezést: $(L_1, \varphi_1) \leq (L_2, \varphi_2)$ akkor és csak akkor, ha $L_1 \leq L_2$ résztest és φ_2 megszorítása L_1-re megegyezik φ_1-gyel. $\mathcal{H}$ egy nemüres halmaz, hiszen $K \leq F$, ezért $(K, \iota) \in \mathcal{H}$, ahol $\iota \colon K \to F$ a természetes tartalmazás. Továbbá $\mathcal{H}$ zárt a felszálló unióra, ezért alkalmazható a Zorn lemma: legyen (L_0, φ_0) a $\mathcal{H}$ egy maximális eleme. Tegyük fel először, hogy $L_0 \neq \overline{K}$, azaz van egy $\alpha \in \overline{K}$, melyre $\alpha \notin L_0$. Legyen α minimálpolinomja L_0 felett $m_\alpha(x) \in L_0[x]$. A [2] 1.9-es Állítás szerint φ_0 kiterjesztései $L_0(\alpha)$-ra bijekcióban vannak $\varphi_0(m_\alpha(x))$ F-beli gyökeivel. Mivel F algebrailag zárt, ezért $\varphi_0(m_\alpha)$-nak van gyöke F-ben, tehát létezik egy $\psi \colon L_0(\alpha) \to F$ K-homomorfizmus kiterjesztése φ_0-nak, ami ellentmond (L_0, φ_0) maximalitásának. Tehát $L_0 = \overline{K}$ és $\varphi_0 \colon \overline{K} \to L$ egy K-homomorfizmus, speciálisan injektív. A szürjektivitáshoz legyen $\beta \in F$ tetszőleges. Mivel F/K algebrai, ezért β-nak van egy $m_\beta(x) \in K[x]$ minimálpolinomja K felett, melynek különböző gyökei F-ben $\beta_1 = \beta, \dots, \beta_n$. Ekkor m_β-nak $\overline{K}$-ban is n különböző gyöke van: $\beta'_1, \dots, \beta'_n$ (valóban, a különböző gyökök száma leolvasható a polinomról többszörös deriválással). Node $\beta'_1, \dots, \beta'_n$ mind $\beta_1, \dots, \beta_n$-be mehet csak a φ_0 testhomomorfizmusnál, speciálisan β is benne van φ_0 képében, azaz φ_0 izomorfizmus. □

3.3. Állítás. *Legyen K egy tökéletes test. Ekkor*

$$\overline{K} \cong \varinjlim_{K \leq L \leq \overline{K},\, L/K \text{ véges}} L \cong \varinjlim_{K \leq L \leq \overline{K},\, L/K \text{ véges Galois}} L \ ,$$

ahol az összekötőleképezések és a részbenrendezés a tartalmazás.

Bizonyítás. Ha L_1, L_2 két véges bővítése K-nak $\overline{K}$-ban, akkor L_1-nek és L_2-nek van közös felső korlátja (bővítünk mindkettő generátoraival), tehát a direkt limesznek van értelme. Másrészt, ha $\alpha \in \overline{K}$, akkor van olyan $K \leq L_0 \leq \overline{K}$ véges közbülső test, melyben α benne van, sőt, ha K tökéletes, akkor még Galois-bővítés is van ilyen. Tehát α-hoz hozzárendelhetjük $\alpha \in L_0$ osztályát a $\varinjlim L$ direkt limeszben, mely hozzárendelés egy K-homomorfizmus. Ez a K-homomorfizmus nyilvánvalóan bijektív. □

3.4. Definíció. *Egy F/K végtelen algebrai bővítést Galois-bővítésnek nevezünk, ha szeparábilis és normális. A fenti bizonyítással analóg érvelés miatt ez azzal ekvivalens, hogy F véges Galois-bővítések direkt limesze.*

3.5. Állítás. *Ha F/K Galois-bővítés, akkor*

$$\mathrm{Gal}(F/K) := \mathrm{Hom}_K(F, F) \cong \varprojlim_{K \leq L \leq F, L/K \text{ véges Galois}} \mathrm{Gal}(L/K) \ ,$$

ahol a jobb oldalon $K \leq L_1 \leq L_2$ véges Galois bővítések esetén a $\mathrm{Gal}(L_2/K) \to \mathrm{Gal}(L_1/K)$ összekötő leképezések a megszorítás által indukált faktorleképezések.

Bizonyítás. Ha $\tau \in \mathrm{Hom}_K(F, F)$, akkor τ nyilván injektív, és a 3.2-es Tétel bizonyításának végéhez hasonló gondolatmenet miatt szürjektív is, azaz invertálható. Tehát $\mathrm{Gal}(F/K)$ egy csoport. Továbbá ha $\tau \in \mathrm{Hom}_K(F, F)$, akkor τ-t megszoríthatjuk minden L véges Galois közbülső testre, így a $\tau \mapsto (\tau_L)_L$ egy $\mathrm{Gal}(F/K) \to \varprojlim \mathrm{Gal}(L/K)$ csoporthomomorfizmus lesz, hiszen $(\tau_{L_2})_{L_1} = \tau_{L_1}$. Az injektivitás világos, hiszen ha $\tau \neq \mathrm{id}$, akkor van olyan $\alpha \in F$, melyre $\tau(\alpha) \neq \alpha$, de α benne van egy véges bővítésben is. A szürjektivitás szintén világos, hiszen ha van τ_L-eknek egy kompatibilis rendszere, akkor ez megad egy $\tau \colon F \to F$ K-homomorfizmust a következőképpen: ha $\alpha \in F$, akkor van olyan L véges bővítés, mely tartalmazza α-t. Ekkor $\tau(\alpha) := \tau_L(\alpha)$ legyen, és ez nyilván nem függ L választásától, mivel $(\tau_L)_L$ kompatibilis volt. □

3.6. Definíció. *A K tökéletes test abszolút Galois-csoportján a* $\mathrm{Gal}(\overline{K}/K)$ *csoportot értjük. Ezen értelmezhető az inverz limesz topológia (a* $\mathrm{Gal}(L/K)$ *véges csoportokon a diszkrét topológiát választva), melyre nézve egy kompakt csoport, hiszen véges (spec. kompakt) csoportok inverz limesze. Véges csoportok inverz limeszeit* provéges *csoportoknak nevezzük. Ha K nem tökéletes, akkor $\overline{K}$ nem Galois-bővítése K-nak. Ebben az esetben $\overline{K}$ helyett K maximális szeparábilis K^{sep} bővítését („szeparábilis lezárt") kell venni az abszolút Galois csoport definíciójában.*

Híres megoldatlan probléma az inverz Galois-probléma, mely ebben a kontextusban azzal ekvivalens, hogy minden véges csoport előáll-e a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ csoport folytonos homomorf képeként, azaz $\mathbb{Q}$ véges bővítésének Galois-csoportjaként.

Hivatkozások

[1] Pelikán József, *Algebra*, `http://www.cs.elte.hu/~pelikan/11_Testek.pdf`

[2] Zábrádi Gergely, K-homomorfizmusok, szeparábilis bővítések, Galois-elmélet, `http://www.cs.elte.hu/~zger/Algebra4_2013/szeparabilis.pdf`