Testek

1. Alapfogalmak

2. Faktortest

3. Testbővítések

1. Alapfogalmak

2. Faktortest

3. Testbővítések

[Sz] V/3, XIII/1,2; [F] III/1-7 (+ előismeretek!)

Definíció

Ha egy nemüres halmazon kettő kétváltozós művelet is értelmezve van (nevezzük az egyiket összeadásnak, a másikat szorzásnak) úgy, hogy az alaphalmaz az összeadás műveletével kommutatív csoportot, a szorzás műveletével pedig félcsoportot alkot, és a szorzás disztributív az összeadásra, akkor ezt a kétműveletes struktúrát **gyűrűnek** nevezzük.
Formálisan: $(R; +, \cdot)$ gyűrű, ha R nemüres halmaz, és

(1) $(R; +)$ Abel-csoport;

(2) $(R; \cdot)$ félcsoport;

(3) $\forall a, b, c \in R : a \cdot (b + c) = a \cdot b + a \cdot c$ és $(b + c) \cdot a = b \cdot a + c \cdot a$.

Definíció

Az $(R; +)$ csoportot az $(R; +, \cdot)$ gyűrű **additív csoportjának** nevezzük, és ennek megfelelően beszélhetünk **additív egységelemről** és **additív inverzről** is.
Az $(R; \cdot)$ félcsoportot neve: a gyűrű **multiplikatív félcsoportja**.

Tetszőleges gyűrűben 0 jelöli az additív egységelemet, az a gyűrűelem additív inverzét pedig $-a$ jelöli, és értelmezhetjük a kivonás műveletét a $b - a = b + (-a)$ képlettel.

Állítás

Ha $(R; +, \cdot)$ gyűrű, akkor minden $a \in R$ esetén $a \cdot 0 = 0 \cdot a = 0$ teljesül.

Megjegyzés

Sok hasonló, az egész számokkal végzett műveleteknél megszokott tulajdonság érvényes tetszőleges gyűrűben, például

$$a\,(b - c) = ab - ac, \qquad -\,(ab) = (-a)\,b = a\,(-b)\,.$$

De vigyázat: a szorzás általában nem kommutatív, így például
$(a + b)\,(a - b) = a^2 - b^2$ vagy $(a + b)^2 = a^2 + 2ab + b^2$
már *nem* teljesül minden gyűrűben!

Definíció

Ha egy gyűrűben nemcsak az összeadás, hanem a szorzás is kommutatív, akkor **kommutatív gyűrűnek** nevezzük. Ha pedig nemcsak additív, de **multiplikatív egységelem** is létezik (amelyet általában 1 jelöl), akkor **egységelemes gyűrűről** beszélünk.

Definíció

Ha egy gyűrű a, b elemeire $ab = 0$ teljesül, de se a, se b nem nulla, akkor azt mondjuk, hogy a és b **zérusosztók**. Ha egy gyűrűben nincsenek zérusosztók (azaz nullától különböző elemek szorzata sosem nulla), akkor **zérusosztómentes gyűrűnek** nevezzük. A kommutatív, egységelemes, zérusosztómentes gyűrű neve **integritástartomány**.

Állítás

Integritástartományban lehet nemzéró elemmel egyszerűsíteni, azaz tetszőleges $a, b, c \ \ (c \neq 0)$ *elemekre*

$$ac = bc \implies a = b.$$

Definíció

Legyen R egységelemes gyűrű. Az $a \in R$ elemet **egységnek** nevezzük, ha létezik **multiplikatív inverze**, azaz létezik olyan $a^{-1} \in R$ elem, amelyre $aa^{-1} = a^{-1}a = 1$ teljesül.

Tétel

Az egységek bármely egységelemes gyűrűben csoportot alkotnak a szorzás műveletére nézve.

Definíció

Az R gyűrű egységeinek multiplikatív csoportját R **egységcsoportjának** nevezzük és R^*-gal jelöljük.

Definíció

Testnek nevezünk egy integritástartományt, ha legalább kételemű, és minden nemnulla elemének van multiplikatív inverze.

Definíció

Ha T test, akkor $(T \setminus \{0\}; \cdot)$ Abel-csoport, amelyet a T test **multiplikatív csoportjának** hívjuk.

Megjegyzés

A definíció alapján világos, hogy egy legalább kételemű R kommutatív egységelemes gyűrű akkor és csak akkor test, ha egységcsoportja a nulla kivételével minden elemet tartalmaz, azaz $R^* = R \setminus \{0\}$.

Mivel gyűrűben és testben a két műveletet általában $+$ és $\cdot$ jelöli, ezeket nem írjuk mindig ki, tehát $(R; +, \cdot)$ illetve $(T; +, \cdot)$ helyett egyszerűen csak R gyűrűről, illetve T testről beszélünk.

Példa

- $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$: test
- $\mathbb{Z}$: integritástartomány, egységcsoportja: $\{1, -1\}$
- $\mathbb{R}^+$, $\mathbb{Q}^+$, $\mathbb{N}$: nem is gyűrű
- $\{$páros számok$\}$:
  kommutatív, zérusosztómentes gyűrű (nem egységelemes)
- $\{$páratlan számok$\}$: nem is gyűrű
- $\{$irracionális számok$\}$: nem is gyűrű
- $\{$véges tizedestörtek$\}$: integritástartomány (mi az egységcsoportja?)
- $\mathbb{Z}_{12}$: kommutatív, egységelemes gyűrű (nem zérusosztómentes)
- $\mathbb{Z}_{13}$: test
- $\mathbb{R}^{n\times n}$: egységelemes gyűrű (nem kommutatív és nem zérusosztómentes), egységcsoportja: $\mathrm{GL}_n(\mathbb{R})$

Definíció

Legyen R egy gyűrű és $S \subseteq R$. Ha S az R-ből „örökölt” műveletekkel maga is gyűrű, akkor azt mondjuk, hogy S **részgyűrűje** az R gyűrűnek. Hasonlóan definiálható a **résztest** fogalma is.

Állítás

Tetszőleges R gyűrű és $\emptyset \neq S \subseteq R$ esetén S akkor és csak akkor részgyűrűje R-nek, ha

- *S zárt az összeadásra:* $\forall a, b \in S : \ a + b \in S$;
- *S zárt a kivonásra:* $\forall a, b \in S : \ a - b = a + (-b) \in S$;
- *S zárt a szorzásra:* $\forall a, b \in S : \ a \cdot b \in S$.

Állítás

Tetszőleges T test és $\emptyset \neq S \subseteq T$ esetén S akkor és csak akkor részteste T-nek, ha

- *S zárt az összeadásra:* $\forall a, b \in S : \ a + b \in S$;
- *S zárt a kivonásra:* $\forall a, b \in S : \ a - b = a + (-b) \in S$;
- *S zárt a szorzásra:* $\forall a, b \in S : \ a \cdot b \in S$;
- *S zárt az osztásra:* $\forall a, b \in S : \ a/b = a \cdot b^{-1} \in S$, *ha* $b \neq 0$.

Tétel

Részgyűrűk metszete is részgyűrű, résztestek metszete is résztest.

Definíció

Legyen R egy gyűrű, és $B \subseteq R$. A B halmaz által **generált részgyűrű** a legszűkebb olyan részgyűrű, ami tartalmazza B-t:

$$[B]_{\text{gy}} = \bigcap_{B \subseteq S \leq R} S.$$

Megjegyzés

Az üres halmaz generátuma a legszűkebb részgyűrű: $[\emptyset]_{\text{gy}} = \{0\}$.

Definíció

Ha $[B]_{\text{gy}} = R$, akkor azt mondjuk, hogy B **generátorrendszere** az R gyűrűnek.

Megjegyzés

Hasonló módon definiálható a **generált résztest**, illetve test generátorrendszerének fogalma is. A legszűkebb résztest: $[\emptyset]_{\text{t}} = [0,1]_{\text{t}} = [1]_{\text{t}} =?$ (Később visszatérünk rá.)

Állítás

Az R gyűrűben a $B \subseteq R$ részhalmaz által generált részgyűrű azokból az elemekből áll, amelyek megkaphatók $B \cup \{0\}$ elemeiből az első három alapművelet segítségével.

Állítás

A T testben a $B \subseteq T$ részhalmaz által generált résztest azokból az elemekből áll, amelyek megkaphatók $B \cup \{0, 1\}$ elemeiből az első négy alapművelet segítségével.

Példa

Határozzuk meg a komplex számok testében a megadott részhalmaz által generált részgyűrűt, illetve résztestet.

- $[\emptyset]_{\text{gy}} = [0]_{\text{gy}} = \{0\}$
- $[\emptyset]_{\text{t}} = [0, 1]_{\text{t}} = [1]_{\text{t}} = \mathbb{Q}$
- $[1]_{\text{gy}} = \mathbb{Z}$
- $[i]_{\text{gy}} = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$
- $[i]_{\text{t}} = \mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$

Példa (folyt.)

- $\left[\mathbb{Z} \cup \left\{\sqrt{2}\right\}\right]_{\text{gy}} = \mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \colon a, b \in \mathbb{Z}\right\}$
- $\left[\mathbb{Q} \cup \left\{\sqrt{2}\right\}\right]_{\text{t}} = \mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} \colon a, b \in \mathbb{Q}\right\}$
- $\left[\mathbb{Z} \cup \left\{\sqrt[3]{2}\right\}\right]_{\text{gy}} = \mathbb{Z}\left[\sqrt[3]{2}\right] = \left\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \colon a, b \in \mathbb{Z}\right\}$
- $\left[\mathbb{Q} \cup \left\{\sqrt[3]{2}\right\}\right]_{\text{t}} = \mathbb{Q}\left(\sqrt[3]{2}\right) = \left\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \colon a, b \in \mathbb{Q}\right\}$
- $\left[\mathbb{Z} \cup \{\pi\}\right]_{\text{gy}} = \mathbb{Z}[\pi] = \{f(\pi) : f \in \mathbb{Z}[x]\}$
- $\left[\mathbb{Q} \cup \{\pi\}\right]_{\text{t}} = \mathbb{Q}(\pi) = \{t(\pi) : t \in \mathbb{Q}(x)\} =$

$$= \left\{\frac{f(\pi)}{g(\pi)} \colon f, g \in \mathbb{Z}[x], g(\pi) \neq 0\right\}$$

Definíció

Az $a \in R$ elem $S \leq R$ részgyűrű szerinti **mellékosztályán** az $a + S = \{a + s : s \in S\}$ halmazt értjük.

Megjegyzés

Az a és b elemek akkor és csak akkor esnek ugyanabba az S szerinti mellékosztályba, ha $a - b \in S$.

Definíció

Az $I \leq R$ részgyűrűt **ideálnak** nevezzük (jelölés: $I \lhd R$), ha rendelkezik a szívó tulajdonsággal:

$$\forall a \in I \ \forall r \in R : \ ar \in I \text{ és } ra \in I.$$

Példa

Legyen R integritástartomány és $m \in R$. Ekkor az

$$(m) := \{mr : r \in R\} = \{a \in R : m \mid a\}$$

halmaz ideál, amelyet az m elem által generált **főideálnak** nevezünk.
A megfelelő mellékosztályozás éppen a modulo m kongruencia:

$$a+(m) = b+(m) \iff a-b \in (m) \iff m \mid a-b \iff a \equiv b \pmod{m}.$$

Tétel

Ha $I \triangleleft R$, akkor az I szerinti mellékosztályozás kompatibilis osztályozása R-nek. A megfelelő faktoralgebra gyűrű, melyet az R gyűrű I ideál szerinti **faktorgyűrűjének** *nevezünk és R/I -vel jelöljük.*
A faktorgyűrűbeli műveleteket a következőképpen végezzük:

$$(a+I)+(b+I)=(a+b)+I \qquad (a+I)\cdot(b+I)=(a\cdot b)+I.$$

Biz.

[F] III. fejezet, 3.8. és 3.9. Tétel.

Mivel az R-beli összeadás kommutatív, $(I;+)$ normálosztó $(R;+)$-ban, így az I szerinti mellékosztályozás kompatibilis az összeadással.
A szorzással való kompatibilitás a szívó tulajdonságon (és a disztributivitáson) múlik:

$$(a+I)\cdot(b+I) = a\cdot b + a\cdot I + I\cdot b + I\cdot I \subseteq a\cdot b + I + I + I = a\cdot b + I.$$

□

Tétel

Ha $\sim$ kongruenciája az R gyűrűnek, akkor $I := \{a \in R : a \sim 0\} \triangleleft R$, és a $\sim$ kongruenciához tartozó kompatibilis osztályozás nem más, mint az I ideál szerinti mellékosztályozás.

Biz.

[F] III. fejezet, 3.8. Tétel. □

Példa

Ha $I = (m)$, akkor $R/(m)$ az R gyűrű modulo m **maradékosztály-gyűrűje**.

Definíció

Ha az R integritástartományban minden ideál főideál, akkor azt mondjuk, hogy R **főideálgyűrű**.

Példa

Az egész számok gyűrűje, a test feletti polinomgyűrűk (és általában minden euklideszi gyűrű) főideálgyűrű, de például $\mathbb{Z}[x]$ nem főideálgyűrű, mert $\{f \in \mathbb{Z}[x] : f(0) \text{ páros}\} \triangleleft \mathbb{Z}[x]$ de nem főideál (HF).

Definíció

Legyen R és S két gyűrű, és $\varphi\colon R \to S$ egy leképezés. Azt mondjuk, hogy φ **gyűrűhomomorfizmus**, ha felcserélhető az összeadással és a szorzással is, azaz

$$\forall a, b \in R: \quad (a_1 + a_2)\,\varphi \;=\; a_1\varphi + a_2\varphi;$$
$$\forall a, b \in R: \quad (a_1 \cdot a_2)\,\varphi \;=\; a_1\varphi \cdot a_2\varphi.$$

Definíció

Legyen I ideálja az R gyűrűnek. Ekkor a

$$\nu\colon R \to R/I,\ \ a \mapsto a + I$$

leképezés szürjektív homomorfizmus (HF), amelyet az I ideálhoz tartozó **természetes homomorfizmusnak** nevezünk.

A természetes homomorfizmus mutatja, hogy minden faktorgyűrű előáll homomorf képként. Ennek a fordítottja is igaz: minden homomorf kép faktorgyűrű (legalábbis izomorfia erejéig).

Definíció

A $\varphi\colon R \to S$ gyűrűhomomorfizmus **magja** :

$$\ker \varphi := \{a \in R\colon a\varphi = 0\}.$$

Tétel (Gyűrűelméleti homomorfiatétel)

Ha $\varphi\colon R \to S$ *gyűrűhomomorfizmus, akkor* $\ker \varphi \lhd R$ *és*

$$R/\ker \varphi \cong R\varphi \leq S.$$

Tétel (I. izomorfiatétel)

Ha $S \leq R$ *és* $I \lhd R$*, akkor* $I \lhd S + I \leq R$ *és* $S \cap I \lhd S \leq R$*, továbbá*

$$(S + I)/I \cong S/S\cap I.$$

Tétel (Megfeleltetési tétel)

Ha $I \triangleleft R$, akkor R/I részgyűrűi kölcsönösen egyértelműen megfelelnek az R gyűrű I-t tartalmazó részgyűrűinek.
A $J \leq R$ részgyűrűnek (ahol $I \leq J$) az $F := J/I \leq R/I$ részgyűrű felel meg.

Tétel (II. izomorfiatétel)

Ha $J \leq R$ és $F \leq R/I$ a fentiek szerint egymásnak megfelelő részgyűrűk, akkor $J \triangleleft R \iff F \triangleleft R/I$. Ha ez teljesül, akkor $(R/I)/F \cong R/J$, azaz

$$(R/I)/(J/I) \cong R/J.$$

Definíció

Az A és B gyűrűk **direkt szorzatán** azt a gyűrűt értjük, melynek tartóhalmaza $A \times B$, műveletei pedig a következőképpen vannak definiálva:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2) \quad \text{és}$$
$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2)\,.$$

Tétel

Ha n és m relatív prímek, akkor $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$.

Biz.

[Sz] X/4.5. Tétel. □

Következmény

Ha n és m relatív prímek, akkor $\mathbb{Z}_n^* \times \mathbb{Z}_m^* \cong \mathbb{Z}_{nm}^*$.

Biz.

Világos (?), hogy izomorf gyűrűk egységcsoportjai is izomorfak. Tehát

$$\mathbb{Z}_{nm}^* \cong (\mathbb{Z}_n \times \mathbb{Z}_m)^* \overset{!}{=} \mathbb{Z}_n^* \times \mathbb{Z}_m^*.$$ □

1. Alapfogalmak

2. Faktortest

3. Testbővítések

[Sz] XIII/2; [F] VI/4 (+ előismeretek!)

Tétel

Bármely legalább kételemű kommutatív egységelemes R gyűrű esetén az alábbiak ekvivalensek:

(1) R **egyszerű** *gyűrű (azaz csak két ideálja van:* $\{0\}$ *és* R*);*

(2) R *test.*

Biz.

R egyszerű $\implies$ R test:

Csak azt kell belátni, hogy R minden nemnulla elemének van multiplikatív inverze. Tetszőleges $a \in R \setminus \{0\}$ esetén $\{0\} \neq (a) \triangleleft R$, ezért R egyszerűsége miatt $(a) = R$. Ebből következik, hogy $1 \in (a)$, azaz $\exists b \in R : ab = 1$.

R test $\implies$ R egyszerű:

Legyen $\{0\} \neq I \triangleleft R$ és $0 \neq a \in I$. A szívó tulajdonság miatt minden $r \in R$ esetén $r = \left(ra^{-1}\right) a \in I$, tehát $I = R$. $\square$

Következmény

Legyen R kommutatív egységelemes gyűrű és $I \triangleleft R$. Ekkor az alábbiak ekvivalensek.

(1) *I* **maximális ideál** *(azaz $\nexists J \triangleleft R : I \subset J \subset R$).*

(2) *Az R/I faktorgyűrű test.*

Biz.

A megfeleltetési tétel szerint I pontosan akkor maximális ideál, ha R/I legalább kételemű egyszerű gyűrű, vagyis – az előző tétel szerint – test. □

Következmény

Legyen R főideálgyűrű de nem test, és legyen $m \in R$. Ekkor az alábbiak ekvivalensek:

(1) *Az $m \in R$ elem irreducibilis.*

(2) *Az $R/(m)$ faktorgyűrű test.*

Biz.

Az oszthatóság és az asszociáltság szoros kapcsolatban van a főideálokkal:

$$\forall a, b \in R: \quad a \mid b \quad \Longleftrightarrow \quad (a) \supseteq (b)$$

$$\forall a, b \in R: \quad a \sim b \quad \Longleftrightarrow \quad (a) = (b)$$

Emiatt m valódi osztói megfelelnek az (m) „fölötti” (fő)ideáloknak.

Következésképp az (m) ideál akkor és csak akkor maximális, ha m-nek asszociáltság erejéig pontosan két osztója van: 1 és maga m.

Ezek éppen az irreducibilis elemek, kivéve ha $m = 0$ és R test (miért)? □

Következmény

$\mathbb{Z}_m$ *test* $\iff$ m *prímszám*

- elemek: $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$
- számolás:
  - összeadás, additív inverz (kivonás), szorzás: egyszerű, csak modulo p kell számolni
  - multiplikatív inverz (osztás): lineáris kongruenciát vagy diofantoszi egyenletet kell megoldani (ha másképp nem megy, akkor euklideszi algoritmussal)

Példa

Számoljunk $\mathbb{Z}_{17}$-ben.

$$\begin{aligned}
\overline{12} + \overline{13} &= \overline{25} = \overline{8} \\
-\overline{12} &= \overline{-12} = \overline{5} \\
\overline{12} \cdot \overline{13} &= \overline{156} = \overline{3} \\
\overline{12}^{-1} &= \overline{u} \iff \overline{12} \cdot \overline{u} = \overline{1} \\
&\iff 12u \equiv 1 \pmod{17} \\
&\iff \exists v \in \mathbb{Z} : 12u = 1 + 17v \\
&\iff u \equiv 10 \pmod{17} \\
&\iff \overline{u} = \overline{10}
\end{aligned}$$

Következmény

Tetszőleges T test és n-edfokú $f \in T[x]$ esetén

$$T[x]/(f) \text{ test} \iff f \text{ irreducibilis } T \text{ felett.}$$

- elemek: $T[x]/(f) = \{\overline{g} : g \in T[x],\ \deg g \leq n-1\} =$
$$= \left\{\overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} : a_0, a_1, \ldots, a_{n-1} \in T\right\}$$
- számolás:
  - összeadás, additív inverz (kivonás), szorzás: egyszerű, csak modulo f kell számolni
  - multiplikatív inverz (osztás): lineáris kongruenciát vagy „diofantoszi" egyenletet kell megoldani (ha másképp nem megy, akkor euklideszi algoritmussal)

Következmény

Ha $f \in \mathbb{Z}_p[x]$ egy n-edfokú irreducibilis polinom, akkor $\mathbb{Z}_p[x]/(f)$ egy p^n elemszámú test.

Megjegyzés

Meg lehet mutatni, hogy minden p prímszám és n természetes szám esetén létezik n-edfokú irreducibilis polinom $\mathbb{Z}_p$ felett. Következésképp minden q prímhatványra létezik q-elemű test.

Példa

Melyek testek az alábbi faktorgyűrűk közül?

- $\mathbb{Z}_2[x]/(x^2+1)$: nem,
  mert $x^2+1=(x+1)^2$.
- $\mathbb{Z}_3[x]/(x^2+1)$: igen,
  mert x^2+1 csak másodfokú, és nincs gyöke $\mathbb{Z}_3$-ban.
- $\mathbb{Z}_2[x]/(x^2+x+1)$: igen,
  mert x^2+x+1 csak másodfokú, és nincs gyöke $\mathbb{Z}_2$-ben.
- $\mathbb{Z}_2[x]/(x^3+x+1)$: igen,
  mert x^3+x+1 csak harmadfokú, és nincs gyöke $\mathbb{Z}_2$-ben.
- $\mathbb{Z}_2[x]/(x^4+x^2+1)$: nem,
  mert $x^4+x^2+1=(x^2+x+1)^2$.
- $\mathbb{R}[x]/(x^2+1)$: igen,
  mert x^2+1 csak másodfokú, és nincs valós gyöke.
- $\mathbb{C}[x]/(x^2+1)$: nem,
  mert $x^2+1=(x-i)(x+i)$.
- $\mathbb{Q}[x]/(x^4+4x^3+6x^2+8x+10)$: igen,
  mert $x^4+4x^3+6x^2+8x+10$ irreducibilis $\mathbb{Q}$ felett (miért?).

Példa

Határozzuk meg a $K = \mathbb{Q}[x] / \left(x^3 - 7\right)$ testben a $\overline{2 - x}$ elem multiplikatív inverzét.

K elemei $\overline{ax^2 + bx + c}$ $(a, b, c \in \mathbb{Q})$ alakúak, ilyen alakban szeretnénk az $\overline{u} = \overline{2 - x}^{-1}$ elemet is megkapni.

$$
\begin{aligned}
\overline{2 - x}^{-1} = \overline{u} &\iff \overline{2 - x} \cdot \overline{u} = \overline{1} \\
&\iff (2 - x)\, u \equiv 1 \pmod{x^3 - 7} \\
&\iff \exists v \in \mathbb{Q}[x] : (2 - x)\, u = 1 + \left(x^3 - 7\right) v \\
&\iff u \equiv x^2 + 2x + 4 \pmod{x^3 - 7} \\
&\iff \overline{u} = \overline{x^2 + 2x + 4}
\end{aligned}
$$

Tehát $\overline{2 - x}^{-1} = \overline{x^2 + 2x + 4}$.

Példa

Számoljunk a $\mathbb{Z}_2[x]/\left(x^2+x+1\right)$ négyelemű testben.

$$\mathbb{Z}_2[x]/\left(x^2+x+1\right) = \left\{\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1}\right\}$$

$$\overline{x+1}+\overline{1} = \overline{x}$$

$$-\overline{x+1} = \overline{x+1}$$

$$\overline{x+1}\cdot\overline{x+1} = \overline{x^2+1} = \overline{x}$$

$$\overline{x+1}^{-1} = \overline{u} \iff \overline{x+1}\cdot\overline{u} = \overline{1}$$

$$\iff (x+1)\,u \equiv 1 \pmod{x^2+x+1}$$

$$\iff \exists v \in \mathbb{Z}_2[x] : (x+1)\,u = 1 + \left(x^2+x+1\right)v$$

$$\iff u \equiv x \pmod{x^2+x+1}$$

$$\iff \overline{u} = \overline{x}$$

A négyelemű $K := \mathbb{Z}_2[x] / \left(x^2 + x + 1\right)$ test művelettáblázatai:

$+$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{x+1}$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{x+1}$	$\overline{0}$	$\overline{1}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{x}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{x+1}$	$\overline{1}$
$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{1}$	$\overline{x}$

Ugyanez tömörebben, a $0 := \overline{0}$, $1 := \overline{1}$, $\alpha := \overline{x}$, $\beta := \overline{x+1}$ jelöléssel:

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Figyeljük meg, hogy

- $\{0, 1\} = \left\{\overline{0}, \overline{1}\right\}$ egy $\mathbb{Z}_2$-vel izomorf résztestet alkot K-ban;
- $\alpha = \overline{x}$ gyöke az $x^2 + x + 1 \in K[x]$ polinomnak:
  $f(\alpha) = \alpha^2 + \alpha + 1 = \overline{x}^2 + \overline{x} + \overline{1} = \overline{x^2 + x + 1} = \overline{0} = 0$.

Példa

Számoljunk az $\mathbb{R}[x]/(x^2+1)$ testben

- elemek: $\overline{a+bx}$ $(a,b\in\mathbb{R})$
- összeadás: $\overline{a+bx}+\overline{c+dx}=\overline{(a+c)+(b+d)x}$
- szorzás:

$$\overline{a+bx}\cdot\overline{c+dx}=\overline{ac+(ad+bc)x+bdx^2}=\overline{(ac-bd)+(ad+bc)x}$$

Használjuk az $a:=\overline{a}\,(a\in\mathbb{R})$ és $\alpha:=\overline{x}$ rövidítéseket:

- elemek: $a+b\alpha$ $(a,b\in\mathbb{R})$
- számolási szabály: $\alpha^2+1=\overline{x}^2+\overline{1}=\overline{x^2+1}=\overline{0}=0$, azaz $\alpha^2=-1$
- összeadás: $(a+b\alpha)+(c+d\alpha)=(a+c)+(b+d)\alpha$
- szorzás: $(a+b\alpha)\cdot(c+d\alpha)=(ac-bd)+(ad+bc)\alpha$

Ha α helyett az i betűt használjuk, akkor világos, hogy

$$\mathbb{R}[x]/(x^2+1)\cong\mathbb{C}.$$

Tétel

Ha $f \in T[x]$ irreducibilis polinom, akkor a $K := T[x]/(f)$ faktortestben

$$T_1 := \{\overline{a} \colon a \in T\}$$

egy T-vel izomorf résztestet alkot, továbbá $\alpha := \overline{x} \in K$ gyöke az $f \in K[x]$ polinomnak.

Biz.

Az alábbi leképezés izomorfizmus T és T_1 között:

$$\varphi \colon T \to T_1 \leq K, \ a \mapsto \overline{a}.$$

Általában nem is különböztetjük meg az $\overline{a}$ és a ($a \in T$) elemeket egymástól, így T részteste lesz K-nak.

Ezzel az $f = a_n x^n + \cdots + a_1 x + a_0 \in T[x]$ polinomot is azonosítottuk az

$$\overline{a_n} x^n + \cdots + \overline{a_1} x + \overline{a_0} \in T_1[x] \leq K[x] \text{ polinommal.}$$

Így már van értelme kiszámítani $f(\alpha)$ értékét:

$$\begin{aligned} f(\alpha) = a_n \cdot \alpha^n + \cdots + a_1 \cdot \alpha + a_0 &= \overline{a_n} \cdot \overline{x}^n + \cdots + \overline{a_1} \cdot \overline{x} + \overline{a_0} \\ &= \overline{a_n x^n + \cdots + a_1 x + a_0} \\ &= \overline{f} = \overline{0} = 0. \end{aligned}$$

□

Megjegyzés

- Az előbbi konstrukcióval bármely $f \in T[x]$ polinomnak lehet „gyököt csinálni” az alaptest egy megfelelő K kibővítésében. (Ha f nem irreducibilis, akkor dolgozzunk egy irreducibilis osztójával.)
- Az eljárást ismételve olyan test is konstruálható, amelyben már f-nek annyi gyöke van, amennyi a fokszáma, azaz f elsőfokú polinomok (gyöktényezők) szorzatára bomlik (f felbontási teste).
- Transzfinit indukcióval igazolható olyan $\overline{T}$ test létezése is, amelyben már nem csak egy kiválasztott $f \in T[x]$ polinom bomlik lineáris tényezők szorzatára, hanem minden T feletti polinom (a $\overline{T}$ testet a T test algebrai lezártjának nevezzük).
- Az algebra alaptétele szerint a komplex számok teste algebrailag zárt ($\overline{\mathbb{C}} = \mathbb{C}$), ez a valós számtest algebrai lezártja is ($\overline{\mathbb{R}} = \mathbb{C}$).
- A racionális számtest algebrai lezártja az algebrai számok teste.

1. Alapfogalmak

2. Faktortest

3. Testbővítések

[F] VI/1-5

Definíció

- Az L testet a K test **bővítésének** nevezzük, ha K részteste L-nek. Jelölés: $L \mid K$.
- Ha létezik véges sok $\alpha_1, \ldots, \alpha_k$ elem úgy, hogy L megegyezik a $K \cup \{\alpha_1, \ldots, \alpha_k\}$ halmaz által generált testtel, akkor azt mondjuk, hogy az $L \mid K$ bővítés **végesen generált**.
  Jelölés: $L = K(\alpha_1, \ldots, \alpha_n)$.
- Ha létezik $\alpha \in L$ úgy, hogy $L = K(\alpha)$, akkor azt mondjuk, hogy $L \mid K$ **egyszerű bővítés**.
- Az $L_1 \mid K$ és $L_2 \mid K$ testbővítések közötti **izomorfizmuson** olyan $\varphi\colon L_1 \to L_2$ leképezést értünk, amelyre
  - $\varphi\colon L_1 \to L_2$ testizomorfizmus
  - $\varphi|_K = \mathrm{id}_K$, azaz minden $a \in K$ esetén $a\varphi = a$.

Állítás

Ha $L \mid K$ testbővítés, akkor L vektorteret alkot K felett.

Biz.

Az L test műveletei adják a ${}_K L$ vektortér műveleteit:

- az $\alpha, \beta \in L$ vektorok összege: $\alpha + \beta \in L$;
- az $\alpha \in L$ vektornak a $c \in K$ skalárral való szorzata: $c\alpha \in L$.

Könnyű ellenőrizni, hogy a testaxiómákból következnek a vektortér-axiómák (HF). □

Definíció

Az ${}_K L$ vektortér dimenzióját az $L \mid K$ testbővítés **fokszámának** nevezzük. Jelölés: $[L : K] := \dim_K L$.

Példa

- $[\mathbb{C} : \mathbb{R}] = 2$; egy bázis: $1, i$
- $\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2$; egy bázis: $1, \sqrt{2}$
- $[\mathbb{R} : \mathbb{Q}] = \infty$; egy lineárisan független rendszer: $1, \pi, \pi^2, \pi^3, \ldots$

Tétel (fokszámtétel)

Bármely $K \leq L \leq M$ *testtoronyra* $[M : K] = [M : L] \cdot [L : K]$.

Biz. (csak véges fokszámokra).

Legyen $\alpha_1, \ldots, \alpha_n$ bázisa az ${}_K L$ vektortérnek és $\beta_1, \ldots, \beta_m$ bázisa az ${}_L M$ vektortérnek. Ekkor $\alpha_i \beta_j$ $(i = 1, \ldots, n; j = 1, \ldots, m)$ bázisa az ${}_K M$ vektortérnek. (HF [F] VI/1.) □

Példa

Legyen $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$, $M = L(i) = \mathbb{Q}(\sqrt{2}, i)$.

Az ${}_K L$ vektortér egy bázisa: $\alpha_1 = 1,\ \alpha_2 = \sqrt{2}$. (világos)

Az ${}_L M$ vektortér egy bázisa: $\beta_1 = 1,\ \beta_2 = i$. (majd később világos lesz)

Az ${}_K M$ vektortér egy bázisa:

$$\alpha_1\beta_1 = 1,\ \alpha_2\beta_1 = \sqrt{2},\ \alpha_1\beta_2 = i,\ \alpha_2\beta_2 = \sqrt{2}i.$$

Az ${}_K M$ vektortér egy tetszőleges elemének felírása ebben a bázisban:

$$a + b\sqrt{2} + ci + d\sqrt{2}i\ \ (a, b, c, d \in \mathbb{Q})$$

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén

1. *A $K \cup \{\alpha\}$ halmaz által generált részgyűrű:*

   $$\{f(\alpha) : f \in K[x]\} =: K[\alpha].$$

2. *A $K \cup \{\alpha\}$ halmaz által generált résztest:*

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

Biz.

1. Az világos, hogy minden $f(\alpha)$ $(f \in K[x])$ alakú elem előállítható a $K \cup \{\alpha\}$ halmazból az első három alapművelettel.

   Másrészt az is világos, hogy ezen elemek halmaza már zárt az első három alapműveletre, tehát ez lesz a $K \cup \{\alpha\}$ halmaz által generált részgyűrű.

2. Az világos, hogy minden $t(\alpha)$ $(t \in K(x))$ alakú elem előállítható a $K \cup \{\alpha\}$ halmazból a négy alapművelettel.

   Másrészt az is világos, hogy ezen elemek halmaza már zárt a négy alapműveletre, tehát ez lesz a $K \cup \{\alpha\}$ halmaz által generált résztest.

□

Állítás

Tetszőleges $\alpha \in L \mid K$ *esetén* $Gy_\alpha := \{f \in K[x] : f(\alpha) = 0\} \lhd K[x]$.

Biz.

HF □

Állítás

Legyen $\alpha \in L \mid K$ *és tegyük fel, hogy* $Gy_\alpha \neq \{0\}$. *Ekkor bármely* $f \in K[x]$ *polinomra az alábbi három állítás ekvivalens.*

(1) *Az* f *polinom generálja a* Gy_α *ideált:* $(f) = Gy_\alpha$.

(2) *Az* f *polinom minimális fokszámú azon nemnulla polinomok között, amelyeknek* α *gyöke.*

(3) *Az* f *polinom irreducibilis* K *felett, és* α *gyöke* f*-nek.*

Biz.

(1) $\implies$ (2): Tegyük fel, hogy $(f) = Gy_\alpha$. Ekkor nyilván $f(\alpha) = 0$.

Ha $0 \neq g \in K[x]$ és $g(\alpha) = 0$, akkor

$$g \in Gy_\alpha \implies f \mid g \implies \deg f \leq \deg g,$$

tehát f fokszáma valóban minimális.

Állítás

Tetszőleges $\alpha \in L \mid K$ *esetén* $Gy_\alpha := \{f \in K[x] : f(\alpha) = 0\} \lhd K[x]$.

Biz.

HF □

Állítás

Legyen $\alpha \in L \mid K$ *és tegyük fel, hogy* $Gy_\alpha \neq \{0\}$. *Ekkor bármely* $f \in K[x]$ *polinomra az alábbi három állítás ekvivalens.*

(1) *Az* f *polinom generálja a* Gy_α *ideált:* $(f) = Gy_\alpha$.

(2) *Az* f *polinom minimális fokszámú azon nemnulla polinomok között, amelyeknek* α *gyöke.*

(3) *Az* f *polinom irreducibilis* K *felett, és* α *gyöke* f*-nek.*

Biz.

(2) $\implies$ (3): Tegyük fel, hogy f minimális fokszámú, de nem irreducibilis: $f = gh$ $(\deg g, \deg h < \deg f)$. Ekkor

$$f(\alpha) = g(\alpha)\, h(\alpha) = 0 \implies g(\alpha) = 0 \text{ vagy } h(\alpha) = 0,$$

ami ellentmond $\deg f$ minimalitásának.

Állítás

Tetszőleges $\alpha \in L \mid K$ *esetén* $Gy_\alpha := \{f \in K[x] : f(\alpha) = 0\} \lhd K[x]$.

Biz.

HF □

Állítás

Legyen $\alpha \in L \mid K$ *és tegyük fel, hogy* $Gy_\alpha \neq \{0\}$. *Ekkor bármely* $f \in K[x]$ *polinomra az alábbi három állítás ekvivalens.*

(1) *Az* f *polinom generálja a* Gy_α *ideált:* $(f) = Gy_\alpha$.

(2) *Az* f *polinom minimális fokszámú azon nemnulla polinomok között, amelyeknek* α *gyöke.*

(3) *Az* f *polinom irreducibilis* K *felett, és* α *gyöke* f*-nek.*

Biz.

(3) $\implies$ (1): Tegyük fel, hogy $f(\alpha) = 0$ és f irreducibilis.

$$\left.\begin{array}{l} f(\alpha) = 0 \implies (f) \subseteq Gy_\alpha \\ f \text{ irred.} \implies (f) \text{ max. ideál} \end{array}\right\} \implies (f) = Gy_\alpha \text{ vagy } Gy_\alpha = K[x].$$ □

Definíció

Legyen $\alpha \in L \mid K$.

- Ha $Gy_\alpha \neq \{0\}$, akkor azt mondjuk, hogy α **algebrai** K felett.

  A Gy_α ideált generáló főpolinomot (mely egyértelműen meghatározott), az α elem K feletti **minimálpolinomjának** nevezzük. Jelölés: $m_{\alpha,K}$. Az $m_{\alpha,K}$ polinom fokszámát az α **algebrai elem fokszámának** nevezzük.

- Ha $Gy_\alpha = \{0\}$, akkor azt mondjuk, hogy α **transzcendens** K felett.

- A $\mathbb{C} \mid \mathbb{Q}$ testbővítés algebrai illetve transzcendens elemeit **algebrai számoknak** illetve **transzcendens számoknak** nevezzük.

Példa

- Ha $\alpha \in K$, akkor (és csak akkor) α elsőfokú algebrai elem: $m_{\alpha,K} = x - \alpha$.
- $i \in \mathbb{C} \mid \mathbb{R}$ másodfokú algebrai elem: $m_{i,\mathbb{R}} = x^2 + 1$.
- $i \in \mathbb{C} \mid \mathbb{Q}\left(\sqrt{2}\right)$ másodfokú algebrai elem: $m_{i,\mathbb{Q}(\sqrt{2})} = x^2 + 1$.
- Ha $z \in \mathbb{C} \setminus \mathbb{R}$, akkor z másodfokú algebrai elem $\mathbb{R}$ felett: $m_{z,\mathbb{R}} = x^2 - 2\,\mathrm{Re}\, z \cdot x + |z|^2$.

Példa

- $\sqrt{2}$ másodfokú algebrai szám: $m_{\sqrt{2},\mathbb{Q}} = x^2 - 2$.
- $\sqrt[n]{2}$ n-edfokú algebrai szám: $m_{\sqrt[n]{2},\mathbb{Q}} = x^n - 2$ (miért irreducibilis?).
- π és e transzcendens számok.
- A Liouville-féle $\sum \frac{1}{10^{n!}}$ konstans transzcendens szám.
- Ha $\alpha \neq 0, 1$ és $\beta \notin \mathbb{Q}$ algebrai számok, akkor α^β transzcendens szám. Például $2^{\sqrt{2}}$, $\sqrt{2}^{\sqrt{2}}$ és $e^{-\pi/2} = i^i$ transzcendens számok.

Példa

Határozzuk meg $\alpha = 4 - \sqrt{3}$ minimálpolinomját $\mathbb{C}$, $\mathbb{R}$ és $\mathbb{Q}$ felett.

- $\alpha \in \mathbb{C} \implies m_{\alpha,\mathbb{C}} = x - \alpha$
- $\alpha \in \mathbb{R} \implies m_{\alpha,\mathbb{R}} = x - \alpha$
- $(\alpha - 4)^2 = 3 \implies \alpha^2 - 8\alpha + 13 = 0 \implies m_{\alpha,\mathbb{Q}} = x^2 - 8x + 13$ (miért irreducibilis?)

Példa

Határozzuk meg $\alpha = i\sqrt{2-\sqrt{2}}$ minimálpolinomját $\mathbb{C}$, $\mathbb{R}$ és $\mathbb{Q}$ felett.

- $\alpha \in \mathbb{C} \implies m_{\alpha,\mathbb{C}} = x - \alpha$
- $\alpha^2 = -\left(2-\sqrt{2}\right) \implies \alpha^2 + 2 - \sqrt{2} = 0 \implies m_{\alpha,\mathbb{R}} = x^2 + 2 - \sqrt{2}$
  (miért irreducibilis?)
- $\left(\alpha^2+2\right)^2 = 2 \implies \alpha^4 + 4\alpha^2 + 2 = 0 \implies m_{\alpha,\mathbb{Q}} = x^4 + 4x^2 + 2$
  (miért irreducibilis?)

Példa

Határozzuk meg az $\alpha = \sqrt{2} + i$ algebrai szám $\mathbb{Q}$ feletti minimálpolinomját.

$$\alpha^2 = 1 + 2\sqrt{2}i \implies \left(\alpha^2 - 1\right)^2 = -8 \implies \alpha^4 - 2\alpha^2 + 9 = 0$$

Tehát α gyöke az $x^4 - 2x^2 + 9$ polinomnak. Ez irreducibilis $\mathbb{Q}$ felett?

Az $x^4 - 2x^2 + 9$ polinom

- komplex gyökei:
  $\alpha = \sqrt{2} + i,\ \overline{\alpha} = \sqrt{2} - i,\ -\alpha = -\sqrt{2} - i,\ -\overline{\alpha} = -\sqrt{2} + i;$
- $\mathbb{C}$ feletti irreducibilis faktorizációja:
  $(x - \alpha)(x - \overline{\alpha}) \cdot (x + \alpha)(x + \overline{\alpha});$
- $\mathbb{R}$ feletti irreducibilis faktorizációja:
  $\left(x^2 - 2\sqrt{2}x + 3\right) \cdot \left(x^2 + 2\sqrt{2}x + 3\right);$
- $\mathbb{Q}$ feletti irreducibilis faktorizációja: $x^4 - 2x^2 + 9$.

Tehát $m_{\alpha,\mathbb{Q}} = x^4 - 2x^2 + 9$.

Tétel

Ha $\alpha \in L \mid K$ transzcendens K felett, akkor

(1) $K(\alpha) \mid K \cong K(x) \mid K$ *az alábbi φ izomorfizmus mellett:*

$$\varphi\colon K(x) \to K(\alpha),\ t \mapsto t(\alpha);$$

(2) $[K(\alpha) : K] = \infty$.

Biz.

(1): Ha $t = \frac{f}{g} \in K(x)$, akkor $t(\alpha)$ értelmezett, mert α transzcendenciája miatt $g(\alpha) \neq 0$. Így definiálhatjuk a

$$\psi\colon K(x) \to L,\ t \mapsto t(\alpha)$$

homomorfizmust. Ennek magja $\{0\}$, értékkészlete pedig $K(\alpha)$.
A homomorfiatétel szerint $K(x) \cong K(x)/(0) \cong K(\alpha)$; a megfelelő izomorfizmus éppen a fenti φ leképezés.

Minden $c \in K$ esetén $c\varphi = c(\alpha) = c$, tehát φ nem csak a $K(x)$ és $K(\alpha)$ testek, de a $K(x) \mid K$ és $K(\alpha) \mid K$ testbővítések között is izomorfizmust létesít.

Tétel

Ha $\alpha \in L \mid K$ transzcendens K felett, akkor

(1) $K(\alpha) \mid K \cong K(x) \mid K$ *az alábbi φ izomorfizmus mellett:*

$$\varphi\colon K(x) \to K(\alpha),\ t \mapsto t(\alpha);$$

(2) $[K(\alpha) : K] = \infty$.

Biz.

(2): Az $1, x, x^2, x^3, \ldots$ vektorrendszer lineárisan független a ${}_K K(x)$ vektortérben, ezért ennek φ melletti képe, azaz $1, \alpha, \alpha^2, \alpha^3, \ldots$ is lineárisan független vektorrendszer a ${}_K K(\alpha)$ vektortérben.
Tehát $[K(\alpha) : K] = \infty$.

Konkrétabban: ha $1, \alpha, \alpha^2, \alpha^3, \ldots$ lineárisan összefüggő lenne, akkor valamelyik tagja előállna az őt megelőző tagok lineáris kombinációjaként:

$$\alpha^{k+1} = c_k\alpha^k + \cdots + c_1\alpha + c_0 1 \ (c_0, c_1, \ldots, c_k \in K).$$

Ekkor α gyöke lenne a nemzéró $x^{k+1} - c_k x^k - \cdots - c_1 x - c_0 \in K[x]$ polinomnak, ami ellentmond α transzcendenciájának. □

Következmény

Test egyszerű transzcendens bővítése izomorfia erejéig egyértelműen meghatározott.

Ha $K(\alpha) \mid K$ *és* $K(\beta) \mid K$ *egyszerű transzcendens bővítések, akkor* $K(\alpha) \mid K \cong K(\beta) \mid K$ *az alábbi* φ *izomorfizmus mellett:*

$$\varphi\colon K(\alpha) \to K(\beta),\ t(\alpha) \mapsto t(\beta) \quad (t \in K(x)).$$

Biz.

Tudjuk, hogy $K(\alpha) \mid K \cong K(x) \mid K \cong K(\beta) \mid K$:

$$\begin{array}{ccccc} K(\alpha) & \xleftarrow{\sigma} & K(x) & \xrightarrow{\tau} & K(\beta) \\ t(\alpha) & \longmapsfrom & t & \longmapsto & t(\beta) \end{array}$$

A két izomorfizmust „összevarrva” kapjuk a $\varphi = \sigma^{-1}\tau$ izomorfizmust:

$$\begin{array}{ccc} K(\alpha) & \xrightarrow{\sigma^{-1}\tau} & K(\beta) \\ t(\alpha) & \longmapsto & t(\beta) \end{array}$$

□

Következmény

Minden K testnek létezik egyszerű transzcendens bővítése, és ez a bővítés izomorfia erejéig egyértelműen meghatározott.

Biz.

- unicitás: most láttuk
- egzisztencia: $K(x)$

□

Tétel

Ha $\alpha \in L \mid K$ algebrai K felett, akkor

(0) $K(\alpha) = K[\alpha]$

(1) $K(\alpha) \mid K \cong K[x]/(m_{\alpha,K}) \mid K$ *az alábbi φ izomorfizmus mellett:*

$$\varphi\colon K[x]/(m_{\alpha,K}) \to K(\alpha),\ \overline{f} \mapsto f(\alpha);$$

(2) $[K(\alpha) : K] = \deg m_{\alpha,K}$.

Biz.

(0) & (1): Tekintsük a

$$\psi\colon K[x] \to L,\ f \mapsto f(\alpha)$$

homomorfizmust. Ennek magja $Gy_\alpha = (m_{\alpha,K})$, értékkészlete pedig $K[\alpha]$. A homomorfiatétel szerint $K[x]/(m_{\alpha,K}) \cong K[\alpha]$; a megfelelő izomorfizmus éppen a fenti φ leképezés.

Mivel $m_{\alpha,K}$ irreducibilis, $K[x]/(m_{\alpha,K})$ test, így $K[\alpha]$ is az. Következésképp $K[\alpha] = K(\alpha)$.

Minden $c \in K$ esetén $\overline{c}\varphi = c(\alpha) = c$, tehát φ a megfelelő testbővítések között is izomorfizmust létesít.

Tétel

Ha $\alpha \in L \mid K$ algebrai K felett, akkor

(0) $K(\alpha) = K[\alpha]$

(1) $K(\alpha) \mid K \cong K[x]/(m_{\alpha,K}) \mid K$ *az alábbi φ izomorfizmus mellett:*

$$\varphi\colon K[x]/(m_{\alpha,K}) \to K(\alpha),\ \overline{f} \mapsto f(\alpha);$$

(2) $[K(\alpha) : K] = \deg m_{\alpha,K}$.

Biz.

(2): Legyen $n = \deg m_{\alpha,K}$. A $K[x]/(m_{\alpha,K})$ test elemei egyértelműen előállnak

$$\overline{a_{n-1}x^{n-1} + \cdots + a_1x + a_0} = a_{n-1}\overline{x}^{n-1} + \cdots + a_1\overline{x} + a_0 \ (a_0, a_1, \ldots, a_{n-1} \in K)$$

alakban.

Ez azt jelenti, hogy $1, \overline{x}, \ldots, \overline{x}^{n-1}$ bázisa a K feletti $K[x]/(m_{\alpha,K})$ vektortérnek. Ezen bázis φ melletti képe, azaz $1, \alpha, \ldots, \alpha^{n-1}$ bázisa a ${}_KK(\alpha)$ vektortérnek. □

Következmény

Test egyszerű algebrai bővítését izomorfia erejéig egyértelműen meghatározza az adjungált elem minimálpolinomja.

Ha $K(\alpha) \mid K$ *és* $K(\beta) \mid K$ *egyszerű algebrai bővítések és* $m_{\alpha,K} = m_{\beta,K} = m \in K[x]$, *akkor* $K(\alpha) \mid K \cong K(\beta) \mid K$ *az alábbi* φ *izomorfizmus mellett:*

$$\varphi\colon K(\alpha) \to K(\beta),\ f(\alpha) \mapsto f(\beta) \quad (f \in K[x], \deg f \leq n-1).$$

Biz.

Tudjuk, hogy $K(\alpha) \mid K \cong K[x]/(m) \mid K \cong K(\beta) \mid K$:

$$\begin{array}{ccccc} K(\alpha) & \xleftarrow{\sigma} & K[x]/(m) \mid K & \xrightarrow{\tau} & K(\beta) \\ f(\alpha) & \longleftarrow & f & \longmapsto & f(\beta) \end{array}$$

A két izomorfizmust „összevarrva” kapjuk a $\varphi = \sigma^{-1}\tau$ izomorfizmust:

$$\begin{array}{ccc} K(\alpha) & \xrightarrow{\sigma^{-1}\tau} & K(\beta) \\ f(\alpha) & \longmapsto & f(\beta) \end{array}$$

□

Következmény

Tetszőleges K test és $f \in K[x]$ irreducibilis polinom esetén létezik olyan $K(\alpha)$ egyszerű algebrai bővítés, ahol $m_{\alpha,K} = f$, és ez a bővítés izomorfia erejéig egyértelműen meghatározott.

Biz.

- unicitás: most láttuk
- egzisztencia: $K[x]/(f) = K(\alpha)$, ahol $\alpha = \overline{x}$

□

Példa

A $\mathbb{Q}\left(\sqrt[3]{2}\right) \mid \mathbb{Q}$ bővítés harmadfokú, mert $m_{\sqrt[3]{2},\mathbb{Q}} = x^3 - 2$.

Egy bázis: $1, \sqrt[3]{2}, \sqrt[3]{4}$. Tehát $\mathbb{Q}\left(\sqrt[3]{2}\right)$ elemei egyértelműen előállnak

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} \ \ (a, b, c \in \mathbb{Q})$$

alakban.

(Miért nem alkotnak testet az $a + b\sqrt[3]{2} \ \ (a, b \in \mathbb{Q})$ alakú számok?
Mert ez a halmaz nem zárt a szorzásra, például $\sqrt[3]{4}$ nem áll elő $a + b\sqrt[3]{2}$ alakban.
Ha előállna, akkor $\sqrt[3]{4} - b\sqrt[3]{2} - a = 0$ lenne, azaz $\sqrt[3]{2}$ gyöke lenne az $x^2 - bx - a \in \mathbb{Q}[x]$ polinomnak. Ez lehetetlen, mert $\sqrt[3]{2}$ minimálpolinomja harmadfokú.)

Példa

Számoljunk a $\mathbb{Q}(\alpha)$ testben, ahol $\alpha = \sqrt[3]{7}$.

- elemek: $a\alpha^2 + b\alpha + c \ \ (a, b, c \in \mathbb{Q})$
- számolási szabály: $\alpha^3 = 7$ (mert $m_{\sqrt[3]{7},\mathbb{Q}} = x^3 - 7$)

$$\begin{aligned}(\alpha^2 + \alpha + 1) \cdot (3\alpha^2 - \alpha + 2) &= 3\alpha^4 + 2\alpha^3 + 4\alpha^2 + \alpha + 2 \\ &= 3\alpha \cdot 7 + 2 \cdot 7 + 4\alpha^2 + \alpha + 2 \\ &= 4\alpha^2 + 22\alpha + 16\end{aligned}$$

(Vagy a $3x^4 + 2x^3 + 4x^2 + x + 2$ polinomot maradékosan osztva az $x^3 - 7$ polinommal kapjuk a $4x^2 + 22x + 16$ maradékot.)

$(2 - \alpha)^{-1} = ?$

A $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x] / (x^3 - 7)$ izomorfiát használva, a $\overline{2 - x}^{-1}$ elemet kell kiszámolni. Ezt korábban már kiszámoltuk: $\overline{2 - x}^{-1} = \overline{x^2 + 2x + 4}$. Tehát $(2 - \alpha)^{-1} = \alpha^2 + 2\alpha + 4$, vagyis

$$\frac{1}{2 - \sqrt[3]{7}} = \sqrt[3]{49} + 2\sqrt[3]{7} + 4.$$

Példa

Legyen α gyöke az $x^3 + x + 1$ polinomnak. Határozzuk meg az α^{-2} szám „kanonikus alakját”.

- $\mathbb{Q}(\alpha)$ elemei: $a\alpha^2 + b\alpha + c \ \ (a, b, c \in \mathbb{Q})$
- számolási szabály: $\alpha^3 = -\alpha - 1$ (mert $m_{\alpha,\mathbb{Q}} = x^3 + x + 1$)

Az $x^2 \cdot u \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása: $u \equiv x^2 - x + 1$. Tehát $\alpha^{-2} = \alpha^2 - \alpha + 1$.

Másik lehetőség: az $x \cdot v \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása: $v \equiv -x^2 - 1$. Tehát $\alpha^{-1} = -\alpha^2 - 1$, és így
$\alpha^{-2} = \left(-\alpha^2 - 1\right)^2 = \alpha^4 + 2\alpha^2 + 1 = \alpha\left(-\alpha - 1\right) + 2\alpha^2 + 1 = \alpha^2 - \alpha + 1.$

Harmadik lehetőség: $1 = -\alpha^3 - \alpha = \alpha \cdot \left(-\alpha^2 - 1\right)$, ezért
$\alpha^{-1} = -\alpha^2 - 1$.

Ellenőrzés:
$\alpha^2 \cdot \left(\alpha^2 - \alpha + 1\right) = \alpha^4 - \alpha^3 + \alpha^2 = \alpha\left(-\alpha - 1\right) - \left(-\alpha - 1\right) + \alpha^2 = 1.$

Ugyanez megy $\mathbb{Z}_2$ felett. És $\mathbb{Z}_3$ felett?

Definíció

Ha minden $\alpha \in L \mid K$ algebrai K felett, akkor azt mondjuk, hogy $L \mid K$ **algebrai bővítés**.

Tétel

Minden végesfokú bővítés algebrai.

Biz.

Legyen $[L : K] = n$ és $\alpha \in L$. Az $1, \alpha, \alpha^2, \ldots, \alpha^n$ vektorrendszer lineárisan függő az ${}_K L$ vektortérben, ezért vannak olyan $c_0, \ldots, c_n \in K$ skalárok (nem mind nulla), hogy

$$c_n \alpha^n + \cdots + c_1 a + c_0 1 = 0.$$

Ez azt jelenti, hogy α gyöke a nemnulla $c_n x^n + \cdots + c_1 x + c_0 \in K[x]$ polinomnak. □

Tétel

Ha $L \mid K$ végesfokú bővítés, akkor minden $\alpha \in L$ esetén

$$\deg m_{\alpha,K} \mid [L : K].$$

Biz.

Alkalmazzuk a torony-törvényt a $K \leq K(\alpha) \leq L$ toronyra:

$$[L : K] = [L : K(\alpha)] \cdot [K(\alpha) : K] = [L : K(\alpha)] \cdot \deg m_{\alpha,K}.$$ □

Példa

Legyen $\alpha = i\sqrt{2-\sqrt{2}}$. Benne vannak-e a $\sqrt{2}$, $\sqrt[3]{2}$, $\sqrt[4]{2}$ számok a $\mathbb{Q}(\alpha)$ testben?

- $\sqrt{2} \overset{?}{\in} \mathbb{Q}(\alpha)$: igen, mert $\sqrt{2} = \alpha^2 + 2$.
- $\sqrt[3]{2} \overset{?}{\in} \mathbb{Q}(\alpha)$: nem, mert $\deg m_{\sqrt[3]{2},\mathbb{Q}} = 3 \nmid [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.
- $\sqrt[4]{2} \overset{?}{\in} \mathbb{Q}(\alpha)$: nem.

  $\sqrt[4]{2} \in \mathbb{Q}(\alpha) \implies \mathbb{Q}\left(\sqrt[4]{2}\right) \subseteq \mathbb{Q}(\alpha) \implies \mathbb{Q}\left(\sqrt[4]{2}\right) = \mathbb{Q}(\alpha)$,

  mert mindkettő negyedfokú bővítése $\mathbb{Q}$-nak.

  Ez viszont lehetetlen, hiszen $\alpha \notin \mathbb{Q}\left(\sqrt[4]{2}\right)$.

Tétel

Tetszőleges $L \mid K$ testbővítésben a K felett algebrai elemek résztestet alkotnak.

Biz.

Legyenek $\alpha, \beta \in L$ algebraiak K felett. Ekkor β algebrai $K(\alpha)$ felett is, és a fokszámtétel segítségével megbecsülhetjük a $K(\alpha, \beta) \mid K$ bővítés fokszámát:

$$\begin{aligned}
[K(\alpha,\beta) : K] &= [K(\alpha)(\beta) : K(\alpha)] \cdot [K(\alpha) : K] \\
&= \deg m_{\beta, K(\alpha)} \cdot \deg m_{\alpha, K} \\
&\leq \deg m_{\beta, K} \cdot \deg m_{\alpha, K}.
\end{aligned}$$

Tehát $K(\alpha, \beta) \mid K$ végesfokú, ezért minden eleme algebrai K felett. Speciálisan $\alpha + \beta,\ \alpha - \beta,\ \alpha \cdot \beta,\ \alpha/\beta$ (ha $\beta \neq 0$) is algebraiak K felett. □

Következmény

Az algebrai számok testet alkotnak.

Tétel

Ha α algebrai szám, akkor $\sqrt[n]{\alpha}$ is algebrai (a gyöknek mind az n értékére).

Biz.

Ha α gyöke az $f \in \mathbb{Q}[x]$ polinomnak, akkor $\sqrt[n]{\alpha}$ gyöke a $g(x) = f(x^n) \in \mathbb{Q}[x]$ polinomnak. □

Következmény

*A **gyökmennyiségek**, azaz a racionális számokból a négy alapművelet és gyökvonások véges számú alkalmazásával megkapható számok mind algebraiak.*

Biz.

A racionális számok (elsőfokú) algebrai számok, és az algebrai számok halmaza zárt a négy alapműveletre és a gyökvonásokra. □

Tétel

Van olyan algebrai szám, ami nem gyökmennyiség.