

Глава 4

Раширења поља

4.1 Кронекерова конструкција; коренско поље полинома

У овом делу позабавићемо се питањем проширивања поља до нових поља. Видећемо да се, уколико дати полином са коефицијентима у неком пољу, нема нулу у том пољу, увек може наћи поље које садржи то почетно, а у коме полином има нулу. Осим тога, видећемо како можемо конструисати коначна поља, а такође и када се до ширег поља може доћи „додавањем“ само једног елемента.

Размотримо следећи пример.

Пример 4.1 Проверити да је са:

$$f(p(X)) = p(i),$$

где је i имагинарна јединица, дефинисан један хомоморфизам $f: \mathbb{R}[X] \rightarrow \mathbb{C}$ и применити на тај хомоморфизам теорему о изоморфизму прстена.

Решење. Проверимо да је f заиста хомоморфизам прстена. Нека су $a(X), b(X) \in \mathbb{R}[X]$ и искажемо да је $c(X) = a(X) \cdot b(X)$. Тада је

$$\begin{aligned} f(a(X)) &= a(i) = a_0 + a_1 i + a_2 i^2 + \cdots + a_m i^m, \\ f(b(X)) &= b(i) = b_0 + b_1 i + b_2 i^2 + \cdots + b_n i^n \end{aligned}$$

и

$$f(c(X)) = c(i) = c_0 + c_1 i + c_2 i^2 + \cdots + c_{m+n} i^{m+n},$$

при чому смо претпоставили да је степен полинома $a(X)$ једнак m , а степен полинома $b(X)$ једнак n . Но, знамо како се множе полиноми, па је за $k = \overline{0, m+n}$:

$$c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0,$$

при чemu је наравно $a_l = 0$ за $l > m$, односно $b_s = 0$ за $s > n$. Но, тада је јасно да је заиста

$$c(i) = a(i) \cdot b(i),$$

те је

$$f(a(X) \cdot b(X)) = f(a(X)) \cdot f(b(X)).$$

Још лакше се проверава да је $f(a(X) + b(X)) = f(a(X)) + f(b(X))$, а јасно је и да је $f(1) = 1$ (константан полином има константну вредност).

Теорема о изоморфизмима за прстене даје следећи изоморфизам:

$$\mathbb{R}[X]/\text{Ker}(f) \cong \text{Im}(f).$$

Идентификујмо слику и јсзгро хомоморфизма f .

Уколико је $a + bi$ произвољни елемент из \mathbb{C} , јасно је да је $f(a + bX) = a + bi$, па је f „на“. Претпоставимо да $a(X) \in \text{Ker}(f)$. То значи да је $a(i) = 0$. Дакле, $a(X)$ је полином са реалним коефицијентима чија је једна нула комплексан број i . Из средње школе нам је познато да је тада и $-i$ обавезно нула тог полинома. Но, a је нула полинома $a(X)$ ако и само ако $X - \alpha$ дели $a(X)$ (ово смо већ имали прилике да користимо). Добијамо да и $X - i$ дели $a(X)$, али да и $X + i = X - (-i)$ такође дели $a(X)$. Полиноми $X - i$ и $X + i$ су узајамно прости, па закључујемо да полином $X^2 + 1 = (X - i)(X + i)$ дели $a(X)$. Заправо, то можемо видети и овако. Пошто $(X + i) | a(X)$, то мора бити $a(-i) = 0$. Но, пошто $(X - i) | a(X)$, онда је $a(X) = (X - i)a_1(X)$. Добијамо да је $0 = a(-i) = -2ia_1(-i)$, те је $a_1(-i) = 0$, тј. $(X + i) | a_1(X)$. Стога је $a_1(X) = (X + i)a_2(X)$, те је $a(X) = (X - i)(X + i)a_2(X) = (X^2 + 1)a_2(X)$.

Према томе, ако $a(X) \in \text{Ker}(f)$, онда $(X^2 + 1) | a(X)$. То се може записати и овако:

$$a(X) \in \text{Ker}(f) \implies a(X) \in \langle X^2 + 1 \rangle,$$

где наравно $\langle X^2 + 1 \rangle$ означава главни идеал генерисан полиномом $X^2 + 1$. Јасно је да важи и обратно. Наиме, ако $a(X) \in \langle X^2 + 1 \rangle$, то значи да је $a(X) = q(X)(X^2 + 1)$ за неки полином $q(X)$, но тада је

$$f(a(X)) = f(q(X)(X^2 + 1)) = f(q(X))f(X^2 + 1) = q(i)(i^2 + 1) = 0,$$

па $a(X) \in \text{Ker}(f)$. Закључујемо да је $\text{Ker}(f) = \langle X^2 + 1 \rangle$, те имамо следећи изоморфизам:

$$\mathbb{R}[X]/\langle X^2 + 1 \rangle \cong \mathbb{C}.$$



Урадимо још један пример.

Пример 4.2 Доказати да је $\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ једно потпоље поља \mathbb{C} . Применити теорему о изоморфизмима за прстене на хомоморфизам $f: \mathbb{Q}[X] \rightarrow \mathbb{Q}(\sqrt{2})$ дефинисан са $f(a(X)) = a(\sqrt{2})$.

Решење. Јасно је да је разлика два елемента из $\mathbb{Q}(\sqrt{2})$ такође у $\mathbb{Q}(\sqrt{2})$. Проверимо то за производ.

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2},$$

а како су $ac + 2bd$ и $ad + bc$ рационални бројеви увек када су то и a, b, c, d , закључујемо да $(a + b\sqrt{2})(c + d\sqrt{2}) \in \mathbb{Q}(\sqrt{2})$. Да бисмо показали да је $\mathbb{Q}(\sqrt{2})$ потпопље поља комплексних бројева, треба још само да проверимо да је инверз сваког елемента из $\mathbb{Q}(\sqrt{2}) \setminus \{0\}$ такође у скупу $\mathbb{Q}(\sqrt{2}) \setminus \{0\}$. Приметимо да је $a + b\sqrt{2} = 0$ ако и само ако је $a = b = 0$. Наиме, уколико претпоставимо да је $b \neq 0$, а $a + b\sqrt{2} = 0$, добијамо да је $\sqrt{2} = -\frac{a}{b}$, па би $\sqrt{2}$ био рационалан број, а знато још из средње школе да то није случај. Дакле, уколико је $a + b\sqrt{2} \neq 0$, то је (наравно да је и $a - b\sqrt{2} \neq 0$ за $a, b \in \mathbb{Q}$):

$$\frac{1}{a + b\sqrt{2}} = \frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

На исти начин као и у претходном примеру, проверава се да је f хомоморфизам. Осим тога, како је $f(a + bX) = a + b\sqrt{2}$, видимо да је f „на”. Покажимо да је $\text{Ker}(f) = \langle X^2 - 2 \rangle$.

Уколико $a(X) \in \langle X^2 - 2 \rangle$, то је $a(X) = q(X)(X^2 - 2)$ за неки полином $q(X) \in \mathbb{Q}[X]$, па је

$$f(a(X)) = f(q(X)(X^2 - 2)) = f(q(X))f(X^2 - 2) = q(\sqrt{2})((\sqrt{2})^2 - 2) = 0.$$

Дакле, $\langle X^2 - 2 \rangle \subseteq \text{Ker}(f)$. Покажимо да важи обратна импликација. Нека $a(X) \in \text{Ker}(f)$. То значи да је $a(\sqrt{2}) = 0$, па $(X - \sqrt{2}) | a(X)$. Да бисмо показали да $(X^2 - 2) | a(X)$, потребно нам је, а и доволно, да покажемо да и $(X + \sqrt{2}) | a(X)$, тј. да је $a(-\sqrt{2}) = 0$. Нека је

$$a(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n.$$

Како је $a(\sqrt{2}) = 0$, то је

$$a_0 + a_1\sqrt{2} + a_2 \cdot 2 + a_3 \cdot 2\sqrt{2} + \cdots + a_n(\sqrt{2})^n = 0.$$

Природно је дакле раздвојити парне степене од X и непарне степене од X . Претпоставимо, због једноставности ознака, да је $n = 2k$ (ако је n непаран број, онда додајемо још један кофицијент који је једнак нули – то не мења ништа у полиному, само у запису). Дакле,

$$a(X) = \sum_{i=0}^k a_{2i}X^{2i} + \sum_{i=0}^{k-1} a_{2i+1}X^{2i+1}.$$

Добијамо да је

$$\sum_{i=0}^k a_{2i}2^i + \left(\sum_{i=0}^{k-1} a_{2i+1}2^i \right) \sqrt{2} = 0.$$

Како су $a_s \in \mathbb{Q}$, то мора бити

$$\sum_{i=0}^k a_{2i} 2^i = 0 \quad \text{и} \quad \sum_{i=0}^{k-1} a_{2i+1} 2^i = 0.$$

Но, одавде добијамо да јс и

$$\sum_{i=0}^k a_{2i} 2^i - \left(\sum_{i=0}^{k-1} a_{2i+1} 2^i \right) \sqrt{2} = 0,$$

а то управо значи да јс $a(-\sqrt{2}) = 0$ (примстимо да јс $(-\sqrt{2})^{2i} = 2^i$, а $(-\sqrt{2})^{2i+1} = -2^i \sqrt{2}$). Овим јс завршон доказ да јс $\text{Ker}(f) = \langle X^2 - 2 \rangle$, тс добијамо изоморфизам

$$\mathbb{Q}[X]/\langle X^2 - 2 \rangle \cong \mathbb{Q}(\sqrt{2}).$$



Напомена. Могли смо и краће доказати да је $\text{Ker}(f) \subseteq \langle X^2 - 2 \rangle$. Наимс, ако јс $a(X) \in \text{Ker}(f)$, подслимо $a(X)$ са $X^2 - 2$. Добијамо да јс $a(X) = q(X)(X^2 - 2) + r + sX$, за неки полином $q(X) \in \mathbb{Q}[X]$ и рационалнс бројевс r, s . Како јс $a(\sqrt{2}) = 0$, добијамо да јс $r + s\sqrt{2} = 0$, а како су $r, s \in \mathbb{Q}$, то јс $r = s = 0$, тј. $a(X) \in \langle X^2 - 2 \rangle$. Но, није лоше видети и онај дужи доказ, па је зато и представљен.

У наредним разматрањима биће нам значајан следећи појам. Нека јс K поље. За полином $f \in K[X]$ кажемо да је НЕРАСТАВЉИВ над пољем K ако не постоје полиноми $g, h \in K[X]$, степенс барем један, такви да јс $f = gh$.

Анализирајмо сада мало шта смо добили у претходним примерима. Посматрајмо, да се тако изразимо, „леву” страну у добијним изоморфизмима. Видимо да се у оба случаја ради о количничком прстену прстена полинома по идеалу који је генерисан једним нерастављивим (над пољем \mathbb{Q}) полиномом другог степена. Оставимо за сада по страни чињеницу да је полином другог степена и концентришимо се на то да је он нерастављив. Количнички прстен је у оба случаја заправо поље. То, наравно, није случајно. Доказаћемо следећу важну теорему.

Теорема 4.3 Нека је F поље и $a(X) \in F[X] \setminus \{0\}$ нерастављив полином. Тада важи следеће.

- а) $E = F[X]/\langle a(X) \rangle$ је поље.
- б) Поље E садржи потпоље изоморфно пољу F .
- в) Полином $a(X)$ има бар једну нулу у пољу E .
- г) На основу б) можемо сматрати да је $F \subset E$. Тада се E може видети и као векторски простор над пољем F и димензија тог простора једнака је степену полинома $a(X)$.

Доказ. а) Знамо да је E комутативни прстен са јединицом. Треба да докажемо да је E поље, тј. да сваки елемент из E који није нула има инверз у односу на множење. Означимо идеал $\langle a(X) \rangle$ са I . Дакле, $E = F[X]/I$ и нула у том прстену је заправо $0 + I = I$. Претпоставимо да је $c(X) + I \neq I$, тј. да $c(X)$ не припада идеалу I . То значи да $a(X)$ не дели $c(X)$. Како је $a(X)$ нерастављив полином, закључујемо да је највећи заједнички делилац полинома $a(X)$ и $c(X)$ једнак 1. Стога постоје полиноми¹ $p(X)$ и $q(X)$ за које је

$$a(X)p(X) + c(X)q(X) = 1.$$

Преласком на количнички прстен добијамо једнакост

$$(a(X) + I)(p(X) + I) + (c(X) + I)(q(X) + I) = 1 + I.$$

С обзиром на чињеницу да је $a(X) \in I$ добијамо да је

$$(c(X) + I)(q(X) + I) = 1 + I,$$

те слемент $c(X) + I$ заиста има инверз у E . Дакле, E је заиста поље.

б) Дефинишимо хомоморфизам $f: F \rightarrow E$ са $f(\alpha) = \alpha + I$ за све $\alpha \in F$. Како су једини идеали у ма ком пољу $\{0\}$ и цело поље, то закључујемо да је $\text{Ker}(f) = \{0\}$ (језгро је увек идеал, али не може бити једнако целом пољу пошто се при хомоморфизму јединица слика у јединицу, а не у нулу). Дакле, хомоморфизам f успоставља изоморфизам између F и слике од f , која је потпоље од E .

в) Уочимо слемент $X + I$ у E . Означимо га са \tilde{X} . Означимо и слемент $\alpha + I$ са $\tilde{\alpha}$, за $\alpha \in F$. Уколико је $a(X) = a_0 + a_1X + \dots + a_nX^n$, добијамо да је

$$\begin{aligned} a(\tilde{X}) &= \tilde{a}_0 + \tilde{a}_1\tilde{X} + \tilde{a}_2\tilde{X}^2 + \dots + \tilde{a}_n\tilde{X}^n \\ &= (a_0 + I) + (a_1 + I)(X + I) + \dots + (a_n + I)(X + I)^n, \\ &= (a_0 + a_1X + a_2X^2 + \dots + a_nX^n) + I = a(X) + I = I, \end{aligned}$$

те добијамо да \tilde{X} заиста анулира полином $a(X)$.

г) Како E садржи потпоље F' изоморфно са F , заиста са алгебарске тачке можемо сматрати да је $F \subset E$. Наравно да елементе поља E можемо сабирати, али, с обзиром да је $F \subset E$, можемо их и множити слементима из F . На основу својства операција у пољу E добијамо да је E заиста векторски простор над F . Наш задатак је да докажемо да је димензија овог простора једнака $\deg a(X)$. Доказаћемо заправо да је

$$[1 + I, X + I, \dots, X^{n-1} + I]$$

једна база простора E уколико је полином $a(X)$ степена n .

¹Погледати додатак I.

Покажимо прво да је $\{1+I, X+I, \dots, X^{n-1}+I\}$ генератриса. Уочимо ма који елемент $p(X)+I \in E$. Тада је

$$p(X) = q(X)a(X) + r(X),$$

где је $r(X) = 0$, или је $\deg r(X) < \deg a(X) = n$. Дакле,

$$r(X) = r_0 + r_1X + \dots + r_{n-1}X^{n-1},$$

где наравно неки, па и сви, кофицијенти $r_i \in F$ могу бити једнаки 0. Но, тада је

$$p(X) + I = (q(X) + I)(a(X) + I) + (r(X) + I),$$

те је

$$p(X) + I = r_0(1+I) + r_1(X+I) + \dots + r_{n-1}(X^{n-1}+I).$$

Закључујемо да $1+I, \dots, X^{n-1}+I$ заиста генеришу E , над пољем F .

Докажимо и да је систем $[1+I, X+I, \dots, X^{n-1}+I]$ линсарно независан. Нека је

$$c_0(1+I) + c_1(X+I) + \dots + c_{n-1}(X^{n-1}+I) = 0+I,$$

за неке $c_i \in F$. Тада је

$$(c_0 + c_1X + \dots + c_{n-1}X^{n-1}) + I = I,$$

те

$$c_0 + c_1X + \dots + c_{n-1}X^{n-1} \in I = \langle a(X) \rangle.$$

Но, полином $a(X)$ је степена n и он може да дели $c_0 + c_1X + \dots + c_{n-1}X^{n-1}$ једино ако је $c_0 + c_1X + \dots + c_{n-1}X^{n-1} = 0$. Но, то управо значи да је $c_0 = c_1 = \dots = c_{n-1} = 0$, те закључујемо да су $1+I, \dots, X^{n-1}+I$ заиста линсарно независни. \square

Коментар. Уколико поље E садржи потпоље изоморфно пољу F , тада кажемо да је поље E једно РАШИРЕЊЕ поља F . У том случају можемо сматрати да је E векторски простор над F , а димензију тог простора зовемо И СТЕПЕН РАШИРЕЊА поља E над F и означавамо са $[E : F]$.

Искористимо управо доказану теорему да конструишимо поље од 4 елемента. Примстимо да \mathbb{Z}_4 је комутативан прстен, али наравно да да није поље пошто у \mathbb{Z}_4 важи: $2 \cdot 2 = 0$, а $2 \neq 0$.

Пример 4.4 Конструисати поље, које има тачно 4 елемента.

Решење. Како ово извести? Прво свега, ми знајмо да је \mathbb{Z}_2 поље и да има 2 елемента. Претходна теорема нам каже да ако нађемо нерасстављив полином $a(X) \in \mathbb{Z}_2[X]$, који је степена n онда ће $\mathbb{Z}_2[X]/\langle a(X) \rangle$

бити поље, које је истовремено векторски простор над \mathbb{Z}_2 димензије n . Дакле, то поље је као векторски простор над \mathbb{Z}_2 изоморфно \mathbb{Z}_2^n , те има 2^n елемената. Нама је потребно поље са 4 елемента, тј. потребан нам је нерастављив полином из $\mathbb{Z}_2[X]$ степена 2. Такав полином наравно није тешко наћи. То је полином $a(X) = 1 + X + X^2$. Како је то полином другог степена, он је нерастављив ако и само ако нема ниједну нулу у \mathbb{Z}_2 , а како је $a(0) = 1$ и $a(1) = 1$, то је заиста испуњено. Дакле, наше поље F_4 је дато са

$$F_4 = \mathbb{Z}_2[X]/\langle X^2 + X + 1 \rangle.$$

Означимо са η елемент $X + \langle X^2 + X + 1 \rangle$ у овом пољу. Добијамо да је

$$F_4 = \{0, 1, \eta, 1 + \eta\}.$$

Како у пољу F_4 важи: $\eta^2 = 1 + \eta$ (погледати доказ десла в) теореме 4.3), можемо написати и таблице сабирања и множења у том пољу.

$+$	0	1	η	$1 + \eta$	\cdot	0	1	η	$1 + \eta$
0	0	1	η	$1 + \eta$	0	0	0	0	0
1	1	0	$1 + \eta$	η	1	0	1	η	$1 + \eta$
η	η	$1 + \eta$	0	1	η	0	η	$1 + \eta$	1
$1 + \eta$	$1 + \eta$	η	1	0	$1 + \eta$	0	$1 + \eta$	1	η

На сличан начин могу се конструисати и поља са нпр. 8 или 9 елемената (погледати задатак 4.2)



Вратимо се поново на теорему. Претпоставимо да нам је дат неки полином $a(X) \in F[X]$ где је F неко поље. Тада полином наравно не мора имати линеарну факторизацију над пољем F . Поставља се питање: да ли постоји неко поље E које садржи поље F и у коме је полином $a(X)$ факторише на линеарне факторе? То заиста јесте тачно и претходна теорема нам показује и пут доказа.

Последица 4.5 Нека је F поље и $a(X) \in F[X]$. Тада постоји раширење E поља F у коме се полином $a(X)$ факторише на линеарне факторе.

Доказ. Јасно је да можемо да претпоставимо да је полином $a(X)$ нерастављив, пошто бисмо у супротном његову факторизацију добили тако што бисмо нашли раширење у коме сви његови фактори имају линеарну факторизацију.

На основу доказане теореме, постоји поље E' , које је раширење поља F , а у коме полином $a(X)$ има бар једну нулу, назовимо је α . То значи да у $E'[X]$ важи факторизација

$$a(X) = (X - \alpha)b(X),$$

где је $b(X) \in E'[X]$ и $\deg b(X) = n - 1$. Уколико сада $b(X)$ раставимо на нерастављиве факторе у $E'[X]$, на њих можемо применити претходно закључивање. Тако процес настављамо све док не дођемо до линеарне

факторизације. Јасно је да се процес мора завршити пошто у сваком кораку добијамо бар једну нову нулу почетног полинома, а он ини у једном пољу не може имати више од n нула. \square

Дефиниција 4.6 Нека је $a(X) \in F[X] \setminus \{0\}$, где је F поље. КОРЕНСКО ПОЉЕ полинома $a(X)$ је најмање раширење поља F у коме $a(X)$ има линеарну факторизацију.

Сва поља, која ћемо у даљем разматрати ће бити такозвана бројевна поља, тј. потпоља од \mathbb{C} . Приметимо да свако такво поље обавезно садржи као своје потпоље поље \mathbb{Q} .

4.2 Алгебарска раширења; примитивни елемент

Позабавимо се сада „десном” страном у изоморфизму доказаном у примеру 4.2. Ту се појављује се следећа ознака: $\mathbb{Q}(\sqrt{2})$. Посматрајмо ствари мало општије.

Нека је B комутативни прстен са јединицом, A његов потпрстен (са јединицом наравно) и $b \in B \setminus A$. Како одредити најмањи потпрстен од B који садржи и A (као потпрстен) и b као елемент? Очигледно је да такав прстен мора да садржи и све степене од b , као и све елементе облика $a_0 + a_1b + a_2b^2 + \dots + a_nb^n$ где $a_i \in A$. Дакле, мора да садржи све елементе облика $p(b)$, где $p(X) \in A[X]$. Но, то је заправо и довољно, тј. тражени најмањи потпрстен је

$$A[b] := \{p(b) : p(X) \in A[X]\}.$$

Наиме, $A[b]$, овако дефинисан, је заиста потпрстен од B (очигледно је да је $A \subset A[b]$ и $b \in A[b]$):

$$\begin{aligned} p(b), q(b) \in A[b] &\implies p(b) - q(b) = (p - q)(b) \in A[b]; \\ p(b), q(b) \in A[b] &\implies p(b)q(b) = (pq)(b) \in A[b]. \end{aligned}$$

Слично, уколико је F поље и $\alpha \in \mathbb{C} \setminus F$, онда са $F(\alpha)$ означавамо најмање потполе од \mathbb{C} које садржи (као своје потполе) F и α (као свој елемент). Поставља се природно питање: када је $F[\alpha] = F(\alpha)$? Другим речима, интересује нас у ком је случају прстен $F[\alpha]$ поље. Обратите пажњу да ово има смисла разматрати једино уколико је F поље. На пример, нема смисла разматрати $\mathbb{Z}(i)$, док важи $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.

Није тешко наћи један потребан услов да би $F[\alpha]$ било поље. Претпоставимо да је $F[\alpha]$ поље. Како је

$$F[\alpha] = \{p(\alpha) : p(X) \in F[X]\},$$

а сваки елемент поља, који је различит од нуле има инверз, то и елемент $\alpha \in F[\alpha]$ има инверз у $F[\alpha]$, тј. постоји $a(\alpha) \in F[X]$ такав да је $\alpha \cdot a(\alpha) = 1$. Ако је $a(X) = a_0 + a_1X + \dots + a_nX^n$, то добијамо да је

$$a_n\alpha^{n+1} + \dots + a_1\alpha^2 + a_0\alpha - 1 = 0,$$

тј. постоји полином $p(X) \in F[X]$ такав да је $p(\alpha) = 0$ (то је наравно полином $a_nX^{n+1} + \dots + a_1X^2 + a_0X - 1$).

Дефиниција 4.7 Нека је F потпоље од \mathbb{C} и $\alpha \in \mathbb{C}$. Тада је α АЛГЕБАРСКИ над F уколико постоји полином $p(X) \in F[X]$ за који је $p(\alpha) = 0$.

Дакле, видели смо да је потребан услов да прстен $F[\alpha]$ буде поље да је α алгебарски над F . Но, то је и довољан услов.

Став 4.8 Нека је F потпоље од \mathbb{C} и $\alpha \in \mathbb{C}$. Тада је $F[\alpha]$ поље ако и само ако је α алгебарски над F .

Доказ. Један смер смо већ доказали. Остало је да се покаже да из чињенице да је α алгебарски над F следи да је $F[\alpha]$ поље. Како је α алгебарски над F , посматрајмо идеал $I \triangleleft F[X]$ дефинисан са:

$$I = \{a(X) \in F[X] : a(\alpha) = 0\}.$$

Није тешко проверити да је I заиста идеал (приметимо да $I \neq \{0\}$ следи из чињенице да је α алгебарски елемент). Како је по ставу 3.18 сваки идеал у $F[X]$ главни, то постоји моничан полином $\mu_\alpha(X)$ за који је $I = \langle \mu_\alpha \rangle$.

Приметимо да је полином $\mu_\alpha(X)$ нерастављив. У супротном, нека је $\mu_\alpha(X) = a(X)b(X)$ за неке исконстантне полиноме $a(X), b(X)$ из $F[X]$. Но, тада је $a(\alpha)b(\alpha) = \mu_\alpha(\alpha) = 0$, па следи да је $a(\alpha) = 0$ или $b(\alpha) = 0$. Уколико је, на пример, $a(\alpha) = 0$, добили бисмо да $a(X) \in I$, па $\mu_\alpha(X)$ дели $a(X)$, што није могуће јер је $a(X)$ полином степена мањег од степена полинома $\mu_\alpha(X)$. Слично се добија и у случају да је $b(\alpha) = 0$.

Сада, као и у примерима 4.1 и 4.2, посматрамо хомоморфизам

$$f: F[X] \rightarrow F[\alpha]$$

дефинисан са $f(p(X)) = p(\alpha)$. Хомоморфизам f је очигледно „на”, а $\text{Ker}(f) = I$. Стога по теореми 3.30 добијамо да је

$$F[X]/I \cong F[\alpha].$$

Но, како је $\mu_\alpha(X)$ нерастављив полином, $F[X]/I$ је поље (по теореми 4.3), па је и $F[\alpha]$ такође поље. \square

Коментар. Из претходног доказа следи: ако елемент α није алгебарски над F , тада је $F[X] \cong F[\alpha]$ (јер је $I = \{0\}$). На пример, како π није

алгебарски² над \mathbb{Q} , то је $\mathbb{Q}[X] \cong \mathbb{Q}[\pi]$, што нам даје једну конкретну реализацију прстена $\mathbb{Q}[X]$ (погледати и додатак I).

Приметимо да из доказа овог става и дела г) теореме 4.3 следи:

$$[F(\alpha) : F] = \deg \mu_\alpha(X).$$

Полином $\mu_\alpha(X)$ зове се и **минимални полином** елемента α . Базу за $F(\alpha)$ над F чине елементи $1, \alpha, \dots, \alpha^{n-1}$ уколико је $n = \deg \mu_\alpha(X)$. Приметимо да из доказа претходног става добијамо и следеће (еквивалентне) дефиниције полинома $\mu_\alpha(X)$. Наиме, $\mu_\alpha(X)$ је моничан полином такав да је $\mu_\alpha(\alpha) = 0$ и при томе важи неки од следећих услова (а тиме и сви):

1. $\mu_\alpha(X)$ је полином најмањег степена за који важи претходно;
2. $\mu_\alpha(X)$ је нерастављив;
3. ако је $p(\alpha) = 0$ за неко $p \in F[X]$, тада $\mu_\alpha \mid p$.

Пример 4.9 Нека је $\alpha = \sqrt{2} + \sqrt{3}$.

- a) Показати да је α алгебарски над \mathbb{Q} .
- б) Наћи минимални полином за α над \mathbb{Q} .
- в) Одредити $\frac{1}{\alpha+3}$ у облику $p(\alpha)$ за неки полином $p(X) \in \mathbb{Q}[X]$.

Решење. а) Пронађимо полином који елемент α анулира. Како важи $\alpha - \sqrt{2} = \sqrt{3}$, то је

$$\begin{aligned} (\alpha - \sqrt{2})^2 &= 3 \\ \alpha^2 - 2\alpha\sqrt{2} + 2 &= 3 \\ \alpha^2 - 1 &= 2\alpha\sqrt{2} \\ (\alpha^2 - 1)^2 &= (2\alpha\sqrt{2})^2 \\ \alpha^4 - 2\alpha^2 + 1 &= 8\alpha^2 \\ \alpha^4 - 10\alpha^2 + 1 &= 0. \end{aligned}$$

б) Покажимо да је минимални полином елемента α заиста полином $X^4 - 10X^2 + 1$. Означимо га са $\mu(X)$. Једино треба доказати је овај полином нерастављив над \mathbb{Q} . Како се ради о полиному четвртог степена, уколико је он растављив, он се раставља или на производ полинома првог степена и полинома трећег степена, или на производ два полинома другог степена.

1° $\mu(X)$ је производ полинома првог степена и полинома трећег степена над пољем \mathbb{Q} . То значи да $\mu(X)$ има нулу у \mathbb{Q} . Но, ако полином

$$a_n X^n + \dots + a_1 X + a_0$$

²Доказ овог тврђења превазилази оквире овог иџбеника.

има рационалну нулу r/s (где је r/s нескратив разломак) онда $r \mid a_0$ и $s \mid a_n$. Како је у нашем случају $a_n = a_4 = 1$, то је $s = 1$, а како је $a_0 = 1$, то r може бити само 1 или -1. Но, ни 1 ни -1 нису нуле полинома $\mu(X)$, па овај случај није могућ.

2^o $\mu(X)$ је производ два полинома другог степена над \mathbb{Q} . Дакле,

$$\mu(X) = (X^2 + aX + b)(X^2 + cX + d)$$

(како је $\mu(X)$ моничан, можемо претпоставити да су и ти полиноми монични). Добијамо (изједначавањем одговарајућих коефицијената)

$$a + c = 0 \tag{4.1}$$

$$b + ac + d = -10 \tag{4.2}$$

$$ad + bc = 0 \tag{4.3}$$

$$bd = 1 \tag{4.4}$$

Из (4.1) добијамо да је $c = -a$. Тада из (4.3) следи да је $a(d - b) = 0$. Размотримо два случаја.

2.1^o $a = 0$. Тада је и $c = 0$ и добијамо да се систем своди на двс једначине

$$b + d = -10 \tag{4.5}$$

$$bd = 1 \tag{4.6}$$

Из (4.6) следи да је $d = 1/b$ (сигурно ни b ни d нису једнаки нули). Заменом у (4.5) и сређивањем добијамо квадратну једначину

$$b^2 + 10b + 1 = 0.$$

Решења ове једначине су дата са:

$$b_{1,2} = \frac{-10 \pm \sqrt{96}}{2}$$

По претпоставци $b \in \mathbb{Q}$. Како је $\sqrt{96} = 4\sqrt{6}$, добили бисмо да је $\sqrt{6} \in \mathbb{Q}$. Остављамо читаоцима да покажу да ово није тачно.

2.2^o $a \neq 0$. У овом случају је $b = d$. Из једначине (4.4) добијамо да је $b \in \{1, -1\}$. Заменом у (4.2) (узимајући у обзир да је $c = -a$) добијамо да је $a^2 = 12$ или $a^2 = 8$. По претпоставци је $a \in \mathbb{Q}$ па би из $a^2 = 12$ следило да $\sqrt{3} \in \mathbb{Q}$, а из $a^2 = 8$ да је $\sqrt{2} \in \mathbb{Q}$. Како ни једно ни друго није тачно закључујемо да је $\mu(X)$ нерастављив.

в) За налажење $\frac{1}{\alpha+3}$ можемо користити метод неодређених коефицијената. Наиме, знамо да постоје $a, b, c, d \in \mathbb{Q}$ такви да је

$$\frac{1}{\alpha+3} = a + b\alpha + c\alpha^2 + d\alpha^3. \tag{4.7}$$

Потребно је одредити кофицијенте a, b, c, d . Из (4.7), множењем обе стране са $\alpha + 3$, добијамо

$$1 = (\alpha + 3)(a + b\alpha + c\alpha^2 + d\alpha^3). \quad (4.8)$$

Узимајући у обзир да је $\alpha^4 = 10\alpha^2 - 1$ и да су $1, \alpha, \alpha^2, \alpha^3$ линсарно независни над \mathbb{Q} , добијамо

$$\begin{array}{rcl} 3a & -d & = 1 \\ a + 3b & & = 0 \\ b + 3c + 10d & = 0 \\ c + 3d & = 0 \end{array}$$

Решење овог система једначина је $a = \frac{3}{8}$, $b = -\frac{1}{8}$, $c = -\frac{3}{8}$ и $d = \frac{1}{8}$, па важи

$$\frac{1}{\alpha + 3} = \frac{3}{8} - \frac{1}{8}\alpha - \frac{3}{8}\alpha^2 + \frac{1}{8}\alpha^3.$$



Дакле, видели смо да су од посебног значаја за теорију раширења поља они елементи који су алгебарски над датим пољем.

Дефиниција 4.10 За раширење E поља F кажемо да је АЛГЕБАРСКО раширење ако је сваки елемент из E алгебарски над F .

За раширење E поља F кажемо да је коначно раширење уколико је E коначно димензионални простор над F .

Став 4.11 Свако коначно раширење је алгебарско.

Доказ. Иска је $[E : F] = n$. То значи да је E један n -димензионални простор над пољем F . Узмимо произвољни елемент $\alpha \in E$ и покажимо да је он алгебарски над F . Како је димензија простора једнака n , то је скуп од $n + 1$ вектора $\{1, \alpha, \dots, \alpha^n\}$ сигурно линсарно зависан скуп вектора, тј. постоје $a_0, \dots, a_n \in F$ такви да је

$$a_0 1 + a_1 \alpha + \dots + a_n \alpha^n = 0.$$

Но, то управо значи да је $p(\alpha) = 0$, где је $p(X) = a_0 + a_1 X + \dots + a_n X^n$ полином из $F[X]$. Дакле, елемент α је алгебарски над F . \square

Већ смо се упознали са раширењима облика $F(\alpha)$. Но, ако $\beta \notin F(\alpha)$, може се формирати и раширење $F(\alpha)(\beta)$, које се краће означава са $F(\alpha, \beta)$. Општије, имамо и раширења $F(\alpha_1, \dots, \alpha_n)$. Но, веома је занимљив следећи резултат који нам каже да у случају алгебарских раширења поља \mathbb{Q} ситуација није толико компликована колико изгледа.

Теорема 4.12 (Теорема о примитивном елементу) Свако коначно раширење E поља \mathbb{Q} је облика $\mathbb{Q}(\alpha)$, за неко $\alpha \in E$.

Елемент α је тај ПРИМИТИВНИ ЕЛЕМЕНТ раширења E . Ову тврдимо нећемо доказивати.

Наведимо још два примера за крај.

Пример 4.13 Наћи један примитивни елемент коренског поља полинома $X^4 - X^2 - 2 \in \mathbb{Q}[X]$.

Решење. Другим речима, треба наћи коренско поље K датог полинома и елемент $\alpha \in K$ за који је $K = \mathbb{Q}(\alpha)$. Факторишимо³ наш полином над \mathbb{Q} методом комплетирања квадрата:

$$\begin{aligned} X^4 - X^2 - 2 &= \left(X^2 - \frac{1}{2}\right)^2 - \frac{1}{4} - 2 = \left(X^2 - \frac{1}{2}\right)^2 - \left(\frac{3}{2}\right)^2 = \\ &= \left(X^2 - \frac{1}{2} - \frac{3}{2}\right) \left(X^2 - \frac{1}{2} + \frac{3}{2}\right) = (X^2 - 2)(X^2 + 1) \\ &= (X - \sqrt{2})(X + \sqrt{2})(X - i)(X + i), \end{aligned}$$

где је i наравно имагинарна јединица. Дакле, коренско поље K је поље $K = \mathbb{Q}(\sqrt{2}, i)$. Ми треба да нађемо α за које је $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\alpha)$. Покушајмо да докажемо да се за α може узети елемент $\alpha = \sqrt{2} + i$. Како је $\alpha \in \mathbb{Q}(\sqrt{2}, i)$, следи $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, i)$. Обратна инклузија је нетривијална. Наравно, довољно је да докажемо да нпр. $\sqrt{2} \in \mathbb{Q}(\alpha)$, пошто из тога непосредно следи да и $i = \alpha - \sqrt{2} \in \mathbb{Q}(\alpha)$, а тиме и тражено. Једнакост

$$\alpha = \sqrt{2} + i,$$

„подигнимо“ на трећи степен. Добијамо

$$\alpha^3 = 2\sqrt{2} + 6i - 3\sqrt{2} - i = -\sqrt{2} + 5i = 5(\sqrt{2} + i) - 6\sqrt{2}.$$

Дакле, $\alpha^3 - 5\alpha = -6\sqrt{2}$, па је

$$\sqrt{2} = -\frac{1}{6}(\alpha^3 - 5\alpha) \in \mathbb{Q}(\alpha). \quad \clubsuit$$

Пример 4.14 Нека је K коренско поље полинома $X^4 - 24X^2 + 4 \in \mathbb{Q}[X]$.

- Показати да је $K = \mathbb{Q}(\sqrt{5}, \sqrt{7})$.
- Одређити $\alpha \in \mathbb{C}$ тако да је $K = \mathbb{Q}(\alpha)$.

Решење. Поступимо као у претходном примеру. Важи:

$$\begin{aligned} X^4 - 24X^2 + 4 &= (X^2 - 12)^2 - 144 + 4 \\ &= (X^2 - 12)^2 - 140 \\ &= (X^2 - 12)^2 - (2\sqrt{35})^2 \\ &= (X^2 - 12 - 2\sqrt{35})(X^2 - 12 + 2\sqrt{35}) \\ &= (X^2 - (12 + 2\sqrt{35}))(X^2 - (12 - 2\sqrt{35})), \end{aligned}$$

³Једначина $x^4 - x^2 - 2 = 0$ је биквадратна, па њена решења можемо добити и увођењем смене $u = x^2$ и решавањем одговарајуће квадратне једначине.

Иска је зато $\alpha = \sqrt{12 + 2\sqrt{35}}$ и $\beta = \sqrt{12 - 2\sqrt{35}}$. Дакле, добили смо:

$$X^4 - 24X^2 + 4 = (X - \alpha)(X + \alpha)(X - \beta)(X + \beta),$$

па је

$$K = \mathbb{Q}\left(\sqrt{12 + 2\sqrt{35}}, \sqrt{12 - 2\sqrt{35}}\right).$$

Један савет: увек када добијете овакав резултат, није лоше помножити ова два корсна и видети шта се добија. Примнимо тај савет у овом случају.

$$\sqrt{12 + 2\sqrt{35}} \cdot \sqrt{12 - 2\sqrt{35}} = \sqrt{144 - 140} = \sqrt{4} = 2.$$

Дакле, можемо да закључимо да је $\alpha \cdot \beta = 2$, па је $\beta = \frac{2}{\alpha} \in \mathbb{Q}(\alpha)$. Закључујемо да је $K = \mathbb{Q}(\alpha)$. Тако смо нашли примитивни слемент и урадили пример под б)!

Други савет: када имате корен попут овога: $\sqrt{12 + 2\sqrt{35}}$, проверите да мажда не можете да га „препознате“. Шта то значи? У овом случају, појављује се корен из броја облика $p + q\sqrt{s}$ где су p, q, s цели бројеви. Да ли је мажда тај корен збир (или разлика) два корена из искних целих бројева? Како је $35 = 5 \cdot 7$, намеће се да израчунамо колико је $(\sqrt{5} + \sqrt{7})^2$. Добијамо $(\sqrt{5} + \sqrt{7})^2 = 5 + 2\sqrt{35} + 7 = 12 + 2\sqrt{35}$, тј. баш оно што имамо. Дакле, $\alpha = \sqrt{5} + \sqrt{7}$ (примстимо да је $\beta = \sqrt{7} - \sqrt{5}$), те је $K = \mathbb{Q}(\sqrt{5} + \sqrt{7})$. Ми треба да покажемо да је $K = \mathbb{Q}(\sqrt{5}, \sqrt{7})$. То није тешко, поступићемо као у претходном примеру.

$$\begin{aligned} \alpha &= \sqrt{5} + \sqrt{7} \\ \alpha^3 &= 5\sqrt{5} + 15\sqrt{7} + 21\sqrt{5} + 7\sqrt{7} \\ \alpha^3 &= 26\sqrt{5} + 22\sqrt{7} \\ 22\alpha &= 22\sqrt{5} + 22\sqrt{7} \\ \alpha^3 - 22\alpha &= 4\sqrt{5} \\ \sqrt{5} &= \frac{\alpha^3 - 22\alpha}{4} \in \mathbb{Q}(\alpha) \\ \sqrt{7} &= \alpha - \sqrt{5} \\ \sqrt{7} &= \frac{26\alpha - \alpha^3}{4} \in \mathbb{Q}(\alpha). \end{aligned}$$

Наравно, могли смо то да урадимо и другачије. Пошто смо већ препознали да је $\beta = \sqrt{7} - \sqrt{5}$, онда само треба показати да је

$$\mathbb{Q}(\sqrt{5} + \sqrt{7}, \sqrt{7} - \sqrt{5}) = \mathbb{Q}(\sqrt{5}, \sqrt{7}),$$

а то је наравно врло једноставно.



У овом кратком одељку само смо „загребали“ теорију расириења поља. Но, ипак смо видели како можемо конструисати коначно поље које није облика \mathbb{Z}_p . Коначна поља су веома значајна у применама и о њима ће више речи бити у курсу Алгебре 2. Друго занимљиво питање које ће бити третирано у Алгебри 2 је старо питање могућности поделе угла на три једнака дела лењиром и шестаром. Алгебра нам лако показује зашто то у општем случају није могуће, тако што се покаже, користећи теорију расириења поља, да није могуће конструисати угао од 20° , а сви добро знамо да конструишемо угао од 60° . За тај доказ нам не треба много више теорије него што је имамо, али се негде, како се то каже, ипак мора ставити тачка. И ми је стављамо овде.

Задаци

- 4.1** Доказати да поља $\mathbb{Q}(\sqrt{2})$ и $\mathbb{Q}(\sqrt{3})$ нису изоморфна.
- 4.2** Конструисати поље са: а) 8 слесната; б) 9 слесната.
- 4.3** Показати да је $\alpha = i + \sqrt{3}$ алгебарски над \mathbb{Q} . Нађи минимални полином за α и одредити $\frac{1}{\alpha^2 - 2}$ у облику $p(\alpha)$, где је $p(X) \in \mathbb{Q}[X]$.
- 4.4** Урадити све из претходног задатка за слеснит $\alpha = \sqrt{5} - \sqrt{3}$.
- 4.5** Урадити све из задатка 4.3 за слеснит $\alpha = \sqrt{2 + \sqrt{3}}$.
- 4.6** Нађи α тако да је $\mathbb{Q}(i, \sqrt{5}) = \mathbb{Q}(\alpha)$.
- 4.7** Нађи α тако да је $\mathbb{Q}(\sqrt{5}, \sqrt{7}) = \mathbb{Q}(\alpha)$.
- 4.8** Нађи коренско поље K полинома $X^4 + 2X^2 - 15 \in \mathbb{Q}[X]$ и одредити слеснит α за који је $K = \mathbb{Q}(\alpha)$.
- 4.9** Нађи коренско поље K полинома $X^4 - 12X^2 + 9$ и одредити слеснит α за који је $K = \mathbb{Q}(\alpha)$.
- 4.10** Нађи коренско поље K полинома $X^4 + 12X^2 - 4$ и одредити слеснит α за који је $K = \mathbb{Q}(\alpha)$.