АЛГЕБРА

Поља

Зоран Петровић

Десето предавање

Започнимо ову лекцију једним примером.

Пример 1 Проверити да је са:

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

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

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

$$f(a(X)) = a(i) = a_0 + a_1 i + a_2 i^2 + \cdots + a_m i^m,$$

$$f(b(X)) = b(i) = b_0 + b_1 i + b_2 i^2 + \cdots + b_n i^n$$

и

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

при чему 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 чему је наравно $a_i = 0$ за $i > m$, односно $b_j = 0$, за $j > n$. 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:

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

Идентификујмо слику и језгро 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 $a(X) \in \mathrm{Ker}(f)$. 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, α 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 $a(X)$. Према томе, ако $a(X) \in \mathrm{Ker}(f)$, онда $(X^2+1) \mid a(X)$. То се може записати и овако:

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

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 $a(X) \in \mathrm{Ker}(f)$. Закључујемо да је $\mathrm{Ker}(f) = \langle X^2+1\rangle$, те важи изоморфизам

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

♣

Урадимо још један пример.

Пример 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 $f\colon \mathbb{Q}[X] \to Q(\sqrt{2})$ дефинисан са $f(a(X)) = a(\sqrt{2})$.

Јасно је да је разлика два елемента из $Q(\sqrt{2})$ такође у $Q(\sqrt{2})$. 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 ако су то a,b,c,d, закључујемо да $(a+b\sqrt{2})(c+d\sqrt{2}) \in \mathbb{Q}(\sqrt{2})$. Да бисмо показали да је $\mathbb{Q}(\sqrt{2})$ потпоље поља комплексних бројева, треба још само да проверимо да је инверз сваког не-нула елемента из $\mathbb{Q}(\sqrt{2})$ такође у $\mathbb{Q}(\sqrt{2})$. 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 знамо 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 хоморфизам. Осим тога, како је $f(a+bX) = a+b\sqrt{2}$, видимо да је f „на". Покажимо да је $\mathrm{Ker}(f) = \langle X^2-2\rangle$.

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, $\langle X^2-2\rangle \subseteq \mathrm{Ker}(f)$. Покажимо да важи обратна импликација. Нека $a(X) \in \mathrm{Ker}(f)$. То значи да је $a(\sqrt{2}) = 0$, па $(X-\sqrt{2}) \mid a(X)$. Да бисмо показали да $(X^2-2) \mid a(X)$, потребно нам је, а и довољно, да покажемо да и $(X+\sqrt{2}) \mid a(X)$, 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, то додајемо још један коефицијент 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

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

Но, одавде добијамо да је 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 је $a(-\sqrt{2}) = 0$ ($(-\sqrt{2})^{2i} = 2^i$, а $(-\sqrt{2})^{2i+1} = -2^i\sqrt{2}$). Овим је завршен доказ да је $\mathrm{Ker}(f) = \langle X^2-2\rangle$, те добијамо изоморфизам

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

♣

Напомена 3 Могли смо и краће доказати да је $\mathrm{Ker}(f) \subseteq \langle X^2 - 2\rangle$. Наиме, ако је $a(X) \in \mathrm{Ker}(f)$, поделимо $a(X)$ са $X^2 - 2$. Добијамо да је $a(X) = q(X)(X^2 - 2) + r + sX$, за неки полином $q(X) \in \mathbb{Q}[X]$ и рационалне бројеве r, s. Како је $a(\sqrt{2}) = 0$, добијамо да је $r + s\sqrt{2} = 0$, а како су $r, s \in \mathbb{Q}$, то је $r = s = 0$, тј. $a(X) \in \langle X^2 - 2\rangle$. Но, није лоше видети и онај дужи доказ, па је зато и презентиран.

Изанализирајмо мало шта смо добили у претходним примерима. Посматрајмо, да се тако изразимо, „леву" страну у добијеним изоморфизмима. Видимо да се у оба случаја ради о количничким 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 не може бити случајно. Доказаћемо следећу важну теорему.

Теорема 4 Нека је F поље и $a(X) \in F[X] \setminus \{0\}$ нерастављив полином.

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 а) 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 полиноми $p(X)$ 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 елемент $c(X) + I$ заиста има инверз у E. Закључујемо да је E поље.

б) Дефинишимо хомоморфизам $f: F \to E$ 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 $\mathrm{Ker}(f) = \{0\}$ (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 елемент $X + I$ у E. Означимо га са $\widetilde{X}$. Означимо и елемент $a + I$ са $\widetilde{a}$, за $a \in F$. Уколико је $a(X) = a_0 + a_1X + \cdots a_nX^n$, добијамо да је

$$a(\widetilde{X}) = \widetilde{a}_0 + \widetilde{a}_1\widetilde{X} + \widetilde{a}_2\widetilde{X}^2 + \cdots + \widetilde{a}_n\widetilde{X}^n$$

$$= (a_0 + I) + (a_1 + I)(X + I) + (a_2 + I)(X + I)^2 + \cdots + (a_n + I)(X + I)^n,$$

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

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

г) Како E садржи потпоље F' изоморфно са F, заиста са алгебарске тачке можемо сматрати да је $F \subset E$. У овом случају кажемо и да је поље E једно проширење поља F. Наравно да елементе поља E можемо сабирати, али, с обзиром да је $F \subset E$, можемо их и множити елементима из F. На основу својстава операција у пољу E добијамо да је E заиста векторски простор над F. Димензију тог простора зовемо и степен проширења поља E над F и означавамо са $[E : F]$. Наш задатак је да докажемо да је $[E : F] = \deg a(X)$. Доказаћемо заправо да је

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

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

$\{1 + I, X + I, \ldots, X^{n-1} + I\}$ је 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,

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

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

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

те је

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

Закључујемо да $1 + I, \ldots, X^{n-1} + I$ заиста генеришу E.

Линеарна независност: Нека је

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

за неке $c_i \in F$. Тада је

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

те

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

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

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

Пример 5 Конструисати поље, које има тачно 4 елемента.

Како ово извести? Пре свега, ми знамо да је $\mathbb{Z}_2$ поље и да има 2 елемента. Претходна теорема нам каже да ако нађемо нерастављив 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: $\eta^2=1+\eta$ (зашто?), можемо написати и таблице сабирања и множења у том пољу.

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

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

♣

Вратимо се поново на теорему. Претпоставимо да нам је дат неки полином $a(X) \in F[X]$ где је F неко поље. Тај 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 се полином $a(X)$ факторише на линеарне факторе? То заиста јесте тачно и претходна теорема нам показује и пут доказа.

Последица 6 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 ни у једном пољу не може имати више од n нула. □

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 $\mathbb{Q}$. Најмање раширење поља F у коме се дати полином из $F[X]$ факторише на линеарне факторе назива се коренско поље тог полинома.

Позабавимо се сада „десном" страном у изоморфизму доказаном у другом примеру. 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 подскуп) и b као елемент? Очигледно је да такав прстен мора да садржи и све степене од b, као и све елементе облика $a_0 + a_1 b + a_2 b^2 + \cdots + a_n b^n$ 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 $b \in A[b]$):

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

Уколико је F поље и $\alpha \in \mathbb{C} \setminus F$, онда са $F[\alpha]$ означавамо најмањи потпрстен који садржи F и α, а са $F(\alpha)$ најмање потпоље које садржи (као своје потпоље) 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. Није тешко наћи један потребан услов за то. 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 $a(X) = a_0 + a_1 X + \cdots + a_n X^n$, то добијамо да је

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

тј. постоји полином $p(X) \in F[X]$ такав да је $p(\alpha) = 0$.

Дефиниција 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 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 $I \lhd F[X]$ дефинисан са:

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

Није тешко проверити да је I заиста идеал. Како је 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 неконстантне 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 $\mu_\alpha(X) \mid a(X)$, 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 наведеним примерима, посматрамо хомоморфизам

$$f \colon F[X] \to F[\alpha]$$

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

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

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

Приметимо да смо у оквиру доказа овог става добили и да је

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

Полином $\mu_\alpha(X)$ из овог става зове се и минимални полином елемента α. Базу за $F(\alpha)$ над F чине елементи $1, \alpha, \ldots, \alpha^{n-1}$ уколико је $n = \deg \mu_\alpha(X)$.

Пример 9 Нека је $\alpha = \sqrt{2} + \sqrt{3}$.

а) 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 $p(X) \in \mathbb{Q}[X]$.

а) Нађимо полином који елемент α анулира. Како је $\alpha - \sqrt{2} = \sqrt{3}$, 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 растаља или на производ полинома првог степена и полинома трећег степена, или на производ два полинома другог степена.

$\mu(X)$ 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

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

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 $\mu(X)$.

$\mu(X)$ је производ два полинома другог степена. 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)

$$\begin{aligned} a+c &= 0 && (1)\\ b+ac+d &= -10 && (2)\\ ad+bc &= 0 && (3)\\ bd &= 1 && (4) \end{aligned}$$

Из (1) добијамо да је $c=-a$. Тада из (3) следи да је $a(d-b)=0$. Размотримо два случаја.

$a=0$. Тада је и $c=0$ и добијамо да се систем своди на две једначине

$$\begin{aligned} b+d &= -10 && (5)\\ bd &= 1 && (6) \end{aligned}$$

Из (6) следи да је $d=1/b$ (сигурно ни b ни d нису једнаки нули). Заменом у (5) и сређивањем добијамо квадратну једначину

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

Решења ове једначине су дата са:

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

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 могуће.

$a\neq 0$. У овом случају је $b=d$. Из једначине (4) добијамо да је $b\in\{1,-1\}$. Заменом у (3) (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 такви да је

$$\frac{1}{\alpha+3}=a+b\alpha+c\alpha^2+d\alpha^3. \qquad (7)$$

Потребно је одредити коефицијенте a,b,c,d. Из (7), множењем обе стране са $\alpha+3$, добијамо

$$1=(\alpha+3)(a+b\alpha+c\alpha^2+d\alpha^3). \qquad (8)$$

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

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

Препуштамо читаоцима да реше овај систем једначина. ♣

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

Дефиниција 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 11 Свако коначно раширење је алгебарско.

Доказ. Нека је $[E : F] = n$. То значи да је E 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 $\{1, \alpha, \ldots, \alpha^n\}$ сигурно линеарно зависан скуп вектора, тј. постоје $a_0, \ldots, a_n \in E$ такви да је

$$a_0 1 + a_1\alpha + \cdots + a_n\alpha^n = 0,$$

но, то управо значи да је $p(\alpha) = 0$, где је $p(X) = a_0 + a_1X + \cdots + a_nX^n \in F[X]$. Дакле, елемент α је алгебарски над F. □

Већ смо се упознали са проширењима 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 $F(\alpha_1, \ldots, \alpha_n)$. Но, веома је занимљив следећи резултат који нам каже да у случају алгебарских раширења поља $\mathbb{Q}$ ситуација није толико компликована колико изгледа.

Теорема 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 теорему нећемо доказивати.

Још два примера за крај.

Пример 13 Наћи примитивни елемент коренског поља полинома $X^4 - X^2 - 2 \in \mathbb{Q}[X]$.

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

$$X^4 - X^2 - 2 = \left(X^2 - \frac{1}{2}\right)^2 - \frac{1}{4} - 2 = \left(X^2 - \frac{1}{2}\right)^2 - \left(\frac{3}{2}\right)^2 =$$

$$= \left(X^2 - \frac{1}{2} - \frac{3}{2}\right)\left(X^2 - \frac{1}{2} + \frac{3}{2}\right) = \left(X^2 - 2\right)\left(X^2 + 1\right) =$$

$$= (X - \sqrt{2})(X + \sqrt{2})(X - i)(X + i),$$

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 $\alpha = \sqrt{2} + i$. Јасно је да је $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, i)$. Обратна инклузија је нетривијална. Наравно, довољно је да докажемо да нпр. $\sqrt{2} \in \mathbb{Q}(\alpha)$, пошто из тога непосредно следи да и $i \in \mathbb{Q}(\alpha)$, 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

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

♣

Пример 14 Нека је K коренско поље полинома $X^4 - 24X^2 + 4 \in \mathbb{Q}[X]$.
а) Показати да је $K = \mathbb{Q}(\sqrt{5}, \sqrt{7})$.
б) Одредити $\alpha \in \mathbb{C}$ тако да је $K = \mathbb{Q}(\alpha)$.

Поступимо као у претходном примеру.

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

те добијамо $X^4 - 24X^2 + 4 = (X - \sqrt{12 + 2\sqrt{35}})(X + \sqrt{12 + 2\sqrt{35}})(X - \sqrt{12 - 2\sqrt{35}})(X + \sqrt{12 - 2\sqrt{35}})$. Према томе, добијамо да 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 корена и видети шта се добија. Применимо 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, ако је $\alpha = \sqrt{12 + 2\sqrt{35}}$, а $\beta = \sqrt{12 - 2\sqrt{35}}$, онда 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 елемент и урадили пример под б)!

Други савет: када имате корен попут овога: $\sqrt{12 + 2\sqrt{35}}$, проверите да можда 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 можда тај корен збир (или разлика) два корена из неких 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, $\alpha = \sqrt{5} + \sqrt{7}$ (приметимо да је $\beta = \sqrt{7} - \sqrt{5}$), те је $K = \mathbb{Q}\left(\sqrt{5} + \sqrt{7}\right)$. Ми треба да покажемо да је $K = \mathbb{Q}\left(\sqrt{5}, \sqrt{7}\right)$. 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

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

а то је наравно врло једноставно.