# АЛГЕБРА

## Поља

## Раширења; коренска поља полинома

Зоран Петровић

8. мај 2012.

У једној од претходних лекција показано је да је

$$\mathbb{R}[X]/\langle X^2+1\rangle \cong \mathbb{C}(=\mathbb{R}[i])$$

и

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

У овој лекцији позабавићемо се озбиљније овим конструкцијама. Започнимо лекцију следећом важном теоремом.

**Теорема 1** 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) Како је $a(X)$ нерастављив, то је идеал $I = \langle a(X)\rangle$ максималан у скупу свих главних идеала. Но, у прстену $F[X]$ је сваки идеал главни, те је $I$ максималан идеал. Стога је $E$ поље.

б) Дефинишимо хомоморфизам $f\colon F \to E$ 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 $E$. У даљем идентификујемо $F$ и слику $f[F]$, ради једноставнијег писања, тако да ћемо, између осталог, уместо $a + I$, за $a \in F$ писати само $a$.

в) Уочимо елемент $X + I$ у $E$. Означимо га са $\widetilde{X}$. Уколико је $a(X) = a_0 + a_1X + \cdots + a_nX^n$, добијамо да је

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

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

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 раширење 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 раширења 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 2** 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 $\eta$ 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.

| $+$ | $0$ | $1$ | $\eta$ | $1+\eta$ |
|---|---|---|---|---|
| $0$ | $0$ | $1$ | $\eta$ | $1+\eta$ |
| $1$ | $1$ | $0$ | $1+\eta$ | $\eta$ |
| $\eta$ | $\eta$ | $1+\eta$ | $0$ | $1$ |
| $1+\eta$ | $1+\eta$ | $\eta$ | $1$ | $0$ |

| $\cdot$ | $0$ | $1$ | $\eta$ | $1+\eta$ |
|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $\eta$ | $1+\eta$ |
| $\eta$ | $0$ | $\eta$ | $1+\eta$ | $1$ |
| $1+\eta$ | $0$ | $1+\eta$ | $1$ | $\eta$ |

♣

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 3** 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 $\alpha$. 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.

У претходном је коришћена ознака $\mathbb{Q}[\sqrt{2}]$. Овде је $\mathbb{Q}$ наравно поље, док је $\sqrt{2}$ елемент који није у том пољу. Његовим „додавањем" добијамо структуру, која је поље. Позабавимо се мало општијим разматрањем.

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 $\alpha$, а са $F(\alpha)$ најмање потпоље које садржи (као своје потпоље) $F$ и $\alpha$ (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. Наиме, 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 $a(X) = a_0 + a_1X + \cdots + a_nX^n$, 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 4** Нека је $F$ потпоље од $\mathbb{C}$ и $\alpha \in \mathbb{C}$. Тада је $\alpha$ 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 $\alpha$ алгебарски над $F$. Но, то је и довољан услов.

**Став 5** Нека је $F$ потпоље од $\mathbb{C}$ и $\alpha \in \mathbb{C}$. Тада је $F[\alpha]$ поље ако и само ако је $\alpha$ алгебарски над $F$.

**Доказ.** Један смер смо већ доказали. Остало је да се покаже да из чињенице да је $\alpha$ алгебарски над $F$ следи да је $F[\alpha]$ поље. Како је $\alpha$ 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. 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 нпр. $a(\alpha) = 0$, 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 ранијим 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 $\alpha$. Базу за $F(\alpha)$ над $F$ чине елементи $1, \alpha, \ldots, \alpha^{n-1}$ уколико је $n = \deg \mu_\alpha(X)$.

**Пример 6** Нека је $\alpha = \sqrt{2} + \sqrt{3}$.

а) Показати да је $\alpha$ алгебарски над $\mathbb{Q}$.

б) Наћи минимални полином за $\alpha$ 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 $\alpha$ 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 $\alpha$ 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.

$\mu(X)$ 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 $\mu(X)$ 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

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

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

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

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

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

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. ♣