АЛГЕБРА 2

Поља

Алгебарска раширења; примитивни елемент

Зоран Петровић

15. мај 2012.

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

Дефиниција 1 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 2 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 $p(X) = a_0 + a_1 X + \cdots + a_n X^n \in F[X]$. Дакле, елемент α је алгебарски над F. □

Уколико је E_1 коначно раширење поља F, а E_2 коначно раширење поља E_1, онда је наравно E_2 и једно раширење поља F.

Став 3 Ако су F, E_1 и E_2 поља као у претходној реченици, онда је E_2 коначно раширење поља F и важи

$$[E_2 : F] = [E_2 : E_1][E_1 : F].$$

Доказ. Нека је $[E_1 : F] = n$ и $[E_2 : E_1] = m$. Како је димензија E_1 као векторског простора над пољем F једнака n, то постоји нека база $[\alpha_1, \ldots, \alpha_n]$. Слично, нека је $[\beta_1, \ldots, \beta_m]$ база векторског простора E_2 над пољем E_1. Докажимо да производи $\alpha_i \beta_j$, $i = \overline{1,n}$, $j = \overline{1,m}$ чине базу простора E_2 над пољем F.

Линеарна независност. Претпоставимо да је

$$\sum_{j=1}^{m}\sum_{i=1}^{n} c_{ij}\alpha_i\beta_j = 0,$$

за неке $c_{ij} \in F$. Нека је $d_j = \sum_{i=1}^{n} c_{ij}\alpha_i$, $j = \overline{1,m}$. Елементи d_j су из поља E_1 и за њих важи:

$$\sum_{j=1}^{m} d_j\beta_j = 0.$$

Како је $[\beta_1, \ldots, \beta_m]$ база за E_2 над E_1, то мора бити $d_j = 0$ за све $j \in \{1, \ldots, m\}$. Но, како је $[\alpha_1, \ldots, \alpha_n]$ база за E_1 над пољем F, то из $\sum_{i=1}^{n} c_{ij}\alpha_i = 0$, за $j = \overline{1,m}$ следи да је $c_{ij} = 0$ за $i = \overline{1,n}$, $j = \overline{1,m}$.

Генератриса. Нека је $\gamma \in E_2$. Како је $[\beta_1, \ldots, \beta_m]$ база за E_2 над E_1, то постоје $r_j \in E_1$ такви да је

$$\gamma = \sum_{j=1}^{m} r_j\beta_j.$$

Но, како је $[\alpha_1, \ldots, \alpha_n]$ база за E_1 над F то за свако $j \in \{1, \ldots, m\}$ постоје s_{ij} за које је

$$r_j = \sum_{i=1}^{n} s_{ij}\alpha_i.$$

Коначно добијамо да је

$$\gamma = \sum_{j=1}^{m}\sum_{i=1}^{n} s_{ij}\alpha_i\beta_j.$$

□

У примерима из претходне лекције доказивали смо да су неки елементи алгебарски над датим пољем тако што смо налазили полиноме, које они поништавају, тј. користили смо директно дефиницију. То понекад није лако. Потражите уосталом сами полином, који поништава елемент $i\sqrt{3} + \sqrt[3]{2}$. Заправо, то се може избећи. А ево и како.

Већ смо се упознали са проширењима облика $E(\alpha)$. Но, ако $\beta \notin E(\alpha)$, може се формирати и проширење $E(\alpha)(\beta)$, које се краће означава са $E(\alpha, \beta)$. Уколико су α и β алгебарски над E, онда су степени проширења $[E(\alpha) : E]$ и $E(\beta) : E]$ коначни, а такав мора бити и $E(\alpha, \beta) : E(\alpha)]$ (зашто?). Стога је, на основу претходног става, $[E(\alpha, \beta) : E]$ коначан број, те је проширење $E(\alpha, \beta)$ поља E алгебарско, те је сваки елемент из $E(\alpha, \beta)$, алгебарски над E. Посебно, то су и елементи $\alpha + \beta$, $\alpha \cdot \beta$ и слично.

Општије, имамо и проширења $E(\alpha_1, \ldots, \alpha_n)$. Но, веома је занимљив следећи резултат који нам каже да у случају алгебарских проширења поља $\mathbb{Q}$ ситуација није толико компликована колико изгледа.

Теорема 4 (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, урадићемо неке примере.

Пример 5 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 $\mathbb{Q}$ коришћењем метода 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 6 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.