Материјал за курс Алгебра 3
Школска година 2024/25.

Алгебарско затворење поља

1 Егзистенција

Још смо у средњој школи видели да полином са реалним коефицијентима не мора имати реалне нуле, као и да су све нуле полинома са комплексним коефицијентима комплексни бројеви (прецизније, да је сваки полином из $\mathbb{C}[X]$ производ линеарних полинома из $\mathbb{C}[X]$). Започнимо зато следећом дефиницијом која је централна у овом тексту.

Дефиниција 1.1 За поље F кажемо да је *алгебарски затворено* ако се сваки полином из $F[X]$ може факторисати на линеарне факторе у $F[X]$.

Примери алгебарски затворених поља су $\mathbb{C}$, као и поље алгебарских бројева (обе чињенице ћемо касније доказати), док $\mathbb{R}$ није алгебарски затворено (али јесте потпоље алгебарски затвореног поља $\mathbb{C}$).

Од раније нам је познато како за поље F и полином $f \in F[X]$ можемо конструисати раширење поља F у коме f има линеарну факторизацију (тзв. *коренско поље полинома* f), па се поставља питање да ли за поље F постоји раширење које је алгебарски затворено. Прецизније, имамо следећу дефиницију.

Дефиниција 1.2 Поље E је *алгебарско затворење* поља F ако је његово алгебарско раширење и алгебарски затворено.

Дакле, поље $\mathbb{C}$ је алгебарско затворење поља $\mathbb{R}$. У следећој теореми доказујемо да свако поље има алгебарско затворење.

Теорема 1.3 Свако поље има алгебарско затворење.

Доказ. Нека је F дато поље. Као први корак, користићемо конструкцију сличну Кронекеровој, само што, уместо да један полином из $F[X]$ има нуле у конструисаном пољу, сада желимо да сви полиноми из $F[X]$ имају нуле у том пољу.

Посматрајмо зато прстен полинома над F са бесконачно много неодређених[1]

[1]Елементи овог прстена су коначне суме сабирака облика $c\prod_{f\in A} X_f^{n_f}$ за неки коначан скуп $A \subset F[X]$ и $n_f \in \mathbb{N}$, а операције сабирања и множења су дефинисане на стандардан начин (слично као у $F[X]$).

X_f које су индексиране полиномима $f \in F[X]$, тј. $R = F\left[X_f \mid f \in F[X]\right]$. Посматрајмо идеал I генерисан скупом $S = \{f(X_f) \mid f \in F[X]\}$. Наиме, желимо да X_f буде нула полинома f у конструисаном пољу, па нам је од интереса R/I. Ово не мора бити поље, па зато посматрамо максимални идеал $\mathfrak{m}$ који садржи I. Са курса Алгебра 2 нам је познато да он постоји ако је $I \neq R$, па то проверавамо.

Претпоставимо супротно. Тада је $1 \in I$, па постоји коначан скуп $A \subset F[X]$ и $a_f \in R$ за свако $f \in A$ тако да је

$$1 = \sum_{f \in A} a_f f(X_f). \tag{$*$}$$

Посматрајмо коренско поље F' полинома $\prod_{f \in A} f \in F[X]$. Тада за свако $f \in A$ постоји нула $\alpha_f \in F'$ полинома f, па ако у $(*)$ заменимо X_f са α_f, добијамо да у F' важи једнакост $1 = 0$, што је контрадикција.

Дакле, постоји максимални идеал $\mathfrak{m} \supseteq I$ прстена R, те је $E = R/\mathfrak{m}$ поље. Јасно, E је раширење поља F (садржи потпоље F_0 изоморфно са F) и сваки полином $f \in F[X]$ има нулу $\gamma_f = X_f + \mathfrak{m}$ у E. Докажимо да је E алгебарско раширење поља F. Елемент поља E је облика $p(X_{f_1}, \ldots, X_{f_n}) + \mathfrak{m}$ за неки полином p са коефицијентима у F и неке $f_i \in F[X]$, па да бисмо доказали да је он алгебарски над F (прецизније F_0), довољно је приметити да је садржан у $F_0(\gamma_{f_1}, \ldots, \gamma_{f_k})$, што је коначно[2] раширење поља F_0.

За сада смо конструисали алгебарско раширење E поља F такво да сваки полином из $F[X]$ има нулу у E. Како желимо и да сваки полином из $E[X]$ има нулу, поступак настављамо. Нека је зато $E_0 = E$ и за свако $i \geqslant 0$ конструишимо алгебарско раширење E_{i+1} поља E_i такво да сваки полином из $E_i[X]$ има нулу у E_{i+1} (као што је у претходном делу доказа E конструисано од F).

Коначно, спремни смо да конструишемо алгебарско затворење $\overline{F}$ поља F. Делује да је идеалан кандидат за $\overline{F}$ баш $\bigcup_{i \geqslant 0} E_i$. И било би тако да је $E_i \subseteq E_{i+1}$, али ми имамо (само) утапања $E_i \to E_{i+1}$, па је потребно искористити општију конструкцију, тзв. *колимес*. Нека је зато

$$\overline{F} = \bigsqcup_{i \geqslant 0} F_i \,/\sim,$$

где је $\sim$ релација еквиваленције задата са: $c_i \sim c_j$ за неке $c_i \in F_i$ и $c_j \in F_j$ ако и само ако је $i \leqslant j$ и c_j је слика од c_i при композицији утапања $E_i \to E_j$ или је $j \leqslant i$ уз аналогне услове. Ако је $[c]$ класа елемента c, тада су операције на $\overline{F}$ задате на природан начин, тј. $[c'] + [c''] := [c' + c'']$ и $[c'] \cdot [c''] := [c' \cdot c'']$. Јасно, $\overline{F}$ је раширење поља F и сваки елемент $[c]$ је алгебарски над F (јер је $c \in E_i$ за неко $i \geqslant 0$, а E_i је алгебарско раширење поља F).

Коначно, докажимо да је $\overline{F}$ алгебарски затворено. Нека је $p = \sum_{i=0}^{k} [c_i] X^i \in \overline{F}[X]$. Тада постоје $n_i \geqslant 0$ такви да је $c_i \in E_{n_i}$, па ако за $n = \max\{n_1, \ldots, n_k\}$

[2]Важи $[F_0(\gamma_{f_i}) : F_0] \leqslant \deg f_i$, па је и $[F_0(\gamma_{f_1}, \ldots, \gamma_{f_i}) : F_0(\gamma_{f_1}, \ldots, \gamma_{f_{i-1}})] \leqslant \deg f_i$, те је $F_0(\gamma_{f_1}, \ldots, \gamma_{f_k})$ коначно раширење од F_0 по ланчастом правилу.

са $c^{(i)} \in E_n$ означимо слику c_i при композицији утапања $E_{n_i} \to E_n$, то је $p = \sum_{i=0}^{k}[c^{(i)}]X^i$. При томе, полином $\widetilde{p} = \sum_{i=0}^{k} c^{(i)}X^i \in E_n[X]$ по конструкцији (поља E_{n+1}) има нулу c у E_{n+1}, па је $[c] \in \overline{F}$ нула полинома p. □

2 Јединственост и утапања

У претходном делу конструисано је алгебарско затворење $\overline{\mathbb{R}}$ поља $\mathbb{R}$, а раније је констатовано да је $\mathbb{C}$ једно алгебарско затворење поља $\mathbb{R}$. Поставља се логично питање да ли је $\overline{\mathbb{R}} \cong \mathbb{C}$? Одговор је потврдан, а доказ овог (и општијих) тврђења дајемо у наставку.

Пре самих доказа дајемо неколико запажања која могу помоћи да се наставак текста лакше испрати и да се боље разуме значај наредних тврђења.

Нека су E и F поља. По дефиницији, ако је E раширење поља F, тада поље E садржи потпоље F_0 које је изоморфно пољу F и самим тим имамо хомоморфизам $\theta : F \to E$. Са друге стране, ако имамо хомоморфизам $\varphi : F \to E$, тада је по ставу 13 из скрипти *Алгебра 3* (проф. Петровић) φ и утапање, па је $F \cong \varphi F$ и E је раширење поља F. Дакле, постојање хомоморфизма поља F у поље E је еквивалентно чињеници да је E раширење поља F. Може се рећи и да је ово прецизнија дефиниција раширења поља. Тако, ако имамо низ раширења $F \leqslant E \leqslant L$, при чему су $\theta : F \to E$ и $\mu : E \to L$ одговарајућа утапања, тада претпостављамо да је утапање $F \to L$ које одговара претходном раширењу $F \leqslant L$ баш $\mu\theta$. Наведимо и један пример.

Пример 2.1 Нека је $A = F(X)$ поље рационалних функција са једном неодређеном, а $B = F(X^2)$. Јасно, B је потпоље од A и при томе је димензија векторског простора A над B једнака 2 (проверите, ово није очигледно). Међутим, $A \cong B \subseteq A$, па је A раширење поље A и то такво да је $[A : A] = 2$. Ово делује чудно, па је прецизније рећи да је степен раширења A од A задатог утапањем $A \to A$ таквим да $X \mapsto X^2$ једнак 2, док је наравно степен раширења задатог идентичким утапањем једнак 1.

Нека је $\theta : F \to E$ утапање, а $L \supseteq F$ и $K \supseteq E$ раширења поља F и E, редом. Ако је $\lambda : L \to K$ утапање такво да је $\lambda(c) = \theta(c)$ за све $c \in F$, тада кажемо да λ *проширује* θ и пишемо $\theta \subseteq \lambda$.

Тврђење 2.2 Нека је $L \supseteq F$ алгебарско раширење поља F и $K \supseteq E$ алгебарски затворено поље. Ако је $\theta : F \to E$ утапање, тада постоји утапање $\lambda : L \to K$ које проширује θ (тј. дијаграм са десне стране комутира).

$$\begin{array}{ccc} L & \overset{\lambda}{\dashrightarrow} & K \\ {\scriptstyle\iota}\uparrow & & \uparrow{\scriptstyle\iota} \\ F & \xrightarrow{\theta} & E \end{array}$$

Доказ. Посматрајмо фамилију пресликавања

$$\mathcal{F} = \{\mu \mid \theta \subseteq \mu \text{ и } \mu : L' \to K \text{ за неко међуполе } F \subseteq L' \subseteq L\}.$$

Докажимо да $\mathcal{F}$ испуњава услове Цорнове леме. Пре свега, $\mathcal{F} \neq \emptyset$ (јер $\theta \in \mathcal{F}$). Нека је $\mathcal{L}$ ланац из $\mathcal{F}$ (у односу на $\subseteq$) и нека је домен пресликавања $\mu \in \mathcal{L}$ поље L_μ. Тада $\mathcal{L}$ има горње ограничење у $\mathcal{F}$ и то је пресликавање

$$\nu : \bigcup_{\mu \in \mathcal{F}} L_\mu \to K$$

задато са: ако је $a \in L_\mu$, тада је $\nu(a) = \mu(a)$. Заиста, $\bigcup_{\mu \in \mathcal{F}} L_\mu$ је поље (проверите!), а како је $\mathcal{L}$ ланац ν је добро дефинисано и на основу дефиниције важи $\mu \subseteq \nu$ за свако $\mu \in \mathcal{L}$.

На основу Цорнове леме $\mathcal{L}$ има максимални елемент, нека је то $\lambda' : L' \to K$. Докажимо да је $L' = L$, чиме ће доказ бити завршен.

Претпоставимо супротно. Тада постоји неки елемент $\alpha \in L \setminus L'$. Како је L алгебарско раширење поља F, то је α алгебарски елемент над F, па самим тим и над пољем L'. Нека је $f \in L'[X]$ минимални полином за α над L'. Како је λ' утапање, то је слика L' при λ', тј. $L'' = \lambda' L'$, изоморфна са L', па како је f нерастављив и њему одговарајући полином g при пресликавању λ' је такође нерастављив (ако је $f = \sum c_i X^i$, тада је $g = \sum \lambda'(c_i) X^i$ полином који му одговара). Поље K је алгебарски затворено, па g има нулу β у K. При томе важи $L'(\alpha) \cong L''(\beta)$ и постоји изоморфизам који проширује λ' (погледати Кронекерову конструкцију и доказ о јединствености коренског поља). Како је λ' максимални елемент из $\mathcal{F}$ ово је могуће једино ако је $L'(\alpha) = L'$, што је контрадикција. Дакле, $L' = L$, па можемо узети да је $\lambda = \lambda'$. □

У претходном тврђењу имали смо претпоставке да је $F \subseteq L$ и $E \subseteq K$. Оне су дате из техничких разлога и могу се лако изоставити као што ћемо видети у наредном тврђењу.

Последица 2.3 Нека су $\theta : F \to E$, $\tau : F \to L$ и $\sigma : E \to K$ утапања. Ако је уз то L алгебарско раширење поља F, а K алгебарски затворено поље, тада постоји утапање $\lambda : L \to K$ такво да је $\lambda\tau = \sigma\theta$ (тј. дијаграм са десне стране комутира).

$$\begin{array}{ccc} L & \overset{\lambda}{\dashrightarrow} & K \\ {\scriptstyle\tau}\uparrow & & \uparrow{\scriptstyle\sigma} \\ F & \xrightarrow{\theta} & E \end{array}$$

Доказ. Нека су $\tau' : F \to \tau F$ и $\sigma' : E \to \sigma E$ пресликавања индукована са τ и σ (дакле, $\tau'(a) = \tau(a)$ за све $a \in F$ и $\sigma'(b) = \sigma(b)$ за све $b \in E$). Јасно, σ' и τ' су изоморфизми, $\theta' = \sigma'\theta\tau'^{-1} : \tau F \to \sigma E$ је утапање, те $\tau F \subseteq L$ и $\sigma E \subseteq K$. По претходном тврђењу постоји утапање $\lambda : L \to K$ које проширује θ' и при томе за све $a \in F$ важи

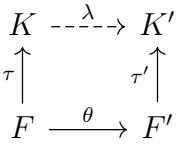
$$\begin{array}{ccc} L & \overset{\lambda}{\dashrightarrow} & K \\ {\scriptstyle\iota}\uparrow & & \uparrow{\scriptstyle\iota} \\ \tau F & \xrightarrow{\theta'} & \sigma E \\ {\scriptstyle\tau'}\uparrow & & \uparrow{\scriptstyle\sigma'} \\ F & \xrightarrow{\theta} & E \end{array}$$

$$\lambda\tau(a) = \lambda(\tau'(a)) = \theta'(\tau'(a)) = \sigma'(\theta(a)) = \sigma\theta(a),$$

чиме је доказ завршен. □

Приметимо да ако у претходној последици узмемо да је $E = F$, $\theta = \mathrm{id}_F$ и L произвољно алгебарско раширење поља F, закључујемо да је K раширење поља L. Коначно, имамо следећу теорему.

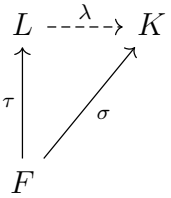
Теорема 2.4 Нека је $\theta : F \to F'$ изоморфизам поља, а K и K' алгебарска затворења поља F и F', редом. Тада постоји изоморфизам $\lambda : K \to K'$ који проширује θ (тј. дијаграм са десне стране комутира).



Доказ. Нека су $\tau : F \to K$ и $\tau' : F' \to K'$ одговарајућа утапања. По претходној последици постоји утапање $\lambda : K \to K'$ такво да је $\tau'\theta = \lambda\tau$. Ако уместо θ узмемо θ^{-1} добијамо да постоји утапање $\lambda' : K' \to K$, такво да је $\lambda'\tau' = \tau\theta^{-1}$. Дакле, $\widetilde{\lambda} := \lambda\lambda' : K' \to K'$ је утапање такво да је $\widetilde{\lambda}\tau' = \lambda\lambda'\tau' = \lambda\tau\theta^{-1} = \tau'\theta\theta^{-1} = \tau'$, тј. $\widetilde{\lambda}$ је идентитета на $\tau'F' \subseteq K'$.

Довољно је доказати да је $\widetilde{\lambda}$ сурјективно (јер ће тада такво бити и λ). Како је $\widetilde{\lambda}K' \cong K'$, то је и $\widetilde{\lambda}K'$ алгебарски затворено поље. Коначно, свако $\beta \in K'$ је алгебарско над F' (прецизније $\tau'F'$), а $\tau'F' \subseteq \widetilde{\lambda}K'$, па је β алгебарски над $\widetilde{\lambda}K'$, а самим тим и садржано у $\widetilde{\lambda}K'$. Дакле, $\widetilde{\lambda}K' = K'$, чиме је доказ завршен. □

Нека је L алгебарско раширење поља F и $\tau : F \to L$ одговарајуће утапање. Посматрајмо неко алгебарско затворење K поља E и одговарајуће утапање $\sigma : F \to K$. По последици 2.3 (примењеној на $E = F$ и $\theta = \mathrm{id}_F$) постоји утапање $\lambda : L \to K$ такво да је $\lambda\tau = \sigma$. Питање је шта можемо рећи о броју оваквих утапања. Означимо зато (за дате F, L и τ) са $\mathcal{F}_{\sigma,K}$ скуп свих оваквих утапања λ (или $\mathcal{F}^L_{\sigma,K}$, када је неопходно).



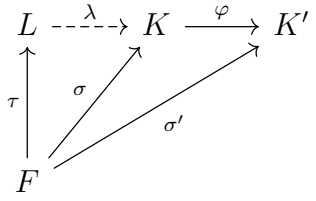
Тврђење 2.5 Нека је L алгебарско раширење поља K и $\tau : F \to L$ одговарајуће утапање. Ако су K и K' алгебарска затворења поља F и $\sigma : F \to K$ и $\sigma' : F \to K'$ одговарајућа утапања, тада постоји бијекција између $\mathcal{F}_{\sigma,K}$ и $\mathcal{F}_{\sigma',K'}$.

Доказ. По теореми 2.4 (примењеној за $E = F$ и $\theta = \mathrm{id}_F$) постоји изоморфизам $\varphi : K \to K'$ такав да је $\sigma' = \varphi\sigma$.

Дефинишимо пресликавање $\Phi : \mathcal{F}_{\sigma,K} \to \mathcal{F}_{\sigma',K'}$ са $\Phi(\lambda) = \varphi\lambda$. Тада је Φ добро дефинисано, јер важи

$$\Phi(\lambda)\tau = \varphi\lambda\tau = \varphi\sigma = \sigma'.$$

Како је φ изоморфизам, то је Φ „1-1”, а уз то за $\lambda' \in \mathcal{F}_{\sigma',K'}$ важи $\varphi^{-1}\lambda' \in \mathcal{F}_{\sigma,K}$ и $\Phi(\varphi^{-1}\lambda') = \lambda'$, па је Φ и „на”.



Претходно тврђење нам омогућује да уведемо следећу дефиницију.

Дефиниција 2.6 Нека је E алгебарско раширење поља F, $\overline{E}$ неко алгебарско затворење поља F и $\sigma : F \to \overline{E}$ утапање. *Сепарабилни степен* поља E над F дефинишемо са

$$[E : F]_s := |\mathcal{F}_{\sigma,\overline{E}}|.$$

Сепарабилни степен је (логично) у вези са сепарабилним проширењима. Пре него што успоставимо ову везу даћемо неколико особина сепарабилног степена.

Тврђење 2.7 Нека је $F \leqslant E \leqslant K$, при чему је E алгебарско раширење поља F, а K алгебарско раширење поља E. Тада важи

$$[K : F]_s = [K : E]_s \cdot [E : F]_s.$$

Доказ. Нека су $\tau : F \to E$, $\tau' : E \to K$ и $\sigma : F \to \overline{F}$ одговарајућа утапања ($\overline{F}$ је алгебарско затворење поља F). По последици 2.3 постоји утапање $\sigma' : E \to \overline{F}$ такво да је $\sigma'\tau = \sigma$. Уз то, скуп свих оваквих утапања је $A := \mathcal{F}^E_{\sigma,\overline{F}}$. Даље, за свако утапање $\sigma' \in \mathcal{F}^E_{\sigma,\overline{F}}$, поново на основу последице 2.3 постоји утапање $\lambda : K \to \overline{F}$ такво да је $\lambda\tau' = \sigma'$. Јасно, тада је $\lambda \in \mathcal{F}^K_{\sigma,\overline{F}}$ (где је $\tau'' = \tau'\tau$ одговарајуће утапање $F \to K$), јер је $\lambda\tau'\tau = \sigma'\tau = \sigma$. Из једнакости $\lambda\tau' = \sigma'$ одмах следи и да су за два различита одабира $\sigma' \in \mathcal{F}^E_{\sigma,\overline{F}}$ одговарајућа пресликавања λ различита. Такође, по последици 2.5, за свако $\sigma' \in \mathcal{F}^E_{\sigma,\overline{F}}$ скуп $\mathcal{F}_{\sigma',\overline{F}}$ има кардиналност $[K : E]_s$. Нека је B један скуп те кардиналности. Следи:

$$[K : F]_s = |\mathcal{F}^K_{\sigma,\overline{F}}| \geqslant |B \times A| = [K : E]_s \cdot [E : F]_s.$$

Са друге стране, ако је $\lambda \in \mathcal{F}^K_{\sigma,\overline{F}}$, тада можемо дефинисати утапање $\sigma' = \lambda\tau' \in \mathcal{F}^E_{\sigma,\overline{F}}$ и важи $\lambda \in \mathcal{F}_{\sigma',\overline{F}}$, па имамо „1-1" пресликавање из $\mathcal{F}^K_{\sigma,\overline{F}}$ у $B \times A$ (јер је за свако σ' скуп $\mathcal{F}_{\sigma',\overline{F}}$ у бијекцији са B). Одавде одмах следи $[K : F]_s \leqslant |B \times A|$, чиме је доказ завршен. □

Код коначних проширења сепарабилни степен није већи од степена проширења, а од посебног је интереса када важи једнакост.

Тврђење 2.8 Нека је E коначно раширење поља E. Тада је $[E : F]_s \leqslant [E : F]$. Уз то, једнакост важи ако и само ако је E сепарабилно раширење поља F.

Доказ. Претпоставимо да је $F \subseteq E$ (доказ се изводи слично и у општем случају, само је запис компликованији). Како је E коначно раширење поља F, то постоје $\alpha_1, \ldots, \alpha_k \in E$ такви да је $E = F(\alpha_1, \ldots, \alpha_k)$ (заиста, можемо бирати $\alpha_{i+1} \in E \setminus F(\alpha_1, \ldots, \alpha_i)$ све док је то могуће, а овај процес ће се завршити јер је E коначно раширење поља F). Како по тврђењу 2.7 важи

$$[E : F]_s = [F(\alpha_1, \ldots, \alpha_k) : F(\alpha_1, \ldots, \alpha_{k-1})]_s \cdots [F(\alpha_1) : F]_s,$$

а по ланчастом правилу

$$[E : F] = [F(\alpha_1, \ldots, \alpha_k) : F(\alpha_1, \ldots, \alpha_{k-1})] \cdots [F(\alpha_1) : F],$$

то је довољно доказати да $[E : F]_s \leqslant [E : F]$ важи у случају када је E просто раширење поља F, тј. када је $E = F(\alpha)$ за неки алгебарски над F елемент α.

Нека је зато $\iota : F \to F(\alpha)$ инклузија и $\sigma : F \to \overline{F}$ утапања. Свако утапање $\lambda : F(\alpha) \to \overline{F}$ такво да важи $\lambda\iota = \sigma$ је у потпуности одређено са $\lambda(\alpha)$. Даље, α је алгебарски над F, па можемо посматрати његов минимални полином $\mu \in F[X]$. Са претходних курсева знамо да је μ нерастављив и да је $[F(\alpha) : F] = \deg \mu$. Нека је $\overline{\mu}$ полином који одговара полиному μ при пресликавању σ. Како је σ утапање, то је $F \cong \sigma F$, па је и полином $\overline{\mu}$ нерастављив над σF. Како је $\lambda(c) = \sigma(c)$ за $c \in F$, то је $\overline{\mu}(\lambda(\alpha)) = \lambda(\mu(\alpha)) = 0$, па је $\lambda(\alpha)$ нула полинома $\overline{\mu}$. Дакле, могућности за $\lambda(\alpha)$ има не више него нула полинома $\overline{\mu}$, а знамо да је њих не више од $\deg \overline{\mu}$, па је $[F(\alpha) : F]_s \leqslant \deg \mu = [F(\alpha) : F]$, чиме је доказ првог дела тврђења завршен.

Докажимо и други део. Претпоставимо прво да важи једнакост $[E : F]_s = [E : F]$ и докажимо да је тада E сепарабилно раширење поља F, тј. да је минимални полином μ произвољног елемента $\alpha \in E$ сепарабилан. Поступамо као у првом делу доказа. Наиме, узимајући за α_1 баш α, закључујемо да је $[F(\alpha) : F]_s = [F(\alpha) : F] = \deg(\mu)$, те да, по претходном делу, μ има $\deg \mu$ нула, што доказује да је сепарабилан.

Коначно, нека је E сепарабилно раширење поља F и нека је $E = F(\alpha_1, \ldots, \alpha_k)$ (што изводимо као у првом делу доказа). Тада по теореми 31 из скрипти *Алгебра 3* (проф. Петровић) закључујемо да је $E = F(\alpha)$ за неко $\alpha \in E$. Нека је μ минимални полином елемента $\alpha \in F[X]$. Он је сепарабилан, па у $\overline{F}$ има $n := \deg(\mu)$ различитих нула $\alpha^{(1)}, \ldots, \alpha^{(n)}$. Тада, по Кронекеровој конструкцији, имамо изоморфизме $\lambda_i : F(\alpha) \to F(\alpha^{(i)})$ такве да је $\lambda_i(\alpha) = \alpha^{(i)}$, па на овај начин добијамо n утапања из $F(\alpha)$ у $\overline{F}$. Дакле, $[F(\alpha) : F]_s \geqslant n = [F(\alpha) : F] \geqslant [F(\alpha) : F]_s$, па важи једнакост и доказ је завршен. □

Коначно, у следећем тврђењу дајемо везу појмова које смо разматрали у овом тексту са нормалним проширењима.

Теорема 2.9 Нека је $F \subseteq E \subseteq \overline{F}$, при чему је E алгебарско раширење, а $\overline{F}$ алгебарско затворење поља F. Тада је E нормално раширење поља F ако и само ако свако утапање $\sigma : E \to \overline{F}$, такво да је $\sigma(c) = c$ за $c \in F$, индукује аутоморфизам поља E.

Доказ. Претпоставимо прво да је E нормално раширење поља F и нека је $\sigma : E \to \overline{F}$ утапање такво да је $\sigma(c) = c$ за $c \in F$. Приметимо следеће: ако је $p \in F[X]$ и $p = (X - \alpha_1) \cdots (X - \alpha_n)$ за неке $\alpha_i \in E$, тада при пресликавању

σ полиному p одговара исти тај полином, па коришћењем Вијетових правила закључујемо да је

$$\sum_{i_1<\cdots<i_k} \sigma(\alpha_{i_1})\cdots\sigma(\alpha_{i_k}) = \sigma\left(\sum_{i_1<\cdots<i_k} \alpha_{i_1}\cdots\alpha_{i_k}\right) = \sum_{i_1<\cdots<i_k} \alpha_{i_1}\cdots\alpha_{i_k}$$

те је $p = (X-\sigma(\alpha_1))\cdots(X-\sigma(\alpha_n))$. Из једнозначности факторизације у $F[X]$ закључујемо да елементи $\sigma(\alpha_i)$ чине пермутацију елемената α_i.

Докажимо сада да за свако $\alpha \in E$ важи $\sigma(\alpha) \in E$. Нека је $\mu \in F[X]$ минимални полином за α. Тада је по претходном $\sigma(\alpha)$ нула полинома μ, па како је E нормално раширење поља E важи $\sigma(\alpha) \in E$. Дакле, $\sigma E \subseteq E$, па је довољно доказати да важи једнакост. Нека је зато $\beta \in E$. Како је E нормално раширење поља F, то постоји полином $p \in F[X]$ такав да је $p(\beta) = 0$ и уз то се p разлаже на линеарне факторе у $E[X]$. По примедби са почетка доказа, тада је $\beta = \sigma(\gamma)$ за неку нулу $\gamma \in E$ овог полинома, па је заиста $\beta \in \sigma E$.

Докажимо и обрнуту импликацију, тј. да је тада E нормално раширење поља F. Нека је зато $p \in F[X]$ нерастављив полином и $\alpha \in E$ његова нула. Докажимо да се свака нула β (која је у $\overline{F}$) полинома p налази у E. По Кронекеровој конструкцији постоји изоморфизам $\theta : F(\alpha) \to F(\beta)$ такав да је $\theta(\alpha) = \beta$ и $\theta(c) = c$ за све $c \in F$. По последици 2.3, постоји утапање $\lambda : E \to \overline{F}$ које продужује θ, па важи $\lambda(\alpha) = \beta$. Како по претпоставци λ индукује аутоморфизам на E, то је $\beta \in E$. □