Algebarska proširenja polja

Borovec, Elizabeta

Master's thesis / Diplomski rad

2015

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:217:571422

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-28**

Repository / Repozitorij:

Repository of the Faculty of Science - University of Zagreb

zir.nsk.hr

DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Elizabeta Borovec

ALGEBARSKA PROŠIRENJA POLJA

Diplomski rad

Voditelj rada:
prof. dr. sc. Dražen Adamović

Zagreb, rujan, 2015.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Posvećujem majci i ocu koji su mi omogućili studiranje, te im zahvaljujem na pruženoj potpori i strpljenju.

Posebna zahvala prof. dr. sc. Draženu Adamoviću na korisnim savjetima i pruženoj pomoći prilikom izrade diplomskog rada.

Sadržaj

Sadržaj **iv**

Uvod **3**

1 Osnovno o poljima **4**

1.1 Uvodne definicije 4

2 Proširenja polja **10**

2.1 Proširenja polja 10

2.2 Algebarska proširenja polja 15

3 Algebarsko zatvorenje **23**

3.1 Polje cijepanja 23

3.2 Algebarsko zatvorenje 28

4 Konačna polja **37**

4.1 Prosta potpolja 37

4.2 Konačna polja 38

Bibliografija **44**

Uvod

Algebra je jedna od osnovnih grana matematike koja se bavi proučavanjem algebarskih struktura i operacija. Strukturu imaju skupovi na kojima je definirana barem jedna operacija. Stoga je algebarska struktura skup na kojem je definirana barem jedna operacija. Neke od osnovnih algebarskih strukutra su: grupe, prsteni, ideali, polja, matrice i algebre. Na njima su definirane algebarske operacije, kao što su naprimjer zbrajanje i množenje.
Cilj ovog diplomskog rada je upoznavanje algebarskih proširenja polja i proučavanje njihovih svojstava. Pokušat ćemo iznijeti osnovne rezultate o konačnim i algebarskim proširenjima polja te o algebarskim zatvorenjima i konačnim poljima.
U prvom poglavlju definiramo pojmove koji su nam potrebni za proučavanje algebarskih proširenja polja. Navodimo definicije prstena, ideala, integralne domene i polja te navodimo nekoliko primjera prstena i polja. Definiramo pojam polinoma i stupnja polinoma te definiramo pojam ireducibilnog polinoma. Na kraju ovog poglavlja definiramo homomorfizam prstena i navodimo jedan od fundamentalnih rezultata o homomorfizmima prstena.
Na početku drugog poglavlja definiramo proširenje polja:

Definicija 2.1.1. *Neka je K polje koje sadrži potpolje k. Polje K tada zovemo* ***proširenje polja*** *k i označavamo sa K/k.*

Navodimo nekoliko rezultata koji su nam potrebni za daljnje proučavanje algebarskih proširenja. Zatim definiramo kada je element proširenja polja algebarski, a kada transcendentan te kada je proširenje polja algebarsko.

Definicija 2.2.1 *Neka je K/k proširenje polja. Kažemo da je element $\alpha \in K$ algebarski nad k ako postoji neki nenul polinom $f(x) \in k[x]$ čiji je korijen α. Inače, za α kažemo da je transcendentan nad k. Za proširenje K/k kažemo da je algebarsko ako je svaki $\alpha \in K$ algebarski nad k.*

U **propoziciji 2.2.2.** pokazujemo da ako je K/k konačno proširenje polja, tada je ono i algebarsko proširenje polja. Definiramo minimalni polinom i pokazujemo da postoji jedinstveni ireducibilni normirani polinom u $\mathbb{Q}[x]$ čiji je korijen algebarski cijeli broj α. Dokazujemo i sljedeći teorem:

Teorem 2.2.4.

(i) *Ako je K/k proširenje polja i $\alpha \in K$ je algebarski nad k, tada postoji jedinstveni ireducibilni normirani polinom $p(x) \in k[x]$ čiji je korijen α. Osim toga, ako $I = (p(x))$, tada $k[x]/I \cong k(\alpha)$. To znači da postoji izomorfizam $\varphi : k[x]/I \to k(\alpha)$ definiran s $\varphi(x + I) = \alpha$ i $\varphi(c + I) = c, \forall c \in k$.*

(ii) *Ako je $a' \in K$ drugi korijen od $p(x)$, tada postoji izomorfizam $\theta : k(\alpha) \to k(\alpha')$ definiran s $\theta(\alpha) = \alpha'$ i $\theta(c) = c, \forall c \in k$.*

Na kraju poglavlja dokazujemo teorem koji nam govori o stupnju konačnog proširenja polja K/k:

Teorem 2.2.8 *Neka su $k \subseteq E \subseteq K$ polja, pri čemu je E konačno proširenje od k i K konačno proširenje od E. Tada je K konačno proširenje od k i vrijedi:*

$$[K : k] = [K : E][E : k].$$

Treće poglavlje je o algebarski zatvorenim poljima. Na početku poglavlja navodimo jedan važan teorem, Kroneckerov teorem:

Teorem 3.1.1. *Neka je k polje i $f(x) \in k[x]$. Postoji polje K čije je potpolje k, a $f(x)$ je produkt linearnih polinoma u $K[x]$.*

Uvodimo pojam polje cijepanja te navodimo primjere u kojima vidimo da polje cijepanja nekog polinoma ovisi o odabranom polju, ali i o polinomu. Iskazujemo definiciju algebarski zatvorenog polja i algebarskog zatvarača polja:

Definicija 3.2.1. *Polje K nazivamo **algebarski zatvoreno** ako svaki nekonstantni polinom $f(x) \in K[x]$ ima korijen u K. **Algebarski zatvarač polja** k je algebarsko proširenje $\overline{k}$ od k koje je algebarski zatvoreno.*

U **teoremu 3.2.5** pokazujemo da algebarski zatvarač $\overline{k}$ od k postoji i dokazujemo da ako je k prebrojivo polje, onda je $\overline{k}$ prebrojiv. U ovom poglavlju definiramo i $k-$preslikavanja:

Definicija 3.2.7. *Neka su F/k i K/k proširenja polja. $k-$preslikavanje je homomorfizam prstenova $\varphi : F \to K$ koji fiksira sve elemente od k.*

Na kraju ovog poglavlja dokazujemo važan rezultat o izomorfizmu između dva algebarska zatvarača:

Teorem 3.2.13. *Bilo koja dva algebarska zatvarača polja k su izomorfna s obzirom na $k-$preslikavanje.*

U posljednjem, četvrtom poglavlju, proučavamo konačna polja. Na početku definiramo prosto potpolje:

Defincija 4.1.1. *Ako je k polje, tada je presjek svih potpolja od k **prosto potpolje polja** k.*

Dokazujemo da je prosto potpolje polja k izomorfno s $\mathbb{Q}$ ili F_p. Nakon toga definiramo konačno polje i definiramo karakteristiku polja u ovisnosti o njegovom prostom potpolju. Dokazujemo sljedeću propoziciju:

Propozicija 4.2.4 *Ako je k konačno polje, tada je $|k| = p^n$ za neki prosti broj p i neki $n \geqslant 1$.*

Kao važan teorem za konačna polja, pojavljuje se Galoisov teorem:

Teorem 4.2.5 *Ako je p prost i n pozitivan cijeli broj, tada postoji polje koje sadrži točno p^n elemenata.*

Na samom kraju ovog poglavlja dokazujemo Mooreov korolar:

Korolar 4.2.10 *Bilo koja dva konačna polja s p^n elementa su izomorfna.*

Poglavlje 1

Osnovno o poljima

U ovom poglavlju definiramo pojmove koji su nam važni za kasnije proučavanje proširenja polja. Navodimo definicije osnovnih algebarskih struktura: prstena, ideala, integralne domene i polja. Osim toga, definiramo polinome pomoću nizova te definiramo ireducibilni polinom. Na kraju poglavlja iskazujemo dva važna teorema, Teorem o dijeljenju s ostatkom i Prvi teorem o izomorfizmu.

1.1 Uvodne definicije

U ovom poglavlju koristimo oznake R za prsten $(R, +, \cdot)$ te K, k, F i E za polja.

Definicija 1.1.1. *Prsten R je skup na kojem su definirane operacije zbrajanja i množenja tako da vrijedi:*

(i) *R je komutativna grupa s obzirom na zbrajanje;*

(ii) *množenje je asocijativno, tj. $a(bc) = (ab)c, \ \forall a, b, c \in R$;*

(iii) *vrijedi distributivnost množenja prema zbrajanju, tj.*

$$a(b + c) = ab + ac, \ \forall a, b, c \in R;$$

$$(b + c)a = ba + ca, \ \forall a, b, c \in R.$$

Kažemo da je R **prsten s jedinicom** ako postoji jedinični element (kraće: jedinica) $1 \in R$ takav da vrijedi:

$$1 \cdot x = x \cdot 1 = x, \ \forall x \in R.$$

Prsten R je komutativan ako vrijedi $ab = ba$, za sve $a, b \in R$.
U ovom diplomskom radu ćemo uvijek pretpostavljati da svi prstenovi imaju jedinicu.

Definicija 1.1.2. *Podskup $I \subseteq R$ se naziva **ideal** u R ako vrijede sljedeći uvjeti:*

(i) $0 \in I$;

(ii) $a, b \in I \Rightarrow a + b \in I$;

(iii) $a \in I, r \in R \Rightarrow ra \in I$.

Za ideal koristimo oznaku:

$$I \trianglelefteq R.$$

Prsten R i skup $\{0\}$ su uvijek ideali u komutativnom prstenu R. Ako je $I \neq R$ kažemo da je I **pravi ideal**.

Definicija 1.1.3. *Neka su $b_1, b_2, ..., b_n \in R$. Skup svih linearnih kombinacija*

$$I = \{r_1 b_1 + r_2 b_2 + \cdots + r_n b_n : r_i \in R \text{ za sve } i\}$$

se naziva ideal u R.

Koristimo oznaku $I = (b_1, b_2, ..., b_n)$ i kažemo da je I ideal **generiran s** $b_1, b_2, ..., b_n$. Posebno, ako je $n = 1$, tada je:

$$I = (b) = \{rb : r \in R\}$$

također ideal u R. Ideal $I = (b)$, generiran samo jednim elementom naziva se **glavni ideal**.

Definicija 1.1.4. *Komutativan prsten R koji zadovoljava sljedeće:*

(i) $1 \neq 0$*;*

(ii) $\forall a, b, c \in R$*, ako je* $ca = cb$ *i* $c \neq 0$ *onda je* $a = b$*.*

se naziva ***integralna domena*** *(kraće: domena).*

Definicija 1.1.5. *Komutativan prsten F u kojem je* $1 \neq 0$ *i svaki nenul element je invertibilan, tj.* $\exists\, a^{-1}$ *takav da je* $a \cdot a^{-1} = a^{-1} \cdot a = 1$ *naziva se* ***polje****.*

Primjer 1.1.6. *Neki od primjera polja su:* $\mathbb{Q}$*,* $\mathbb{R}$*,* $\mathbb{C}$ *i* $\mathbb{Z}/p\mathbb{Z}$*, za* $p \in \mathbb{N}$ *prost broj.*

Polje $\mathbb{Z}/p\mathbb{Z}$ je prsten ostataka modulo p i to je jedan primjer konačnog polja, o čemu će biti riječi kasnije.

Definicija 1.1.7. *Neka je S potprsten polja K. Ako je S polje, tada kažemo da je S potpolje polja K.*

Vrijedi napomenuti da su sva polja prsteni, ali nisu svi prsteni polja.
U sljedećoj definiciji, iz [2], koristimo oznaku A za komutativan prsten s jedinicom 1.

Definicija 1.1.8. *Neka je A komutativan prsten s jedinicom, neka je* $A[x]$ *skup svih nizova* $f = (a_0, a_1, ..., a_n)$ *iz A takvih da je* $a_i = 0$ *za sve osim za konačno mnogo i. To jest:*

$$f = (a_0, a_1, ..., a_n, 0, 0...)$$

Niz $f = (a_0, a_1, ..., a_n, 0, 0...)$ *nazivamo* ***polinom*** *nad A.*

Neka su $f = (a_0, a_1, ..., a_n)$ i $g = (b_0, b_1, ..., b_n)$. Definiramo operaciju zbrajanja na sljedeći način:

$$f + g = (a_0, a_1, ...) + (b_0, b_1, ...) = (a_0 + b_0, a_1 + b_1, ..., a_n + b_n, ...);$$

te operaciju množenja:

$$fg = (a_0, a_1, ...)(b_0, b_1, ...) = (c_0, c_1, ..., c_n, ...),$$

pri čemu je neki c_i jednak:

$$c_i = \sum_{i=0}^{n} a_{n-i}b_i = a_n b_0 + a_{n-1}b_1 + ... + a_1 b_{n-1} + a_0 b_n.$$

(A[x], +, ·) nazivamo prsten polinoma u varijabli x s koeficijentima iz A.

Nul-polinom definiramo kao:

$$f = (0, 0, 0, ...).$$

U nekom nenul polinomu $f = (a_0, a_1, ..., a_n, 0, ...) \in A[x]$, element $a_n \neq 0$ nazivamo **vodeći koeficijent**. Broj $n \in \mathbb{N}$ nazivamo **stupanj polinoma** i koristimo oznaku:

$$\text{st}(f) := n.$$

Ako je vodeći koeficijent $a_n = 1$ kažemo da je polinom $f \in A[x]$ **normiran**.

Jedinica $1 \in A[x]$ je niz:

$$1 = (1, 0, 0, ...).$$

Varijabla $x \in A[x]$ je niz:

$$x = (0, 1, 0, 0, ...),$$

a njene potencije zapisujemo kao nizove:

$$x^2 = (0, 0, 1, 0, ...),$$

$$x^3 = (0, 0, 0, 1, 0, ...),$$

$$\vdots$$

$$x^n = (0, 0, ..., 1, 0, ...).$$

Sada polinom $f \in A[x]$ možemo zapisati na uobičajeni način:

$$\begin{aligned} f &= (a_0, a_1, a_2, ..., a_n, 0, ...) \\ &= (a_0, 0, ...) + (0, a_1, 0, ...) + \cdots + (0, 0, ..., a_n, 0, ...) \\ &= a_0(1, 0, ...) + a_1(0, 1, 0, ...) + \cdots + a_n(0, 0, ..., 1, 0, ...) \\ &= a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n. \end{aligned}$$

To jest, $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in A[x]$.

Definicija 1.1.9. *Polinom f naziva se **ireducibilan** ako se ne može prikazati kao produkt $f_1 f_2$ dvaju polinoma f_1 i f_2 koji su svaki stupnja barem 1.*

Ireducibilnost polinoma ovisi o polju kojem pripadaju koeficijenti polinoma. Npr. polinom $x^2 - 3$ je ireducibilan ako su koeficijenti iz polja $\mathbb{Z}$, no može se faktorizirati na $(x - \sqrt{3})(x + \sqrt{3})$ ako su koeficijenti iz polja $\mathbb{R}$.

Teorem 1.1.10 (Teorem o dijeljenju s ostatkom)**.** *Neka je k polje i $f(x), g(x) \in k[x]$ polinomi pri čemu je $f(x) \neq 0$. Postoje jedinstveni polinomi $q(x), r(x) \in k[x]$ takvi da vrijedi*

$$g(x) = q(x)f(x) + r(x),$$

pri čemu je ili $r(x) = 0$ ili $\mathrm{st}(r) < \mathrm{st}(f)$.

Dokaz se nalazi u [1] na stranici 102.

Definicija 1.1.11. *Neka su R i S dva prstena (ne nužno komutativna). Preslikavanje $f : R \to S$ naziva se **homomorfizam prstena** ako vrijedi:*

$$f(x + y) = f(x) + f(y), \forall x, y \in R;$$

$$f(xy) = f(x)f(y), \forall x, y \in R;$$

$$f(1) = 1.$$

Homomorfizam f koji je još i injekcija naziva se **monomorfizam**, f koji je i surjekcija zovemo **epimorfizam**, a homomorfizam koji je bijektivan zovemo **izomorfizam**.
Za dva prstena R i S kažemo da su izomorfni ako postoji izomorfizam $f : R \to S$. Koristimo oznaku $R \cong S$.
Kažemo da je $f : K \to L$ homomorfizam polja, ako je to homomorfizam prstena.

Definicija 1.1.12. *Neka je R prsten i pretpostavimo da postoji $m \in \mathbb{N}$ takav da je:*

$$mx = 0, \quad \forall x \in R.$$

*Definiramo **karakteristiku prstena** R sa:*

$$\text{char } R := \text{minimalan takav } m.$$

Ako m ne postoji, kažemo da je R karakteristike nula i pišemo

$$\text{char } R = 0.$$

Na kraju ovog poglavlja, navest ćemo jedan od osnovnih rezultata o homomorfizmima prstena, a čije tvrdnje ćemo koristiti u nekim dokazima:

Teorem 1.1.13. *(Prvi teorem o izomorfizmu)*
Neka je preslikavanje $f : R \to S$ proizvoljan homomorfizam prstena. Tada je $\text{Ker } f \trianglelefteq R$ *ideal,* $\text{Im } f \leqslant S$ *potprsten i vrijedi:*

$$R/\text{Ker } f \cong \text{Im } f.$$

Dokaz se nalazi u [1] na stranici 157.

Poglavlje 2

Proširenja polja

U ovom poglavlju detaljnije proučavamo temu diplomskog rada. Definiramo što je to proširenje polja, a zatim što je to algebarsko proširenje polja i kakvo još proširenje postoji. Nakon toga navodimo rezultate vezane uz algebarska proširenja polja i ireducibilne polinome. Definiramo i minimalni polinom te stupanj proširenja konačnog polja, a na kraju poglavlja navodimo teorem koji pokazuje zašto je stupanj proširenja konačnog polja dobro definiran.

2.1 Proširenja polja

Na početku ovog poglavlja navodimo definiciju proširenja polja i nekoliko propozicija koje su važne u kasnijem dijelu rada.

Definicija 2.1.1. *Neka je K polje koje sadrži potpolje k. Polje K tada zovemo* ***proširenje polja k*** *i označavamo sa K/k.*

Uočimo da je tada K vektorski prostor nad k. Ako je K konačno-dimenzionalni vektorski prostor nad k, tada je proširenje polja K/k konačno proširenje. Dimenziju od K označavamo s $[K : k]$ i zovemo **stupanj** od K/k.

Kasnije ćemo u propoziciji 2.1.4 (v) navesti važan argument za ovakvu definiciju.
Navedimo propoziciju koja nam govori o vezi između ireducibilnog polinoma i kvocijentnih prstenova.

Propozicija 2.1.2. *Neka je k polje i neka je $I = (f(x))$, pri čemu je $f(x)$ nenul polinom iz $k[x]$. Sljedeće tvrdnje su ekvivalentne:*

(i) $f(x)$ *je ireducibilan polinom;*

(ii) $k[x]/I$ *je polje;*

(iii) $k[x]/I$ *je domena.*

Dokaz. Prvo pokažimo da $(i) \Rightarrow (ii)$. Pretpostavimo da je $f(x)$ ireducibilan. Budući da je $I = (f(x))$ pravi ideal, $1 + I \in k[x]/I$ je različito od nule. Ako i za neki proizvoljan $g(x)$ vrijedi da $g(x) + I \in k[x]/I$ različito od nule, tada $g(x) \notin I$, to jest $f \nmid g$. Zaključujemo da su f i g relativno prosti pa postoje polinomi $s, t \in k[x]$ takvi da vrijedi $sg + tf = 1$. Iz toga slijedi $sg - 1 \in I$ te je $1 + I = sg + I = (s + I)(g + I)$. Vidimo da svaki nenul element iz $k[x]/I$ ima inverz pa je $k[x]/I$ polje.
Budući da je svako polje integralna domena, to $(ii) \Rightarrow (iii)$.
Pokažimo sada $(iii) \Rightarrow (i)$. Pretpostavimo da je $k[x]/I$ integralna domena. Ako $f(x)$ nije ireducibilan, znači da ga možemo zapisati kao umnožak linearnih faktora: $f(x) = g(x)h(x) \in k[x]$, pri čemu vrijedi $\mathrm{st}(g) < \mathrm{st}(f)$ i $\mathrm{st}(h) < \mathrm{st}(f)$. Znamo da je nula u $k[x]/I$ oblika $0 + I = I$. Iz toga slijedi, ako je $g + I = I$, tada je $g \in I = (f)$ i $f \mid g$, tj. polinom f dijeli g. Došli smo do kontradikcije jer je $st(g) < st(f)$. Dakle, $g + I \neq I$. Analognim postupkom dobijemo $h + I \neq I$. Međutim, umnožak $(g + I)(h + I) = f + I = I$ je nula u kvocijentnom prstenu, što je u kontradikciji s tvrdnjom da je kvocijentni prsten $k[x]/I$ integralna domena. Pretpostavka nije točna, tj. $f(x)$ je ireducibilan polinom. □

Lema 2.1.3. *Neka je k polje, R nenul prsten, a $f : k \to R$ homomorfizam prstena. Tada je preslikavanje f injekcija.*

Dokaz. Budući da je $f(1) = 1$, to je f netrivijalan. Pogledajmo $\mathrm{Ker}\, f$. $\mathrm{Ker}\, f$ je ideal u polju k pa je zato $\mathrm{Ker}\, f = (0)$. Tvrdnja slijedi. □

Propozicija 2.1.4. *Neka je k polje, neka je $p(x)$ ireducibilan polinom u $k[x]$ stupnja d, $K = k[x]/I$ pri čemu je I=(p(x)) te neka je $\beta = x + I \in K$.*

(i) K je polje i $k' = \{a + I : a \in K\}$ je potpolje od K izomorfno s k. Dakle, ako k' identificiramo s k, tada je k potpolje od K.

(ii) β je korijen od $p(x)$ u K;

(iii) Ako je $g(x) \in k[x]$ i β je korijen od $g(x)$, tada $p(x)|g(x)$ u $k[x]$.

(iv) $p(x)$ je jedinstveni ireducibilni normirani polinom u $k[x]$ čiji je korijen β;

(v) Skup $\{1, \beta, \beta^2, ..., \beta^{d-1}\}$ je baza od K kao vektorskog prostora nad k te je $dim_k(K) = d$.

Dokaz. Pokažimo (*i*). Budući da je $p(x)$ ireducibilan, prema propoziciji 2.1.2 slijedi da je kvocijentni prsten $K = k[x]/I$ polje, a prema lemi 2.1.3 slijedi da je $a \mapsto a + I$ izomorfizam $k \to k'$.

Pokažimo sada (*ii*). Uzmimo proizvoljan polinom $p(x) \in k[x]$. Neka je

$$p(x) = a_0 + a_1 x + \cdots + a_{d-1} x^{d-1} + x^d,$$

$a_i \in k$ za sve i. U $K = k[x]/I$ vrijedi:

$$\begin{aligned} p(\beta) &= (a_0 + I) + (a_1 + I)\beta + \cdots + (1 + I)\beta^d \\ &= (a_0 + I) + (a_1 + I)(x + I) + \cdots + (1 + I)(x + I)^d \\ &= (a_0 + I) + (a_1 x + I) + \cdots + (1x^d + I) \\ &= a_0 + a_1 x + \cdots + x^d + I \\ &= p(x) + I \\ &= I, \end{aligned}$$

jer je $I = (p(x))$. S druge strane, I možemo zapisati kao $I = 0 + I$ te je on nul-element od $K = k[x]/I$. Slijedi da je β korijen od $p(x)$.

Pokažimo tvrdnju (*iii*). Budući da je $p(x)$ ireducibilan, ako $p(x) \nmid g(x)$ u $k[x]$ slijedi da je njihov najveći zajednički djelitelj 1. Stoga, postoje $s(x), t(x) \in k[x]$ takvi da vrijedi $1 = sp + tg$. Znamo da je $k[x] \subseteq K[x]$, pa ovo možemo smatrati relacijom u $K[x]$. Evaluacijom polinoma u β, dolazimo do jednakosti $1 = 0$, a to ne vrijedi.

Dokažimo (*iv*). Uzmimo proizvoljan $h(x) \in k[x]$ ireducibilan normirani polinom čiji je korijen β. Tvrdnja (*iii*) nam govori da $p(x) \mid h(x)$. Budući da je $h(x)$ također ireducibilan, vrijedi $h(x) = cp(x)$ za neku konstantu c. No poznato nam je da su $h(x)$ i $p(x)$ oba polinoma normirani pa slijedi da je $c = 1$, tj. $h(x) = p(x)$.

Pokažimo da vrijedi tvrdnja (*v*). Svaki element iz K je oblika $f(x) + I$, gdje je $f(x) \in k(x)$. Prema Teoremu o dijeljenju s ostatkom (teorem 1.1.10), postoje polinomi $q(x), r(x) \in k[x]$ takvi da je $f = qp + r$ te vrijedi $r(x) = 0$ ili $st(r) < d = st(p)$. Budući da je $f - r = qp \in I$, slijedi da $f(x) + I = r(x) + I$. Neka je $r(x) = b_0 + b_1 x + \cdots + b_{d-1}x^{d-1}$, $b_i \in k\ \forall i$, tada analogno dokazu u (*ii*) slijedi da je

$$r(x) + I = b_0 + b_1\beta + \cdots + b_{d-1}\beta^{d-1}.$$

Iz toga slijedi da $\{1, \beta, \beta^2, ..., \beta^{d-1}\}$ razapinje K.

Sada još treba pokazati jedinstvenost. Pretpostavimo da

$$b_0 + b_1\beta + \cdots + b_{d-1}\beta^{d-1} = c_0 + c_1\beta + \cdots + c_{d-1}\beta^{d-1}.$$

Definiramo $g(x) \in k[x]$ kao $g(x) = \sum_{i=0}^{d-1}(b_i - c_i)x^i$. Ako je $g(x) = 0$, tvrdnja vrijedi i gotovi smo. Ako $g(x) \neq 0$, tada možemo definirati $\mathrm{st}(g)$ i vrijedi $\mathrm{st}(g) < d = \mathrm{st}(p)$. S druge strane, β je korijen od $g(x)$ pa iz (*iii*) slijedi $p(x) \mid g(x)$. Dakle, vrijedilo bi $\mathrm{st}(p) \leqslant \mathrm{st}(g)$, no to je kontradikcija. Zaključujemo da je $\{1, \beta, \beta^2, ..., \beta^{d-1}\}$ baza od K kao vektorskog polja nad poljem k i iz toga slijedi $\dim_k(K) = d$. □

Primjer 2.1.5. *Polinom $x^2 + 1 \in \mathbb{R}[x]$ je ireducibilan. Definiramo kvocijentni skup $K = \mathbb{R}[x]/(x^2 + 1)$. Tada je $K/\mathbb{R}$ proširenje polja stupnja 2. Neka je β korijen polinoma $x^2 + 1$. Slijedi da je $\beta^2 = -1$. Također vrijedi da svaki element iz K možemo prikazati na jedinstveni način kao $a + b\beta$, pri čemu su $a, b \in \mathbb{R}$. Primjetimo da smo ovako zapravo konstruirali skup $\mathbb{C}$.*

Definirajmo sada izomorfizam iz K u $\mathbb{C}$. Razmotrimo preslikavanje $\varphi : \mathbb{R}[x] \to \mathbb{C}$ definirano s $\varphi : f(x) \mapsto f(i)$. Preslikavanje je surjektivno jer $a + ib = \varphi(a + xb) \in \mathrm{Im}\,\varphi$.

Nadalje, jezgra preslikavanja φ je skup svih polinoma iz $\mathbb{R}[x]$ čiji je korijen i, tj: $\mathrm{Ker}\,\varphi = \{f(x) \in \mathbb{R}[x] : f(i) = 0\}$. *Polinom $x^2 + 1 \in \mathrm{Ker}\,\varphi$ pa vrijedi da je $(x^2 + 1) \subseteq \mathrm{Ker}\,\varphi$. S druge strane, ako je polinom $g(x) \in \mathrm{Ker}\,\varphi$, tada je i njegov korijen.*

Slijedi da je $\mathrm{Ker}\,\varphi = (x^2 + 1)$ *pa po Prvom teoremu o izomorfizmu (teorem 1.1.13) vrijedi:*

$$\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}.$$

Budući da smo definirali skup $\mathbb{C}$ kao kvocijentni skup, možemo definirati množenje na sljedeći način:

$$\begin{aligned}(a + ib)(c + id) &= ac + (ad + bc)i + bdi^2 \\ &= ac - bd + (ad + bc)i,\end{aligned}$$

ako i promatramo kao varijablu te nakon sređivanja iskoristimo uvjet $i^2 = 1$.
Općenito, ako je β korijen polinoma $p(x) \in k[x]$, tada u kvocijentnom prstenu $k[x]/(p(x))$ izraz:

$$(b_0 + b_1 x + \cdots + b_{n-1}x^{n-1})(c_0 + c_1 + \cdots + c_{n-1}x^{n-1}),$$

množimo tako da faktore izmnožimo kao polinome u varijabli β te iskoristimo uvjet $p(\beta) = 0$.

2.2 Algebarska proširenja

Definicija 2.2.1. *Neka je K/k proširenje polja. Kažemo da je element $\alpha \in K$ algebarski nad k ako postoji neki nenul polinom $f(x) \in k[x]$ čiji je korijen α. Inače, za α kažemo da je transcendentan nad k. Za proširenje K/k kažemo da je algebarsko ako je svaki $\alpha \in K$ algebarski nad k.*

Kada za neki realan broj kažemo da je transcendentan, podrazumijevamo da je transcendentan nad $\mathbb{Q}$. Npr. e i π su transcendentni brojevi.

Propozicija 2.2.2. *Ako je K/k konačno proširenje polja, tada je K/k algebarsko proširenje.*

Dokaz. Po definiciji konačnog proširenja, slijedi da je $[K : k] = n < \infty$. Niz od $n + 1$ vektora: $1, \alpha, \alpha^2, ..., \alpha^n$ je zavisan ako postoje koeficijenti $c_0, c_1, ..., c_k \in k$, od kojih je bar jedan različit od 0, takvi da vrijedi:

$$\sum c_i a^i = 0.$$

Iz toga slijedi da je polinom $f(x) = \sum c_i a^i$ različit od nulpolinoma te da je α njegov korijen. Dakle, α je algebarski element nad k. □

Definicija 2.2.3. *Ako je K/k proširenje i $\alpha \in K$, tada definiramo $k(\alpha)$ kao presjek svih potpolja od K koja sadrže k i α. Skup $k(\alpha)$ nazivamo potpolje od K dobiveno pridruživanjem α s k.*

Općenito, ako je A podskup od K, definiramo $k(A)$ kao presjek svih potpolja od K koja sadrže $k \cup A$; pri čemu $k(A)$ nazivamo podskup od K dobiven pridruživanjem A s k. Posebno, ako je $A = \{z_1, ..., z_n\}$ konačan podskup, tada možemo pisati $k(A)$ kao $k(z_1, ..., z_n)$. Najmanje potpolje od K koje sadrži k i A je upravo $k(A)$. Ako je B bilo koje potpolje od K koje sadrži k i A, tada $k(A) \subseteq B$.

Teorem 2.2.4.

(i) Ako je K/k proširenje polja i $\alpha \in K$ je algebarski nad k, tada postoji jedinstveni ireducibilni normirani polinom $p(x) \in k[x]$ čiji je korijen α. Osim toga, ako $I = (p(x))$, tada $k[x]/I \cong k(\alpha)$. To znači da postoji izomorfizam $\varphi : k[x]/I \to k(\alpha)$ definiran s $\varphi(x + I) = \alpha$ i $\varphi(c + I) = c, \forall c \in k$.

(ii) Ako je $a' \in K$ drugi korijen od $p(x)$, tada postoji izomorfizam $\theta : k(\alpha) \to k(\alpha')$ definiran s $\theta(\alpha) = \alpha'$ i $\theta(c) = c, \forall c \in k$.

Dokaz. Dokažimo tvrdnju (*i*). Pogledajmo preslikavanje $\varphi : k[x] \to K$ definirano sa $\varphi : f(x) \to f(\alpha)$. Kod takvog preslikavanja, slika $\operatorname{Im}\varphi$ je potprsten od K koji sadrži sve elemente oblika $f(\alpha)$ pri čemu je $f(x) \in k[x]$. Također slijedi da je jezgra $\operatorname{Ker}\varphi$ ideal u $k[x]$ koji sadrži sve $f(x) \in k[x]$ čiji je korijen α. Budući da je svaki ideal u $k[x]$ glavni ideal, za neki normirani polinom $p(x) \in k[x]$ vrijedi da $\operatorname{Ker}\varphi = (p(x))$. No također znamo da je $k[x]/(p(x)) \cong \operatorname{Im}\varphi$, što je integralna domena te po propoziciji 2.1.2 slijedi da je $p(x)$ ireducibilan.

Ta ista propozicija (2.1.2) kaže da je $k[x]/(p(x))$ polje, a prema teoremu 1.1.13 slijedi $k[x]/(p(x)) \cong \operatorname{Im}\varphi$, što znači da je $\operatorname{Im}\varphi$ potpolje od K koje sadrži k i α. Budući da svako potpolje od K koje sadrži k i α mora sadržavati i $\operatorname{Im}\varphi$, imamo $\operatorname{Im}\varphi = k(\alpha)$. Jedinstvenost polinoma $p(x)$ slijedi iz propozicije 2.1.4 (iv).

Dokažimo sada (*ii*). Koristeći slične argumente kao u prvom dijelu dokaza, postoje izomorfizmi $\varphi : k[x]/I \to k(\alpha)$ i $\psi : k[x]/I \to k(\alpha')$ definirani s $\varphi(c + I) = c$ i $\psi(c) = c + I$ za

sve $c \in k$. Štoviše, vrijedi $\varphi : x + I \to \alpha$ i $\psi : x + I \to \alpha'$. Njihova kompozicija $\theta = \psi \cdot \varphi^{-1}$ je traženi izomorfizam. □

Definicija 2.2.5. *Neka je K/k proširenje polja i $\alpha \in K$ algebarski nad k.* ***Minimalni polinom*** *od α nad k je jedinstveni ireducibilni normirani polinom $p(x) \in k[x]$ čiji je korijen α. Koristimo oznaku:*

$$irr(\alpha, k) = p(x).$$

Minimalni polinom ovisi o polju k, tj. nije isti minimalni polinom nad poljem $\mathbb{R}$ i nad poljem $\mathbb{C}$. Npr. $irr(i, \mathbb{R}) = x^2 + 1$, dok je $irr(i, \mathbb{C}) = x - i$.

Pretpostavimo da postoji normirani polinom $f(x) \in \mathbb{Z}[x]$ čiji je korijen α algebarski cijeli broj. Budući da je $\mathbb{Z}[x] \subseteq \mathbb{Q}[x]$, svaki α ima jedinstven minimalni polinom $m(x) = irr(\alpha, \mathbb{Q}) \in \mathbb{Q}[x]$ te je $m(x)$ ireducibilan u $\mathbb{Q}[x]$.
U nastavku navodimo Gaussovu Lemu iz [1] koja govori o faktorizaciji polinoma iz $\mathbb{Q}[x]$ s koeficijentima iz $\mathbb{Z}[x]$.

Lema 2.2.6. *Neka je polinom $f(x) \in \mathbb{Z}[x]$. Ako postoji faktorizacija $f(x) = G(x)H(x) \in \mathbb{Q}[x]$, pri čemu su $\mathrm{st}(G), \mathrm{st}(H) < \mathrm{st}(f)$, tada postoji faktorizacija $f(x) = g(x)h(x) \in \mathbb{Z}[x]$ i vrijedi $\mathrm{st}(g) = \mathrm{st}(G), \mathrm{st}(h) = \mathrm{st}(H)$.*

Dokaz. Neka su n', n'' pozitivni cijeli brojevi takvi da je $g(x) = n'G(x)$ i $h(x) = n''H(x)$. Označimo s n njihov umnožak, tj. $n = n'n''$. Tada imamo:

$$nf(x) = n'G(x)n''H(x) = g(x)h(x) \in \mathbb{Z}[x].$$

Neka je p prosti djelitelj od n. Promotrimo preslikavanje $\mathbb{Z}[x] \to F_p[x]$ koje svakom koeficijentu polinoma iz $\mathbb{Z}[x]$ pridružuje ostatak pri dijeljenju s p. Sada imamo:

$$0 = \overline{g}(x)\overline{h}(x).$$

Budući da je skup F_p polje, slijedi da je $F_p[x]$ integralna domena. Prema tome, jedan od faktora jednak je 0. Pretpostavimo da je $\overline{g}(x) = 0$. Budući da smo djelovali s mod p, to

znači da su svi koeficijenti od $g(x)$ višekratnici od p. Za polinom $g(x)$ vrijedi $g(x) = pg'(x)$, pri čemu su svi koeficijenti od $g'(x)$ iz $\mathbb{Z}$.
Ako je n višekratnik od p, pišemo $n = pm$ i vrijedi

$$pmf(x) = pg'(x)h(x) \in \mathbb{Z}[x].$$

Skratimo jednakost s p te nastavimo kratiti s prostim brojevima dok ne dođemo do faktorizacije $f(x) = g^*(x)h^*(x) \in \mathbb{Z}[x]$. Primjetimo da je $\text{st}(g^*) = \text{st}(g)$ i $\text{st}(h^*) = \text{st}(h)$. □

U dokazu sljedećeg korolara koristimo Gaussovu lemu (lema 2.2.6):

Korolar 2.2.7. *Ako je α algebarski cijeli broj, tada* $\text{irr}(\alpha, \mathbb{Q}) \in \mathbb{Z}[x]$.

Dokaz. Neka je polinom $p(x) \in \mathbb{Z}[x]$ monom najmanjeg stupnja čiji je korijen α. Ako $p(x)$ možemo faktorizirati u $\mathbb{Q}[x]$, tada je $p(x) = G(x) \cdot H[x]$, pri čemu je $\text{st}(G) < \text{st}(p)$ i $\text{st}(H) < \text{st}(p)$. Tada je α korijen od $G(x)$ ili $H(x)$. Prema Gaussovoj lemi, postoji faktorizacija $p(x) = g(x) \cdot h(x)$ u $\mathbb{Z}[x]$ u kojoj je $\text{st}(g) = \text{st}(G)$ i $\text{st}(h) = \text{st}(H)$. Zapravo, postoje racionalni brojevi c i d takvi da $g(x) = c \cdot G(x)$ i $h(x) = d \cdot H(x)$. Ako je a vodeći koeficijent od $g(x)$ i b vodeći koeficijent od $h(x)$, tada mora vrijediti $a \cdot b = 1$ jer je $p(x)$ normirani polinom. Dakle, imamo dva slučaja za a i b: ili je $a = 1 = b$ ili je $a = -1 = b$, za $a, b \in \mathbb{Z}$. U oba slučaja dolazimo do zaključka kako su oba polinoma, $g(x)$ i $h(x)$, normirani. Budući da je α korijen od $g(x)$ ili $h(x)$, dolazimo do kontradikcije s tvrdnjom da je $p(x)$ normirani polinom u $\mathbb{Z}[x]$ najmanjeg stupnja čiji je korijen α. Slijedi da je $p(x) = irr(\alpha, \mathbb{Q})$ jer je to jedinstveni ireducubilni normirani polinom u $\mathbb{Q}[x]$ čiji je korijen α. □

Teorem 2.2.8. *Neka su $k \subseteq E \subseteq K$ polja, pri čemu je E konačno proširenje od k i K konačno proširenje od E. Tada je K konačno proširenje od k i vrijedi:*

$$[K : k] = [K : E][E : k].$$

Dokaz. Uzmimo da je $A = \{a_1, ..., a_n\}$ baza od E nad k i $B = \{b_1, ..., b_m\}$ baza od K nad E. Dovoljno je pokazati da je $X = \{a_i b_j \mid i = 1, ..., n, j = 1, ..., m\}$ baza od K nad k.
Kako bi vidjeli da li X razapinje K, uzmimo $u \in K$. Budući da je B baza od K nad E, postoje skalari $\lambda_j \in E$ takvi da je

$$u = \sum_j \lambda_j b_j.$$

Budući da je A baza od E nad k, postoje skalari $\mu_{ji} \in k$ takvi da

$$\lambda_j = \sum_{i,j} \mu_{ji} a_i.$$

Znači,

$$u = \sum_{i,j} \mu_{ji} a_i b_j,$$

tj. X razapinje K nad k.
Sada još želimo pokazati da je X linearno nezavisan nad k. Pretpostavimo da postoje skalari $\mu_{ji} \in k$ takvi da

$$\sum_{i,j} \mu_{ji} a_i b_j = 0.$$

Definirajmo

$$\lambda_j = \sum_i \mu_{ji} a_i.$$

Slijedi da je $\lambda_j \in E$ i vrijedi

$$\sum_j \lambda_j b_j = 0.$$

Budući da je B linearno nezavisan nad E, slijedi da

$$0 = \lambda_j = \sum_i \mu_{ji} a_i, \forall j.$$

Budući da je i A linearno nezavisan nad k, slijedi da je

$$\mu_{ji} = 0, \forall i, j;$$

što znači da je X linearno nezavisan skup nad k. □

Prije jednog primjera, navedimo teorem koji nam pomaže u traženju racionalnih korijena polinoma:

Teorem 2.2.9. *Ako je $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$, tada je svaki racionalni korijen od $f(x)$ oblika $\frac{b}{c}$, pri čemu $b|a_0$ i $c|a_n$.*
Posebno, ako je $f(x) \in \mathbb{Z}[x]$ normiran, tada je svaki racionalni korijen od $f(x)$ cijeli broj.

Dokaz ovog teorema nalazi se u [1] na stranici 115.

Primjer 2.2.10. *Neka je $f(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$. Ako je β korijen polinoma $f(x)$, tada pomoću formule za općenito rješenje kvadratne jednadžbe:*

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

možemo izračunati β^2:

$$\beta^2 = 5 \pm 2\sqrt{6}.$$

Sada iz jednakosti:

$$a + 2\sqrt{ab} + b = (\sqrt{a} + \sqrt{b})^2,$$

slijedi da je:

$$\beta = \pm(\sqrt{2} + \sqrt{3}).$$

Analogno, iz $a - 2\sqrt{ab} + b = (\sqrt{a} - \sqrt{b})^2$ slijedi da je β:

$$\beta = \pm(\sqrt{2} - \sqrt{3}).$$

Korijeni polinoma $f(x)$ su:

$$\sqrt{2}+\sqrt{3}, \quad -\sqrt{2}-\sqrt{3}, \quad \sqrt{2}-\sqrt{3}, \quad -\sqrt{2}+\sqrt{3}.$$

Budući da su ± 1 jedini mogući racionalni korijeni polinoma $f(x)$, prema teoremu 2.2.9, zapravo smo pokazali da su ova četiri korijena polinoma iracionalni brojevi.

Želimo pokazati da je $f(x)$ ireducibilan u $\mathbb{Q}[x]$. Ako je $g(x)$ kvadratni faktor od $f(x)$ u $\mathbb{Q}[x]$, tada je

$$g(x) = (x - a\sqrt{2} - b\sqrt{3})(x - c\sqrt{2} - d\sqrt{3}),$$

pri čemu su $a, b, c, d \in \{1, -1\}$. Iz gornjeg izraza slijedi:

$$g(x) = x^2 - \left((a+c)\sqrt{2} + (b+d)\sqrt{3}\right)x + 2ac + 3bd + (ad+bc)\sqrt{6}.$$

Broj $(a+c)\sqrt{2} + (b+d)\sqrt{3}$ je racionalan ako i samo ako je $a + c = 0 = b + d$; no iz ovih jednakosti mora biti $ad + bc \neq 0$ pa konstantni član u polinomu $g(x)$ nije racionalan. Zbog toga slijedi $g(x) \neq \mathbb{Q}[x]$ pa je polinom $f(x)$ ireducibilan u $\mathbb{Q}[x]$. Ako je $\beta = \sqrt{2} + \sqrt{3}$, tada je $f(x) = irr(\beta, \mathbb{Q})$.

Promatrajmo polje $E = \mathbb{Q}(\beta) = \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)$. Postoji toranj polja $\mathbb{Q} \subseteq E \subseteq F$, pri čemu je $F = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ te prema teoremu 2.2.8 vrijedi

$$[F : \mathbb{Q}] = [F : E]\,[E : \mathbb{Q}]\,.$$

Budući da je $E = \mathbb{Q}(\beta) = \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)$ i β je korijen ireducibilnog polinoma stupnja 4, $f(x)$, slijedi da je $[E : \mathbb{Q}] = 4$.

S druge strane,

$$[F : \mathbb{Q}] = \left[F : \mathbb{Q}\left(\sqrt{2}\right)\right]\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right].$$

Znamo da je $\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2$ jer je $\sqrt{2}$ korijen ireducibilnog polinoma $x^2 - 2 \in \mathbb{Q}[x]$. Dokažimo da je $\left[F : \mathbb{Q}\left(\sqrt{2}\right)\right] \leqslant 2$. Polje F nastaje pridruživanjem $\sqrt{3}$ k $\mathbb{Q}\left(\sqrt{2}\right)$. Sada imamo dva slučaja:

1° $\sqrt{3} \in \mathbb{Q}\left(\sqrt{2}\right)$ *te je* $\left[F : \mathbb{Q}\left(\sqrt{2}\right)\right] = 1$

2° $x^2 - 3$ *je ireducibilan u* $\mathbb{Q}\left(\sqrt{2}\right)[x]$ *pa je stupanj 2 (zapravo je stupanj točno 2).*

Slijedi da je $[F : \mathbb{Q}] \leqslant 4$ *pa iz jednakosti*

$$[F : \mathbb{Q}] = [F : E][E : \mathbb{Q}],$$

slijedi da je $[F : E] = 1$, *tj.* $F = E$.

Napomenimo da F nastaje iz $\mathbb{Q}$ *pridruživanjem svih korijena od* $f(x)$, *ali također nastaje iz* $\mathbb{Q}$ *pridruživanjem korijena od* $g(x) = (x^2 - 2)(x^2 - 3)$.

Poglavlje 3

Algebarsko zatvorenje

Tema ovog poglavlja su algebarski zatvorena polja. Na početku ovog poglavlja definirat ćemo polje cijepanja i dokazati Kroneckerov teorem te diskutirati njegove posljedice. U nastavku definiramo algebarski zatvoreno polje i algebarski zatvarač polja. Dokazat ćemo jedan od najvažnijih rezultata, a to je da za svako polje k postoji algebarski zatvarač polja k.

3.1 Polje cijepanja

Sljedeći teorem je jedan od važnijih teorema jer nam govori o tome da za bilo koji polinom $f(x)$ možemo pronaći neko veće polje E koje sadrži sve korijene polinoma $f(x)$.

Teorem 3.1.1 (Kronecker)**.** *Neka je k polje i $f(x) \in k[x]$. Postoji polje K čije je potpolje k, a $f(x)$ je produkt linearnih polinoma u $K[x]$.*

Dokaz. Dokaz se provodi indukcijom po $\mathrm{st}(f)$.
Baza. Neka je $\mathrm{st}(f) = 1$, tada je $f(x)$ linearan i možemo odabrati polje $K = k$.
Pretpostavka indukcije. Postoji polje F' koje sadrži potpolje k takvo da je $f(x)$ produkt linearnih polinoma u $F'[x]$.

Korak indukcije. Ako je $st(f) > 1$, faktoriziramo polinom $f(x) = p(x)g(x)$ na način da je $p(x)$ ireducibilan. Tvrdnja (i) iz propozicije 2.1.2 nam govori da postoji polje F koje sadrži k i korijen z polinoma $p(x)$. Stoga, u $F[x]$ postoji $p(x) = (x-z)h(x)$ i $f(x) = (x-z)h(x)g(x)$. Koristeći matematičku indukciju dobivamo da postoji polje K koje sadrži F (pa tako i k), takvo da je $h(x)g(x)$, a s tim i $f(x)$, produkt linearnih faktora u $K[x]$. □

Definicija 3.1.2. *Neka je K/k proširenje polja i $f(x) \in k[x]$ polinom koji nije konstantan. Kažemo da se $f(x)$* ***cijepa*** *nad K ako možemo zapisati $f(x) = \alpha(x-z_1)\cdots(x-z_n)$, pri čemu su $z_1, ..., z_n \in K$, $\alpha \in k$. Proširenje polja E/k nazivamo polje cijepanja $f(x)$ nad k ako se $f(x)$ cijepa nad E, ali se ne cijepa nad nijednim odgovarajućim potpoljem od E.*

Primjer 3.1.3. *Promatrajmo polinom $f(x) = x^2 + 1 \in \mathbb{Q}[x]$. Korijeni ovog polinoma su $x_{1,2} = \pm i$ pa ga možemo zapisati kao $f(x) = (x - i)(x + i)$. To znači da je $f(x)$ produkt linearnih polinoma u $\mathbb{C}[x]$, tj. $f(x)$ se cijepa nad $\mathbb{C}$.*
S druge strane, polje $\mathbb{C}$ nije polje cijepanja $f(x)$ nad $\mathbb{Q}$, već postoje odgovarajuća potpolja od $\mathbb{C}$ koja sadrže polje $\mathbb{Q}$ i sve korijene od $f(x)$. Polje $\mathbb{Q}(i)$ je jedan primjer potpolja od $\mathbb{C}$ koje je polje cijepanja od $f(x)$ nad $\mathbb{Q}$.

Uočimo da polje cijepanja nekog polinoma $g(x) \in k[x]$ ovisi i o polju k i o polinomu $g(x)$. Polje cijepanja polinoma $x^2 + 1$ nad poljem $\mathbb{Q}$ je $\mathbb{Q}(i)$, a nad poljem $\mathbb{R}$ je $\mathbb{R}(i)$, tj. $\mathbb{C}$.

U sljedećem korolaru i njegovom dokazu, možemo vidjeti direktnu primjenu Kroneckerovog teorema.

Korolar 3.1.4. *Ako je k polje i $f(x) \in k[x]$, tada postoji polje cijepanja od $f(x)$ nad k.*

Dokaz. Iz Kroneckerovog teorema (vidi teorem 3.1.1) slijedi da postoji proširenje polja K/k takvo da se $f(x)$ cijepa u $K[x]$, npr. $f(x) = \alpha(x - \alpha_1)\cdots(x - \alpha_n)$. Potpolje $E = k(\alpha_1, ..., \alpha_n)$ od K je polje cijepanja $f(x)$ nad k. □

Primjer 3.1.5. *Neka je k polje i neka je $E = k(y_1, ..., y_n)$ polje racionalnih funkcija, u $n \in \mathbb{N}$ varijabli $y_1, ..., y_n$, nad k. Opći polinom stupnja n nad k definiramo kao:*

$$f(x) = \prod_i (x - y_i) \in E[x],$$

to jest

$$f(x) = (x - y_1)(x - y_2) \cdots (x - y_n).$$

Stavimo $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Tada imamo Viéteove formule:

$$\begin{cases} a_{n-1} = -\sum_i z_i \\ a_{n-2} = \sum_{i<j} z_i z_j \\ a_{n-3} = -\sum_{i<j<k} z_i z_j z_k \\ \vdots \\ a_0 = (-1)^n z_1 z_2 \cdots z_n \end{cases}$$

Sada je $K = k(a_0, ..., a_{n-1})$ polje. Budući da E nastaje iz K pridružujući sve korijene od $f(x)$, tj. sve y, slijedi da je E polje cijepanja od $f(x)$ nad K.

Prije primjera 3.1.9, prisjetimo se nekoliko teorema iz područja grupa i cikličkih grupa. Za početak navedimo Lagrangeov teorem:

Teorem 3.1.6 (Lagrange)**.** *Ako je H podgrupa konačne grupe G, tada je $|H|$ djelitelj od $|G|$.*

Dokaz ovog teorema nalazi se u [1] na stranici 35.

Teorem 3.1.7. *Grupa G reda n je ciklička ako i samo ako za svaki djelitelj d od n, postoji najviše jedna ciklička podgrupa reda d.*

Dokaz ovog teorema nalazi se u [1] na stranici 58.

Teorem 3.1.8. *Neka je k polje. Ako je G konačna podgrupa multiplikativne podgrupe $k^\times$, tada je G ciklička grupa. Posebno, ako je k konačno polje (npr. $k = \mathbb{F}_p$), tada je $k^\times$ ciklička grupa.*

Dokaz. Neka d dijeli $|G|$. Pretpostavimo da postoje dvije podgrupe S i T od G koje su reda d. Tada je $|S \cup T| > d$. No prema Lagrangeovom teoremu, za svaki $a \in S \cup T$ vrijedi $a^d = 1$ stoga je korijen od $x^d - 1$. Budući da polinom $f(x) \in k[x]$ stupnja n ima najviše n korijena u polju k, došli smo do kontradikcije jer ovaj polinom ima više od d korijena u danom polju k. Prema teoremu 3.1.7 slijedi da je G ciklička grupa. □

Primjer 3.1.9. *Neka je $f(x) = x^n - 1 \in k[x]$ za neko polje k. Neka je E/k proširenje polja. Prema teoremu 3.1.8, grupa Γ_n svih $n-$tih korijena jedinice iz E je ciklička grupa: $\Gamma_n = \langle\omega\rangle$, pri čemu je ω primitivan n-ti korijen jedinice. Budući da je svaki $n-$ti korijen jedinice potencija od ω, slijedi da je $k(\omega) = E$ polje cijepanja od $f(x)$.*

Navedimo još jednu propoziciju koja je također posljedica Kroneckerovog teorema.

Propozicija 3.1.10. *Neka je p prost broj, neka je k polje. Ako je $f(x) = x^p - c \in k[x]$ i α je p-ti korijen od c u nekom polju cijepanja, tada je $f(x)$ ireducibilan u $k[x]$ ili c ima $p-$ti korijen u k. U oba slučaja, ako k sadrži $p-$te korijene jedinice, tada je $k(\alpha)$ polje cijepanja od $f(x)$.*

Dokaz. Prema Kroneckerovom teoremu, postoji proširenje polja K/k koje sadrži sve korijene od $f(x)$, to jest K sadrži sve $p-$te korijene od c. Neka je $\alpha^p = c$. Sada svaki takav korijen možemo zapisati u obliku $\omega\alpha$, gdje je ω korijen od $x^p - 1$.
Ako $f(x)$ nije ireducibilan u $k[x]$, tada ga možemo faktorizirati $f(x) = g(x)h(x) \in k[x]$, pri čemu je $g(x)$ nekonstantan polinom za koji vrijedi $d = \mathrm{st}(g) < \mathrm{st}(f) = p$. Konstantni član b polinoma $g(x)$ je, do na predznak, jednak produktu korijena od $f(x)$:

$$\pm b = \alpha^d \omega,$$

gdje je ω i sam $p-$ti korijen jedinice. Slijedi da je:

$$(\pm b)^p = \left(\alpha^d \omega\right)^p = \alpha^{dp} = c^d.$$

Budući da je p prost broj i vrijedi $d < p$, slijedi da su d i p relativno prosti, tj. $(d, p) = 1$. Dakle, postoje cijeli brojevi s i t takvi da je $1 = sd + tp$. Iz toga imamo:

$$c = c^{sd+tp} = c^{sd}c^{tp} = (\pm b)^p sc^{tp} = [(\pm b)^s c^t]^p.$$

Dakle, c ima $p-$ti korijen u k.

Pretpostavimo da je skup Ω, skup svih p-tih korijena jedinice, $\Omega \subseteq k$. Ako je neki $\alpha \in K$, $p-$ti korijen od c, tada iz

$$f(x) = \prod_{\omega \in \Omega} (x - \omega\alpha)$$

zaključujemo da se $f(x)$ cijepa nad K i da je $k(\alpha)$ njegovo polje cijepanja. □

3.2 Algebarsko zatvorenje

U ovom poglavlju dokazat ćemo egzistenciju algebarskog zatvarača polja k. Osim toga, vidjet ćemo i da je algebarski zatvarač prebrojivog polja, također prebrojiv. Definirat ćemo novo preslikavanje, koje nazivamo $k-$ preslikavanje. Kao konačan rezultat, vidjeti ćemo da su svaka dva algebarska zatvarača izomorfna. Za početak, definirajmo algebarski zatvoreno polje:

Definicija 3.2.1. *Polje K nazivamo **algebarski zatvoreno** ako svaki nekonstantni polinom $f(x) \in K[x]$ ima korijen u K. **Algebarski zatvarač** polja k je algebarsko proširenje $\overline{k}$ od k koje je algebarski zatvoreno.*

U propoziciji 2.1.4 dotakli smo se algebarskih proširenja. Sljedeća propozicija nam govori o vezi između konačnih i algebarskih proširenja:

Propozicija 3.2.2. *Neka je K/k proširenje polja. Vrijede sljedeće tvrdnje:*

(i) Neka je $z \in K$. Tada je z algebarski nad k ako i samo ako je $k(z)/k$ konačno proširenje.

(ii) Ako su $z_1, z_2, ..., z_n \in K$ algebarski nad k, tada je $k(z_1, z_2, ..., z_n)/k$ konačno proširenje.

(iii) Neka su $y, z \in K$ algebarski nad k, neka je $y \neq 0$. Slijedi da su $y + z$, yz i y^{-1} također algebarski nad k.

(iv) Definirajmo skup

$$(K/k)_{alg} = \{z \in K | \ z \text{ algebarski nad } k\}.$$

Skup $(K/k)_{alg}$ je potpolje od K.

Dokaz. Dokažimo tvrdnju (i). Prvo ćemo dokazati da iz z algebarski slijedi da je $k(z)/k$ konačno proširenje. Neka je z algebarski. Iz tvrdnje (v) propozicije 2.1.4 slijedi da je $k(z)/k$ konačno proširenje.

Obratno, neka je $k(z)/k$ konačno proširenje. Tada je skup $\{1, z, z^2, ..., z^n\}$ linearno zavisan za neki n. Postoji polinom $f \in k[x]$ takav da je $f(z) = 0$. Slijedi da je z algebarski nad k.
Tvrdnju (*ii*) ćemo dokazati matematičkom indukcijom po n.
Baza: Neka je $n = 1$. Primjetimo da je to slučaj iz tvrdnje (*i*), dakle $k(z)/k$ je konačno proširenje.
Pretpostavka indukcije: Ako su $z_1, z_2, ..., z_n$ algebarski nad k, tada je $k(z_1, z_2, ..., z_n)/k$ konačno proširenje.
Korak indukcije: Neka je

$$k \subseteq k(z_1) \subseteq k(z_1, z_2) \subseteq \cdots \subseteq k(z_1, z_2, ..., z_n) \subseteq k(z_1, ..., z_n)$$

toranj polja. Iz teorema 2.2.4 slijedi da je $[k(z_{n+1}) : k]$ konačan. Označimo sa $d = [k(z_{n+1}) : k]$. Tada je d stupanj normiranog ireducibilnog polinoma iz $k[x]$ čiji je korijen z_{n+1}. Definiramo polje $F = k(z_1, ..., z_n)$. Budući da je z_{n+1} korijen polinoma stupnja d nad poljem k, on zadovoljava i polinom stupnja $d' \leqslant d$ nad poljem F. To jest, vrijedi:

$$d' = [k(z_1, ..., z_{n+1}) : k(z_1, ..., z_n)] = [F(z_{n+1}) : F] \leqslant [k(z_{n+1}) : k] = d.$$

Prema pretpostavci indukcije, $[F : k] = [k(z_1, ...z_n) : k]$ je konačno proširenje pa vrijedi:

$$[k(z_1, ..., z_{n+1}) : k] = [F(z_{n+1}) : k] = [F(z_{n+1}) : F][F : k] \leqslant d[F : k] < \infty.$$

Zaključujemo, $k(z_1, ..., z_{n+1})/k$ je konačno proširenje.
Dokažimo sada tvrdnju (*iii*). Prema tvrdnji (*ii*) slijedi da je $k(y, z)/k$ konačno proširenje. Budući da je potprostor konačno dimenzionalnog vektorskog polja također konačno dimenzionalan, slijedi da su $k(y + z) \subseteq k(y, z)$ i $k(yz) \subseteq k(y, z)$ također konačna proširenja. Iz tvrdnje (*i*) slijedi da su $y + z$, yz i y^{-1} algebarski nad k.
Budući da je $(K/k)_{alg} \subseteq K$ te iz tvrdnje (*iii*) vrijedi da je $(K/k)_{alg}$ polje, slijedi tvrdnja (*iv*). □

Navodimo leme koje ćemo koristiti u dokazu teorema 3.2.5:

Lema 3.2.3. *Neka je k polje i neka je $k[T]$ prsten polinoma u skupu varijabli T. Ako su $t_1, t_2, ..., t_n \in T$ sve različite varijable, a $n \geqslant 2$ i $f_i(t_i) \in k[t_i] \subseteq k[T]$ su polinomi različiti od konstantnog polinoma, tada je ideal $I = (f_1(t_1), ..., f_n(t_n))$ iz $k[T]$ pravi ideal.*

Dokaz. Pretpostavimo da I nije pravi ideal u $k[T]$. Tada postoje $h_i(T) \in k[T]$ takvi da

$$1 = h_1(T)f_1(t_1) + \cdots + h_n(T)f_n(t_n). \tag{3.1}$$

Promatramo proširenje polja $k(\alpha_1, ..., \alpha_n)$ gdje je α_i korijen od $f_i(t_i)$ za $i = 1, ..., n$. Označimo varijable uključene u $h_i(T)$ različite od $t_1, ..., t_n$ s $t_{n+1}, ..., t_m$ (ako postoje). Izračunavajući izraz 3.1 u $t_i = \alpha_i$ za $i \leqslant n$ i $t_i = 0$ za $i \geqslant n + 1$. Dobivamo da je desna strana jednaka 0, a lijeva 1. Došli smo do kontradikcije. Zaključujemo da je I pravi ideal u $k[T]$. □

Lema 3.2.4.

(i) Neka je $k \subseteq K \subseteq E$ toranj polja u pri čemu su E/K i K/k algebarska proširenja. Tada je i proširenje E/k algebarsko.

(ii) Neka je $K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq K_{n+1} \subseteq \cdots$ rastući toranj polja. Ako je K_{n+1}/K_n algebarsko proširenje za sve $n \geqslant 0$, tada je i $K^* = \cup_{n \geqslant 0} K_n$ algebarsko polje nad K_0.

(iii) Neka je $K = k(A)$; to jest, K nastaje pridruživanjem elemenata $a \in A$ (moguće beskonačno mnogo) polju k. Ako je svaki element $a \in A$ algebarski nad k, tada je K/k algebarsko proširenje.

Dokaz. Dokažimo (i). Neka je $e \in E$ proizvoljan element. Budući da je E/K algebarsko proširenje, postoji polinom $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$ čiji je korijen e. Neka je $F = k(a_0, ..., a_n)$. Tada je e algebarski nad F i proširenje $F(e) = k(a_0, ...a_n, e)$ je konačno proširenje od F. To znači da je $[F(e) : F]$ konačan. Budući da je K/k algebarsko

proširenje, jer je svaki a_i algebarski nad k, a iz tvrdnje (*ii*) propozicije 3.2.2 slijedi da je $[F : k]$ konačno, imamo:

$$[k(a_0, ..., a_n, e) : k] = [F(e) : k] = [F(e) : F][F : k] < \infty,$$

to jest, prema tvrdnji (*i*) propozicije 3.2.2, e je algebarski nad k. Zaključujemo da je proširenje E/k algebarsko.

Dokažimo da vrijedi tvrdnja (*ii*). Neka su $y \in K_m$ i $z \in K_n$. Tada su $y, z \in K^*$. Pretpostavimo da je $m \leqslant n$. Stoga imamo $y, z \in K_n \subseteq K^*$. Budući da je K_n polje, ono sadrži $y + z$, yz i y^{-1} za $y \neq 0$. Skup K_n je polje i podskup skupa K^* pa zaključujemo da je i skup K^* polje. Pretpostavimo da je $z \in K^*$. Postoji $n \in \mathbb{N}$ za koji vrijedi $z \in K_n$. Koristeći varijantu tvrdnje (*i*) slijedi da je K_n/K_0 algebarsko proširenje, to jest dobili smo da je z algebarski nad K_0. Budući da je svaki element iz K^* algebarski nad K_0, slijedi da je i proširenje K^*/K_0 algebarsko.

Dokažimo tvrdnju (*iii*). Neka je $z \in k(A)$ proizvoljan element. Neka je $a_1, a_2, ..., a_n \in A$ konačno mnogo elemenata iz A. Slijedi da je $z \in k(a_1, a_2, ..., a_n)$. Prema tvrdnji (*ii*) propozicije 3.2.2 proširenje $k(z)/k$ je konačno pa slijedi da je z algebarski nad k. □

Teorem 3.2.5. *Neka je dano polje k. Tada postoji algebarski zatvarač $\overline{k}$ od k.*

Dokaz. Neka je T skup koji je u bijektivnoj korespodenciji s familijom nekonstantnih polinoma u $k[x]$. Neka je $R = k[T]$ prsten polinoma, te neka je I ideal u R generiran sa svim elementima oblika $f(t_f)$, gdje je $t_f \in T$. To znači da ako je:

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$

pri čemu je $\alpha_i \in k$, tada je:

$$f(t_f) = (t_f)^n + a_{n-1}(t_f)^{n-1} + \cdots + a_0.$$

Želimo pokazati da je ideal I pravi. Pretpostavimo da nije pravi, tada $1 \in I$ pa postoje varijable $t_1, ..., t_n \in T$ i polinomi $h_1(T), ..., h_n(T) \in k[T]$ takvi da

$$1 = h_1(T)f_1(t_1) + \cdots + h_n(T)f_n(t_n),$$

što je u kontradikciji s tvrdnjom leme 3.2.3. Budući da je R prsten polinoma, on ima maksimalni ideal. Budući da je svaki pravi ideal I iz R sadržan u maskimalnom idealu, postoji maksimalan ideal M u R koji sadrži I. Definiramo $K = R/M$. Dokažimo sada nekoliko tvrdnji za K/k koje nam olakšavaju dokaz:

(i) *K/k je poširenje polja.*

M je maksimalan ideal pa slijedi da je $K = R/M$ polje. Neka je $i : k \to k[T]$ preslikavanje prstenova koje elementu $a \in k$ pridružuje konstantan polinom a te neka je θ kompozicija preslikavanja $k \xrightarrow{i} k[T] = R \xrightarrow{nat} R/M = K$. Budući da je k polje, prema lemi 2.1.3 slijedi da je θ injektivno preslikavanje. Možemo identificirati k s $\operatorname{Im}\theta \subseteq K$.

(ii) *Svaki nekonstantni polinom $f(x) \in k[x]$ se cijepa u $K[x]$.*

Postoji $t_f \in T$ takav da je $f(t_f) \in I \subseteq M$ te da je $t_f + M \in R/M = K$ korijen od $f(x)$. Prema aksiomu matematičke indukcije po stupnju polinoma slijedi da se $f(x)$ cijepa nad K.

(iii) *Proširenje K/k je algebarsko.*

Prema tvrdnji (*iii*) iz leme 3.2.4, dovoljno je pokazati da je svaki $t_f + M$ algebarski nad k. Budući da je t_f korijen od $f(x) \in k[x]$ slijedi da je $t_f + M$ algebarski nad k.

Sada nastavljamo s dokazom. Neka je $k_1 = K$ te konstruiramo k_{n+1} iz k_n analogno načinu kako je K konstruiran iz k. Postoji toranj polja

$$k = k_0 \subseteq k_1 \subseteq \cdots \subseteq k_n \subseteq k_{+1} \subseteq \cdots,$$

pri čemu je svako proširenje k_{n+1}/k_n algebarsko i svaki nekonstantan polinom u $k_n[x]$ ima korijen u k_{n+1}. Zbog jednostavnosti zapisa, u dokazu ćemo koristiti oznaku E umjesto $\overline{k}$. Definiramo $E = \bigcup_n k_n$. Prema tvrdnji (ii) iz leme 3.2.4 slijedi da je $E = \bigcup_n k_n$ algebarsko proširenje od k. Želimo pokazati da je E algebarski zatvoreno polje. Ako je $g(x) = \sum_{i=0}^{m} e_i x^i \in E[x]$ nekonstantan polinom, tada on ima konačno mnogo koeficijenata $e_0, ..., e_m$ što znači da postoji neko polje k_q koje ih sve sadrži. Slijedi da je $g(x) \in k_q[x]$ te da $g(x)$ ima korijen u $k_{q+1} \subseteq E$ što smo i trebali pokazati. Zaključujemo, polje E je algebarski zatvarač polja k. □

Korolar 3.2.6. *Neka je k prebrojivo polje. Tada ono ima prebrojiv algebarski zatvarač.*

Posebno, algebarski zatvarači prostih polja $\mathbb{Q}$ i F_p su prebrojivi.

Dokaz. Neka je k prebrojiv. Budući da je $k[x]$ prebrojiv, tada je i skup $T = \{t_1, t_2, ...\}$, skup svih nekonstantnih polinoma, prebrojiv. Stoga, $k[T] = \bigcup_{l \geqslant 1} k[t_1, ..., t_l]$ je prebrojiv, kao i njegov kvocijent k_1 (tu oznaku koristimo u teoremu 3.2.5; također vrijedi da $\bigcup_{n \geqslant 1} k_n$ algebarski zatvarač od k). Koristeći matematičku indukciju po $n \in \mathbb{N}$, slijedi da je svaki k_n prebrojiv. Prebrojiva unija prebrojivih skupova je i sama prebrojiva, dakle i algebarski zatvarač od k je prebrojiv. □

Kroz sljedećih nekoliko lema, pokazat ćemo jedinstvenost algebarskog zatvarača. Definirajmo prvo $k-$ preslikavanje.

Definicija 3.2.7. *Neka su F/k i K/k proširenja polja. $k-$**preslikavanje** je homomorfizam prstenova $\varphi : F \to K$ koji fiksira sve elemente od k.*

Propozicija 3.2.8. *Neka je k polje, polinom $f(x) \in k[x]$ te neka je $E = k(z_1, z_2, ..., z_n)$ polje cijepanja polinoma $f(x)$ nad k. Ako je preslikavanje $\sigma : E \to E$ automorfizam koji fiksira sve elemente od k, tada σ permutira skup svih korijena $\{z_1, z_2, ..., z_n\}$ od $f(x)$.*

Dokaz. Neka je z korijen od $f(x)$. Tada vrijedi:

$$f(x) = z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0.$$

Budući da σ fiksira sve elemente od k, možemo primjeniti σ na gornju jednakost. Slijedi:

$$\begin{aligned} 0 &= \sigma(z)^n + \sigma(a_{n-1})\sigma(z)^{n-1} + \cdot + \sigma(a_1)\sigma(z) + \sigma(a_0) \\ &= \sigma(z)^n + a_{n-1}\sigma(z)^{n-1} + \cdot + a_1\sigma(z) + a_0 \\ &= f\left(\sigma\left(z\right)\right). \end{aligned}$$

Dakle, $\sigma(z)$ je korijen od $f(x)$ pa možemo definirati $\Omega = \{\text{skup svih korijena od } f(x)\}$. Postoji preslikavanje $\sigma|\Omega : \Omega \to \Omega$, pri čemu je $\sigma|\Omega$ restrikcija. Budući da je σ injektivan, tada je i $\sigma|\Omega$ injektivna. Iz toga slijedi da je $\sigma|\Omega$ permutacija od Ω. □

Napomena 3.2.9. *Ako je K/k proširenje polja, $\varphi : K \to K$ $k-$preslikavanje i $f(x) \in k[x]$, tada prema propoziciji 3.2.8 slijedi da φ permutira sve korijene od $f(x)$ koji su iz K.*

Lema 3.2.10. *Ako je K/k algebarsko proširenje, tada je svako $k-$preslikavanje $\varphi : K \to K$ automorfizam od K.*

Dokaz. Budući da je $k-$preslikvanje homomorfizam prstenova, a K polje, prema lemi 2.1.3 slijedi da je $k-$preslikavanje injekcija. Trebamo pokazati da je i surjekcija. Uzmimo proizvoljan $a \in K$. Budući da je K/k algebarsko proširenje, postoji polinom $p(x) \in k[x]$ čiji je korijen a. Definiramo $A = \{\text{skup svih nultočaka od } p(x) \text{ koje leže u } K\}$. Tada $k-$preslikavanje φ permutira skup A. Prema tome, $a \in \varphi(A) \subseteq \operatorname{Im}\varphi$. □

Ponovimo sada:

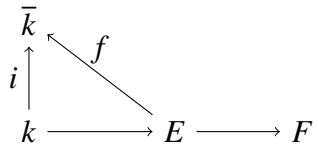
Zornova lema. *Neka je X neprazan, parcijalno uređen skup u kojem svaki niz ima gornju granicu u X. Tada X ima maksimalan element.*

Za neki skup S kažemo da je parcijalno uređen ako postoji relacija $\preceq$ između dva elementa $x, y \in S$, tj. $x \preceq y$, koja je refleksivna, antisimetrična i tranzitivna.

Neka je skup S parcijalno uređen. Za element $m \in S$ kažemo da je **maksimalan** ako ne postoji $x \in S$ takav da je $m \prec x$. Ako vrijedi $m \preceq x$, tada je $m = x$.

Lema 3.2.11. *Neka je k polje i neka je $\overline{k}/k$ algebarski zatvarač. Ako je F/k algebarsko proširenje, tada postoji injektivno $k-$preslikavanje $\psi : F \to \overline{k}$.*

Dokaz. Neka je E međupolje takvo da $k \subseteq E \subseteq F$. Uređeni par (E, f) nazivamo aproksimacija ako je $f : E \to \overline{k}$, $k-$preslikavanje.
U sljedećem dijagramu sve strelice, osim one za f, označavaju ulaganje:



Definiramo skup $X = \{aproksimacije\ (E, f) : k \subseteq E \subseteq F\}$. Skup $X \neq \emptyset$ jer $(k, i) \in X$. Parcijalno uredimo X tako da

$$(E, f) \preceq (E', f'),$$

ako je $E \subseteq E'$ i $f'|E = f$. Restrikcija $f'|E = f$ znači da f' proširuje f, tj. te dvije funkcije se poklapaju za sve elemente iz E: $f'(u) = f(u),\ \forall u \in E$.
Gornja granica niza $S = \{(E_j, f_j) : j \in J\}$ je dana s $\left(\bigcup E_j, \bigcup f_j\right)$. Skup $\bigcup E_j$ je međupolje. Uzmimo neki proizvoljan $u \in \bigcup E_j$. Tada je $u \in E_{j_0}$ za neki j_0.
Definiramo preslikavanje $\Phi : u \mapsto f_{j_0}(u)$, pri čemu je $\Phi = \bigcup f_j$. Provjerimo je li Φ dobro definiran: uzmimo $u \in E_{j_1}$ proizvoljan. Pretpostavimo da je $E_{j_0} \subseteq E_{j_1}$. Budući da f_{j_1} proširuje f_{j_0} slijedi da je $f_{j_1}(u) = f_{j_0}(u)$. Svi f_j su $k-$ preslikavanja pa je i Φ $k-$preslikavanje.
Prema Zornovoj lemi, u X postoji maksimalan element (E_0, f_0). Ako pokažemo da je $E_0 = F$, dokaz je gotov jer tada za ψ možemo uzeti f_0.
Neka je $E_0 \subsetneq F$. Postoji $a \in F$ takav da $a \notin E_0$. Budući da je F/k algebarsko proširenje,

slijedi da je F/E_0 algebarsko, tj. postoji ireducibilan polinom $p(x) \in E_0[x]$ čiji je korijen a. Budući da je $\overline{k}/k$ algebarsko proširenje i da je $\overline{k}$ algebarski zatvoreno polje, postoji faktorizacija polinoma $p(x)$ u $\overline{k}[x]$:

$$f_0^*(p(x)) = \prod_{i=1}^{n} (x - b_i),$$

pri čemu je $f_0^* : E_0[x] \to \overline{k}[x]$ preslikavanje definirano s $f_0^* : e_0 + \cdots + e_n x^n \mapsto f_0(e_0) + \cdots + f_0(e_n)x^n$. Ako svi b_i leže u $f_0(E_0) \subseteq \overline{k}$, tada je $f_0^{-1}(b_i) \in E_0 \subseteq F$ za sve i te postoji faktorizacija od $p(x)$ u $F[x]$. Faktorizacija je dana sa

$$p(x) = \prod_{i=1}^{n} [x - f_0^{-1}(b_i)].$$

S druge strane, $a \notin E_0$ nam govori da $a \neq f_0^{-1}(b_i)$ za bilo koji i. Dakle, $x - a$ je drugi faktor od $p(x)$ u $F[x]$, što je u kontradikciji s jedinstvenošću faktorizacije. Iz toga slijedi da postoji neki $b_i \notin \operatorname{Im} f_0$. Prema tvrdnji (i) iz teorema 2.2.4, definiramo preslikavanje $f_1 : E_0(a) \to \overline{k}$ sa:

$$c_0 + c_1 a + c_2 a^2 + \cdots \mapsto f_0(c_0) + f_0(c_1)b_i + f_0(c_2)b_i^2 + \cdots .$$

Preslikavanje f_1 je dobro definirano $k-$preslikavanje koje proširuje f_0. Stoga, $(E_0, f_0) \prec (E_0(a), f_1)$ je u kontradikciji s maksimalnošću od (E_0, f_0). □

Teorem 3.2.12. *Bilo koja dva algebarska zatvarača polja k su izomorfna s obzirom na $k-$preslikavanje.*

Dokaz. Neka su K i L dva algebarska zatvarača polja k. Prema lemi 3.2.11, postoje $k-$preslikavanja $\psi : K \to L$ i $\theta : L \to K$. Prema tvrdnji leme 3.2.10 slijedi da su obje njihove kompozicije; $\theta\phi : K \to K$ i $\phi\theta : L \to L$ automorfizmi. Zbog toga zaključujemo da su i ϕ i θ, $k-$izomorfizmi. □

Poglavlje 4

Konačna polja

4.1 Prosta potpolja

Na početku ovog poglavlja navodimo definiciju prostog potpolja i propoziciju koja nam govori da je prosto potpolje izomorfno s $\mathbb{Q}$ ili s F_p. Nakon toga definiramo konačna polja i karakteristiku polja. Dokazujemo nekoliko važnih teorema koji se tiču konačnih polja. Na kraju poglavlja pokazujemo da postoji izmorfizam između konačnih polja.

Definicija 4.1.1. *Ako je k polje, tada je presjek svih potpolja od k* ***prosto potpolje*** *polja k.*

Propozicija 4.1.2. *Neka je k polje. Tada je njegovo prosto potpolje izomorfno s $\mathbb{Q}$ ili s F_p, za neki prosti broj p.*

Dokaz. Neka je $\chi : \mathbb{Z} \to k$ homomorfizam prstenova definiran s $\chi(n) = n\varepsilon$, pri čemu ε označava jedinicu u k. Postoji $m \in \mathbb{Z}$ takav da $\mathrm{Ker}\,\chi = (m)$ jer je svaki ideal u $\mathbb{Z}$ glavni.
Ako je $m = 0$, tada je χ injekcija pa postoji izomorfna kopija od $\mathbb{Z}$ koja je potprsten od k. Postoji polje $Q \cong \mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$ čija je slika $\mathrm{Im}\,\chi \subseteq Q \subseteq k$. Budući da je Q potpolje generirano s ε, ono je prosto potpolje od k.

Ako je $m \neq 0$, prema Prvom teoremu o izomorfizmu (vidi teorem 1.1.13), slijedi

$$I_m = \mathbb{Z}/(m) \cong \operatorname{Im}\chi \subseteq k.$$

Budući da je k polje, a $\operatorname{Im}\chi$ je integralna domena, slijedi da je m prost broj. Ako zapišemo p umjesto m, tada je $\operatorname{Im}\chi \cong F_p$ prosto potpolje od k jer je to potpolje generirano s ε. □

4.2 Konačna polja

Do sada smo proučavali polja s obzirom na to jesu li njihova proširenja algebarska ili transcendentna, no polja možemo proučavati i s obzirom na njihovu karakteristiku. Iskažimo prvo definiciju konačnog polja i navedimo primjere.

Definicija 4.2.1. *Konačno polje je polje koje ima konačan broj elemenata.*

Konačna polja se zovu još i **Galoisova polja**. Označavamo ih sa F_p, pri čemu je p neki prost broj. Najmanje konačno polje je F_2 koje se sastoji od dva elementa: 0 i 1, jer po definiciji polje mora imati barem dva različita elementa.

Neka je K polje. **Karakteristika polja** K je najmanji prirodan broj n takav da je

$$1 + 1 + 1 + \cdots + 1 = n \cdot 1 = 0,$$

gdje su 0 i 1 neutralni elementi za zbrajanje, odnosno množenje u polju K.

Definicija 4.2.2. *Kažemo da polje k ima karakteristiku* 0 *ako je njegovo prosto potpolje izomorfno s $\mathbb{Q}$, a karakteristiku p ako je njegovo prosto potpolje izomorfno s F_p za neki prosti broj p.*

Polja $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ imaju karakteristiku 0, dok svako konačno polje ima karakteristiku p, za neki p prost broj. Jedan od primjera konačnog polja s karakteristikom p je $F_p(x)$, prsten svih racionalnih funkcija nad F_p.

Propozicija 4.2.3. *Neka je k polje karakteristike $p > 0$. Ako je $ma = 0$, pri čemu je $m \in \mathbb{Z}$, $a \in k$, tada ili $a = 0$ ili $p \mid m$. Dakle, $pa = 0$ za sve $a \in k$.*

Dokaz. Karakteristika od k je $p > 0$ pa vrijedi $p \cdot 1 = 0$, pri čemu je 1 jedinica u polju k. Stoga, ako je $a = 0$ ili $p \mid m$, slijedi da je $ma = 0$. Obratno, pretpostavimo da je $ma = 0$. Ako $a \neq 0$, tada $0 = m \cdot 1 = maa^{-1}$. Ova jednadžba je u prostom potpolju od k koje je izomorfno s F_p. Zaključujemo $m \equiv 0 \bmod p$, to jest $p \mid m$. □

Propozicija 4.2.4. *Ako je k konačno polje, tada je $|k| = p^n$ za neki prosti broj p i neki $n \geqslant 1$.*

Dokaz. Prema definiciji karakteristike, prosto potpolje od k je izomorfno s F_p za neki prosti broj p. Tako k postaje konačno-dimenzionalni vektorski prostor nad F_p te vrijedi

$$dim_{F_p}(k) = n \Rightarrow |k| = p^n$$

□

Teorem 4.2.5 (Galois)**.** *Ako je p prost i n pozitivan cijeli broj, tada postoji polje koje sadrži točno p^n elemenata.*

Dokaz. Označimo $q = p^n$ te promatrajmo polinom:

$$g(x) = x^q - x \in F_p[x].$$

Prema Kroneckerovom teoremu (teorem 3.1.1), postoji proširenje polja K/F_p u kojem je $g(x)$ produkt linearnih faktora iz $K[x]$. Definiramo skup E kao skup svih korijena od $g(x)$:

$$E = \{\alpha \in K : g(\alpha) = 0\}.$$

Budući da je derivacija $g'(x) = gx^{q-1} - 1 = p^n x^{q-1} - 1 = -1$, vrijedi da je $NZD(g, g') = 1$. Iz toga slijedi da su svi korijeni od $g(x)$ kratnosti 1, tj. E ima točno $q = p^n$ elemenata.

Trebamo još pokazati da je E potpolje od K. Vrijedi da je $1 \in E$. Ako su neki $a, b \in E$, tada je $a^q = a$ i $b^q = b$. Iz toga slijedi $(ab)^q = a^q b^q = ab$ i $ab \in E$. Također vrijedi $(a-b)^q = a^q - b^q = a - b$, to jest i $a - b \in E$. U slučaju da je $a \neq 0$, možemo izraz $a^q = a$ skratiti s a pa imamo $a^{q-1} = 1$ iz čega slijedi da je inverz od a jednak a^{q-2}. Inverz od a leži u E jer je E zatvoren na množenje. Zaključujemo da je E potpolje od K. Ovim je dokaz završen. □

Korolar 4.2.6. *Za svaki prosti broj p i svaki cijeli broj $n \geqslant 1$ postoji ireducibilni polinom $g(x) \in F_p[x]$ stupnja n. Zapravo, ako je α prosti element od F_{p^n}, tada je njegov minimalni polinom $g(x) = irr(\alpha, F_p)$ stupnja n.*

Dokaz. Neka je E/F_p proširenje polja s p^n elemenata, te neka je $\alpha \in E$. Polje $F_p(\alpha)$ sadrži svaki nenul element od E, tj. svaku potenciju od α, pa vrijedi $F_p(\alpha) = E$. Prema tvrdnji (i) teorema 2.2.4, slijedi da je $g(x) = irr(\alpha, F_p) \in F[x]$ ireducibilan polinom čiji je korijen α. Ako je $\mathrm{st}(g) = d$, tada prema tvrdnji (v) propozicije 2.1.4, slijedi da je $[F_p[x]/g(x) : F_p] = d$; no prema teoremu 2.2.4 slijedi $F_p[x]/g(x) \cong F_p(\alpha) = E$, to jest $[E : F_p] = n$. Iz toga zaključujemo $n = d$ pa je $g(x)$ ireducibilan polinom stupnja n. □

Primjer 4.2.7.

(i) Konstruirajmo polje koje se sastoji od četiri elementa:

$$\mathbb{F}_4 = \left\{ \begin{bmatrix} a & b \\ b & a+b \end{bmatrix} : a, b \in \mathbb{F}_2 \right\}.$$

S druge strane, možemo konstruirati polje reda 4 kao kvocijent $F = \mathbb{F}_2[x]/(q(x))$, pri čemu je $q(x) \in \mathbb{F}_2[x]$ ireducibilni polinom $x^2 + x + 1$. Prema tvrdnji (v) propozicije 2.1.4, polje F se sastoji od svih $a + b\beta$, pri čemu je $\beta = x + (q(x))$ korijen od $q(x)$, $a, b \in \mathbb{F}_2$. Budući da je $\beta^2 + \beta + 1 = 0$ slijedi da je $\beta^2 = -\beta - 1 = \beta + 1$. Nadalje,

$$\beta^3 = \beta\beta^2 = \beta(\beta + 1) = \beta^2 + \beta = 1.$$

Postoji izomorfizam prstenova $\varphi : \mathbb{F}_4 \to F$ *definiran sa*

$$\varphi\left(\begin{bmatrix} a & b \\ b & a+b \end{bmatrix}\right) = a + b\beta.$$

(ii) Prema tablici 4.1 postoje tri normirana ireducibilna polinoma drugog stupnja u $\mathbb{F}_3[x]$. *To su:* $p(x) = x^2 + 1$, $q(x) = x^2 + x - 1$ *i* $r(x) = x^2 - x - 1$. *Svaki od tih polinoma čini polje od* $9 = 3^2$ *elemenata. Pogledajmo detaljnije prva dva polinoma. Prema propoziciji 2.1.4* (v) *slijedi da je polje* $E = \mathbb{F}_3[x]/(p(x))$ *dano s:*

$$E = \{a + b\alpha : \alpha^2 + 1 = 0\}.$$

Slično, konstruiramo polje $F = \mathbb{F}_3[x]/(q(x))$ *kao:*

$$F = \{a + b\beta : \beta^2 + \beta - 1 = 0\}.$$

Preslikavanje $\varphi : E \to F$ *definirano s* $\varphi(a + b\alpha) = a + b(1 - \beta)$ *je izomorfizam. Dakle, ova dva polja su izomorfna.*
Sada je i polje $K = \mathbb{F}_3[x]/(r(x))$ *također polje koje ima* 9 *elemenata. Pomoću Mooreovog korolara (korolar 4.2.10) pokazat ćemo da je polje K izomorfno s E i F.*

(iii) Prema tablici 4.1 postoji osam normiranih ireducibilnih polinoma trećeg stupnja $p(x) \in \mathbb{F}_3[x]$. *Svaki od njih čini polje* $\mathbb{F}_3[x]/(p(x))$ *koje ima* $3^3 = 27$ *elemenata. Pomoću Mooreovog korolara (korolar 4.2.10) pokazat ćemo da je svih osam polja međusobno izomorfno.*

stupnja 2:	x^2+1;	x^2+x-1;	x^2-x-1.
stupnja 3:	x^3-x+1;	x^3+x^2-x+1;	x^3-x^2+1;
	x^3-x^2+x+1;	x^3-x-1;	x^3+x^2-1;
	x^3+x^2+x-1;	x^3-x^2-x-1.	

Tablica 4.1: Normirani ireducibilni polinomi drugog i trećeg stupnja nad $\mathbb{F}_3$

Sada ćemo vidjeti koja su od konstruiranih polja izomorfna, a koja nisu. Za početak ćemo navesti lemu koja nam govori da možemo konstruirati izomorfizam između dva polja cijepanja.

Lema 4.2.8. *Neka je $\varphi : k \to k'$ izomorfizam polja, a $\varphi^* : k[x] \to k'[x]$ izomorfizam prstena definiran s $\varphi^* : g(x) = a_0 + a_1x + ... + a_nx^n \mapsto g^*(x) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n$. Neka je $f(x) \in k[x]$ i $f^*(x) = \varphi^*(f) \in k'[x]$. Ako je E polje cijepanja od $f(x)$ nad k i E' polje cijepanja od f^* nad k', tada postoji izomorfizam $\Phi : E \to E'$ koji je proširenje od φ:*

$$\begin{array}{ccc} E & \overset{\Phi}{\dashrightarrow} & E' \\ | & & | \\ k & \xrightarrow[\varphi]{} & k' \end{array}$$

Dokaz. Ova lema dokazuje se indukcijom po $d = [E : k]$.

Baza: Uzmimo $d = 1$. Polinom $f(x)$ možemo zapisati kao umnožak linearnih polinoma iz $k[x]$. Iz toga slijedi da i $f^*(x)$ također možemo faktorizirati u $k'[x]$. Stoga vrijedi $E' = k'$ i možemo pisati $\Phi = \varphi$.

Korak indukcije: Uzmimo korijen $z \in E$ od $f(x)$ takav da on nije iz k. Neka je $p(x) = irr(z, k)$ minimalan polinom od z u k. Budući da $z \notin k$, vrijedi da je $st(p) > 1$, to jest možemo reći da je $st(p) = [k(z) : k]$. Neka je $z' \in E'$ korijen od $p^*(x)$. Uzmimo da je $p^*(x) = irr(z', k')$ ireducibilan normirani polinom u $k'[x]$.

Koristeći varijantu tvrdnje (ii) teorema 2.2.4, dobivamo izomorfizam $\tilde{\varphi} : k(z) \to k'(z')$ koji proširuje φ, definiran s $\tilde{\varphi} : z \mapsto z'$. Polinom $f(x)$ možemo smatrati polinomom s

koeficijentima u $k(z)$, jer $k \subseteq k(z) \Rightarrow k[x]$. Želimo pokazati da je E polje cijepanja od $f(x)$ nad $k(z)$, tj. da je:

$$E = k(z)(z_1, ..., z_n),$$

pri čemu su $z_1, ..., z_n$ korijeni od $f(x)/(x - z)$. To vrijedi jer je:

$$E = k(z, z_1, ..., z_n) = k(z)(z_1, ..., z_n).$$

Analogno slijedi da je E' polje cijepanja od f^* nad $k'(z')$. No znamo da je $[E : k(z)] < [E : k]$ pa nam pretpostavka indukcije omogućava konstrukciju izomorfizma $\Phi : E \Rightarrow E'$ koji proširuje $\tilde{\varphi}$ pa ujedno i φ. □

Teorem 4.2.9. *Ako je k polje i $f(x) \in k[x]$, tada bilo koja dva polja cijepanja od $f(x)$ nad k su izomorfna i postoji izomorfizam koji fiksira sve elemente polja k.*

Dokaz. Neka su E i E' polja cijepanja od $f(x)$ nad k. Ako je preslikavanje φ identiteta, tada primjenom leme 4.2.8 slijedi dokaz teorema. □

Korolar 4.2.10 (Moore)**.** *Bilo koja dva konačna polja s p^n elementa su izomorfna.*

Dokaz. Ako je E polje s $q = p^n$ elemenata, tada nam Lagrangeov teorem (teorem 3.1.6) primjenjen na multiplikativnu grupu $E^\times$ daje $a^{q-1} = 1$ za svaki $a \in E^\times$. Slijedi da je svaki element od E korijen od $f(x) = x^q - x \in F_p[x]$ te je E polje cijepanja od $f(x)$ nad F_p. □

Bibliografija

[1] Rotman J. J., *Advanced Modern Algebra. Graduate Studies in Mathematics*, sv. 114, American Mathematical Society, Providence, RI, (2010.).

[2] Hungerford T. W., *Algebra, Graduate Text in Mathematics*, sv. 73, (Springer, Verlag, New York, 1980), Reprint of the 1974 original.

Sažetak

U ovom diplomskom radu iznijeli smo osnovne rezultate o algebarskim proširenjima polja. Definirali smo algebarska i transcendentna proširenja polja te smo proučavali konačna proširenja polja. Budući da smo definirali proširenja polja, prirodno se nameće pitanje postojanja algebarski zatvorenih polja. Dokazali smo postojanje algebarskog zatvarača za svako polje te da je algebarski zatvarač prebrojivog polja također prebrojiv. Osim toga, dokazali smo da su bilo koja dva algebarska zatvarača polja izomorfna s obzirom na definirano preslikavanje. Podijelili smo vrste polja i s obzirom na njihovu karakteristiku te smo definirali konačno polje i njegovu karakteristiku. Dokazali smo Galoisov teorem koji je važan teorem o konačnim poljima te iskazujemo i dokazujemo kada su bilo koja dva konačna polja izomorfna.

Summary

In this thesis we presented the main results of the algebraic field extensions. We have defined algebraic and transcendental extension fields and studied finite extension fields. Since we defined extension fields, naturally raises the question of the existence of algebraic closed fields. We have proven the existence of algebraic closure of each field and that algebraic closure of countable field is also countable. In addition, we showed that any two algebraic closures fields are isomorphic with respect to the defined mapping. We have divided the field types with respect to their characteristics and defined a finite field and its characteristics. We have proved Galois theorem which is an important theorem on finite fields and stated and proved, when are two finite fields isomorphic.

Životopis

Dana 04. rujna 1990. godine rođena sam u Varaždinu. Godine 1997. upisana sam u VII. osnovnu školu Varaždin. Godinu dana kasnije, upisujem se u Školu stranih jezika Kezele kako bi počela učiti engleski jezik. Tokom svog osnovnoškolskog obrazovanja sudjelovala sam na gradskim i županijskim natjecanjima iz matematike i hrvatskog jezika. Godine 2005. upisujem prvi razred u Prvoj gimnaziji Varaždin. Budući da sam učila engleski jezik, upisujem smjer opća-dvojezična gimnazija u kojem se neki predmeti izvode na engleskom jeziku. Školske godine 2007./2008. sudjelujem na međužupanijskom natjecanju iz logike. Godine 2009. upisujem preddiplomski sveučilišni studij na Matematičkom odsjeku PMF-a, smjer nastavnički. Godine 2013. stječem diplomu za sveučilišnu prvostupnicu edukacije matematike i upisujem diplomski sveučilišni studij Matematika, smjer nastavnički. U zimskom semestru akademske godine 2014./2015. pohađam praksu u Osnovnoj školi A.Šenoa u Zagrebu. U ljetnom semestru te iste godine, pohađam praksu u XV. gimnaziji Zagreb (MIOC). Godine 2015. diplomirala sam na Matematičkom odsjeku PMF-a te stekla akademski naziv magistar edukacije matematike.