# ALGEBRA

Prof. dr. sc. Hrvoje Kraljević

Predavanja održana na Odjelu za matematiku
Sveučilišta Josipa Jurja Strossmayera u Osijeku
u ljetnom semestru akademske godine 2007./2008.

Osijek, 2008.

# Sadržaj

# Poglavlje 1

# Uvodna razmatranja

## 1.1 Djeljivost i faktorizacija cijelih brojeva

U cijelom ovom kolegiju ćemo sa $\mathbb{Z}$ označavati skup svih cijelih brojeva, sa $\mathbb{N}$ skup svih prirodnih brojeva i sa $\mathbb{Z}_+$ skup svih cijelih brojeva $\geq 0$. Dakle,

$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\}, \qquad \mathbb{N} = \{1, 2, 3, \ldots\} = \{n \in \mathbb{Z};\ n > 0\},$$

$$\mathbb{Z}_+ = \{0, 1, 2, 3, \ldots\} = \{n \in \mathbb{Z};\ n \geq 0\} = \mathbb{N} \cup \{0\}.$$

Za $n, k \in \mathbb{Z}$ kažemo da je $k$ **djelitelj**, **divizor**, **faktor** ili **mjera** od $n$, a da je $n$ **multipl** ili **višekratnik** od $k$, ako postoji $\ell \in \mathbb{Z}$ takav da je $n = k\ell$. Također kažemo da $k$ **dijeli** $n$, odnosno, da je $n$ **djeljiv** sa $k$. Činjenicu da je $n$ djeljiv sa $k$ zapisujemo ovako: $k|n$. Ta tzv. **relacija djeljivosti** očigledno ima sljedeća svojstva:

- $n|n\ \forall n \in \mathbb{Z}$.
- Ako su $k, n \in \mathbb{Z}$ tada vrijedi $k|n$ i $n|k$ ako i samo ako je $k = n$ ili $k = -n$, tj. ako i samo ako je $|k| = |n|$.
- Ako su $k, n, m \in \mathbb{Z}$ i ako $k|n$ i $n|m$ onda $k|m$.

Ukoliko broj $n$ nije djeljiv sa $k$, to zapisujemo ovako: $k \nmid n$.

**Propozicija 1.1.** *Neka su $a, b \in \mathbb{Z}$ i $b \neq 0$. Tada postoje jedinstveni $q, r \in \mathbb{Z}$ takvi da je $a = bq + r$ i $0 \leq r < |b|$.*

**Dokaz:** Egzistenciju je dovoljno dokazati za $b > 0$, budući da je $a = bq + r$ ekvivalentno sa $a = (-b)(-q) + r$. Skup

$$A = \{n \in \mathbb{Z};\ bn \leq a\}$$

je neprazan, jer je $-|a| \in A$. Taj je skup odozgo ograničen, jer vrijedi $n \leq \dfrac{a}{b}\ \forall n \in A$. Stavimo $q = \max A$ i $r = a - bq$. Naravno, tada vrijedi $a = bq + r$. Imamo $q \in A$, dakle, $bq \leq a$. Prema tome, vrijedi $r = a - bq \geq 0$. Kad bi bilo $r \geq b$, imali bismo

$$a = bq + r = b(q + 1) + (r - b) \geq b(q + 1),$$

pa bi slijedilo $q + 1 \in A$, što je nemoguće jer je $q = \max A$. Zaključujemo da je $r < b$. Dakle,

$$a = bq + r \qquad \text{i} \qquad 0 \leq r < b.$$

Time je egzistencija dokazana.

Dokažimo sada jedinstvenost. Pretpostavimo da su $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ takvi da je

$$a = bq_1 + r_1 = bq_2 + r_2, \qquad 0 \leq r_1 < |b|, \qquad 0 \leq r_2 < |b|.$$

Tada je

$$b(q_1 - q_2) = r_2 - r_1.$$

Iz $0 \leq r_1 < |b|$ i $0 \leq r_2 < |b|$ slijedi $|r_2 - r_1| < |b|$. No, zbog prethodne jednakosti je $|r_2 - r_1| = |b| \cdot |q_1 - q_2|$, pa je $|r_2 - r_1| < |b|$ moguće samo ako je $|r_2 - r_1| = 0$, tj. $r_1 = r_2$. Slijedi $bq_1 = a - r_1 = a - r_2 = bq_2$, dakle, $q_1 = q_2$. Time je dokazana i jedinstvenost.

Broj $r$ iz iskaza propozicije 1.1. zove se **ostatak** pri dijeljenju broja $a$ s brojem $b$. Naravno, broj $a$ djeljiv je s brojem $b$ ako i samo je taj ostatak pri dijeljenju jednak nuli.

Neka su $a, b \in \mathbb{Z}$ cijeli brojevi koji nisu oba jednaki 0. **Najveća zajednička mjera** brojeva $a$ i $b$ je najveći broj $d \in \mathbb{N}$ takav da $d|a$ i $d|b$. Dakle,

$$d = \max M, \qquad \text{gdje je} \quad M = \{k \in \mathbb{N};\ k|a,\ k|b\}.$$

Najveća zajednička mjera postoji zato što je $M \neq \emptyset$, budući da je $1 \in M$, i zato što je skup $M$ odozgo ograničen; doista, ako je npr. $b \neq 0$, Tada je $k \leq |b|\ \ \forall k \in M$. Najveću zajedničku mjeru označavamo kraticom $GCD$ (iz engleskog *the greatest common divisor*). Dakle, ako je $d$ najveća zajednička mjera brojeva $a$ i $b$, pisat ćemo $d = GCD(a, b)$.

Opisat ćemo sada tzv. **Euklidov algoritam** pomoću kojega možemo izračunati najveću zajedničku mjeru bilo koja dva cijela broja. Neka su $a, b \in \mathbb{Z}$ i $b \neq 0$. Euklidov algoritam sastoji se od uzastopne primjene propozicije 1.1. sve dok ostatak pri dijeljenju ne iščezne:

$$\begin{array}{rcll} a &=& bq_1 + r_1, & 0 < r_1 < |b|, \\ b &=& r_1q_2 + r_2, & 0 < r_2 < r_1, \\ r_1 &=& r_2q_3 + r_3, & 0 < r_3 < r_2, \\ & \vdots & & \\ r_{n-2} &=& r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1}, \\ r_{n-1} &=& r_nq_{n+1}. & \end{array}$$

Primijetimo da je pri svakom dijeljenju ostatak striktno manji od ostatka pri prethodnom dijeljenju. Stoga Euklidov algoritam sigurno završava: nakon konačno mnogo dijeljenja s ostatkom doći ćemo do djeljivosti, tj. do dijeljenja bez ostatka. Naravno, ako $b|a$, Euklidov algoritam završava već u prvom koraku, tj. $n = 0$ :

$$a = bq_1.$$

Ako je $n = 1$, tj. ako $b \nmid a$, ali $r_1|b$, onda Euklidov algoritam završava u drugom koraku:

$$\begin{array}{rcll} a &=& bq_1 + r_1, & 0 < r_1 < |b|, \\ b &=& r_1q_2. & \end{array}$$

**Propozicija 1.2.** *Neka su $a, b \in \mathbb{Z}$, $b \neq 0$ i $d = GCD(a, b)$.*

(a) *Broj $r_n$ iz Euklidovog algoritma je upravo najveća zajednička mjera brojeva $a$ i $b$ : $r_n = d$.*

(b) *Ako $c|a$ i $c|b$ onda $c|d$.*

(c) *Postoje $x, y \in \mathbb{Z}$ takvi da je $d = ax + by$.*

**Dokaz:** (1) Najprije ćemo dokazati da $r_n|a$ i $r_n|b$. Stavimo $r_0 = b$ i $r_{-1} = a$. Tada prvih $n$ jednakosti u Euklidovom algoritmu poprimaju oblik:

$$r_{k-2} = r_{k-1}q_k + r_k \qquad 1 \leq k \leq n. \tag{1.1}$$

Iz posljednje jednakosti u Euklidovom algoritmu, $r_{n-1} = r_n q_{n+1}$, vidi se da $r_n|r_{n-1}$. Sada iz $n-$te jednakosti, $r_{n-2} = r_{n-1}q_n + r_n$, slijedi da $r_n|r_{n-2}$. Neka je $k \leq n$ i pretpostavimo da smo dokazali da $r_n|r_k$ i $r_n|r_{k-1}$. Tada iz $k-$te jednakosti, $r_{k-2} = r_{k-1}q_k + r_k$, slijedi da $r_n|r_{k-2}$. Na taj način silaznom matematičkom indukcijom zaključujemo da $r_n|r_k \ \forall k \geq -1$. Posebno, $r_n|r_{-1}$ i $r_n|r_0$, Tj. $r_n|a$ i $r_n|b$.

(2) Dokazat ćemo da postoje $x, y \in \mathbb{Z}$ takvi da je $r_n = ax + by$. Sada ćemo upotrijebiti uzlaznu matematičku indukciju i uz oznake iz (1) dokazat ćemo da $\forall k \geq -1$ postoje $x, y \in \mathbb{Z}$ takvi da je $r_k = ax + by$. To je trivijalno za $k = -1$ i $k = 0$ :

$$r_{-1} = a = 1 \cdot a + 0 \cdot b, \qquad r_0 = b = 0 \cdot a + 1 \cdot b.$$

Provedimo sada korak indukcije: pretpostavimo da je $1 \leq k < n$ i da je dokazano da postoje $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ takvi da je

$$r_{k-2} = ax_2 + by_2 \qquad \text{i} \qquad r_{k-1} = ax_1 + by_1.$$

Tada iz (1.1) dobivamo

$$r_k = r_{k-2} - r_{k-1}q_k = ax_2 + by_2 - (ax_1 + by_1)q_k = a(x_2 - q_k x_1) + b(y_2 - q_k y_1),$$

dakle, uz oznake $x = x_2 - q_k x_1$ i $y = y_1 - q_k y_1$ imamo $r_k = ax + by$. Time je korak indukcije proveden.

(3) Prema (1) vrijedi $r_n|a$ i $r_n|b$. Ako je $c \in \mathbb{Z}$ takav da $c|a$ i $c|b$, tada pomoću (2) dobivamo da $c|r_n$. Posebno, $c \leq r_n$, pa zaključujemo da je $r_n$ najveća zajednička mjera, $r_n = d$. Time je dokazano $(a)$ i $(b)$, a kako je $r_n = d$, tvrdnja $(c)$ je upravo ono što smo dokazali u (2).

Za brojeve $a, b \in \mathbb{Z}$ kažemo da su **relativno prosti** ako je $GCD(a, b) = 1$. To znači da ne postoji $n \in \mathbb{N}$, $n > 1$, takav da $n|a$ i $n|b$.

**Korolar 1.1.** *Brojevi $a, b \in \mathbb{Z}$ su relativno prosti ako i samo ako postoje $x, y \in \mathbb{Z}$ takvi da je $ax + by = 1$.*

**Dokaz:** Ako su $a$ i $b$ relativno prosti, tada je $GCD(a, b) = 1$, pa iz tvrdnje $(c)$ propozicije 1.2. slijedi da postoje $x, y \in \mathbb{Z}$ takvi da je $ax+by = 1$. Obratno, pretpostavimo da je $ax+by = 1$ za neke $x, y \in \mathbb{Z}$. Tada svaki zajednički djelitelj od $a$ i $b$ dijeli 1. Slijedi da su 1 i $-1$ jedini zajednički djelitelji od $a$ i $b$. Dakle, $GCD(a, b) = 1$.

**Korolar 1.2.** *Neka su brojevi $a, b, c \in \mathbb{Z}$ takvi da su $a$ i $b$ relativno prosti i da su $a$ i $c$ relativno prosti. Tada su $a$ i umnožak $bc$ relativno prosti.*

**Dokaz:** Prema tvrdnji $(c)$ propozicije 1.2. postoje $x, y, u, v \in \mathbb{Z}$ takvi da je

$$ax + by = 1 \qquad \text{i} \qquad au + cv = 1.$$

Tada za $e = axu + cxv + byu$ i $f = yv$ nalazimo

$$ae + (bc)f = a^2xu + acxv + abyu + bcyv = (ax + by)(au + cv) = 1.$$

Prema korolaru 1.1. slijedi $GCD(a, bc) = 1$.

**Korolar 1.3.** *Neka su $a, b, c \in \mathbb{Z}$ i pretpostavimo da su $a$ i $b$ relativno prosti i da $a|bc$. Tada $a|c$.*

**Dokaz:** Prema korolaru 1.1. postoje $x, y \in \mathbb{Z}$ takvi da je $ax + by = 1$. Odatle je $c = cax + cby$, pa ako $a|bc$, tj. $bc = a\ell$ za neki $\ell \in \mathbb{Z}$, tada je

$$c = cax + cby = cax + a\ell y = a(cx + \ell y).$$

Dakle, $a|c$.

**Korolar 1.4.** *Neka su $a, b, c \in \mathbb{Z}$ takvi da je $GCD(a, b) = 1$ i da $a|c$ i $b|c$. Tada $(ab)|c$.*

**Dokaz:** Prema korolaru 1.1. postoje $x, y \in \mathbb{Z}$ takvi da je $ax + by = 1$. Neka su $k, \ell \in \mathbb{Z}$ takvi da je $c = ak$ i $c = b\ell$. Tada nalazimo

$$c = cax + cby = b\ell ax + akby = ab(\ell x + ky).$$

Dakle, $(ab)|c$.

Sada smo u mogućnosti dokazati tzv. **fundamentalni teorem aritmetike** o faktorizaciji u proste faktore. Općenito se prikaz broja $n \in \mathbb{Z}$ kao produkta od dva ili više brojeva iz $\mathbb{Z}$ zove se **faktorizacija** od $n$. Faktorizacija $n = k\ell$ zove se **trivijalna** ako je $k = \pm 1$ ili $\ell = \pm 1$. Ako su $k \neq \pm 1$ i $\ell \neq \pm 1$ ta se faktorizacija zove **netrivijalna**. **Prost broj** ili **primbroj** je prirodan broj $p > 1$ koji nema nijednu netrivijalnu faktorizaciju $p = k\ell$, odnosno koji nije djeljiv ni s jednim prirodnim brojem osim sa 1 i sa $p$.

**Teorem 1.1.** *Neka je $n \in \mathbb{N}$, $n \geq 2$. Postoje $r \in \mathbb{N}$ i prosti brojevi $p_1, \ldots, p_r$ takvi da je $n = p_1 \cdots p_r$. Ako su i $q_1, \ldots, q_s$ prosti brojevi takvi da je $n = q_1 \cdots q_s$, onda je $s = r$ i numeracija se može izabrati tako da bude $q_j = p_j$ za $j = 1, \ldots, r$.*

Glavni korak u dokazu sadržan je u sljedećoj lemi:

**Lema 1.1.** *Ako su $a_1, \ldots, a_s \in \mathbb{Z}$, $s \geq 2$, i ako prost broj $p$ dijeli umnožak $a_1 \cdots a_s$, onda $p|a_i$ za neki $i$.*

**Dokaz** provodimo matematičkom indukcijom u odnosu na $s \geq 2$.

(1) Pretpostavimo najprije da je $s = 2$, dakle $p|(a_1a_2)$, i da $p \nmid a_1$. Budući da su $\pm 1$ i $\pm p$ jedini djelitelji od $p$, slijedi $GCD(a_1, p) = 1$. Sada iz korolara 1.3. (za $m = a_1$, $n = a_2$ i $c = p$) slijedi $p|a_2$.

(2) Provedimo sada i korak indukcije. Neka je $s \geq 3$ i pretpostavimo da je lema dokazana za slučaj umnoška od $s - 1$ faktora. Ako $p$ dijeli umnožak $a_1 \cdots a_s = a_1(a_2 \cdots a_s)$, onda prema (1) vrijedi $p|a_1$ ili $p|(a_2 \cdots a_s)$. U ovom drugom slučaju iz pretpostavke indukcije slijedi $p|a_i$ za neki $i \in \{2, \ldots, s\}$.

**Dokaz egzistencije u teoremu 1.1.** provodimo metodom matematičke indukcije u odnosu na $n \geq 2$. Ako je $n = 2$, tvrdnja je trivijalna: $r = 1$ i $p_1 = 2$. Pretpostavimo da je $n \geq 3$ i da je egzistencija faktorizacije dokazana za prirodne brojeve manje od $n$. Ako je broj $n$ prost, opet imamo faktorizaciju je jednim faktorom: $r = 1$ i $p_1 = n$. Ako $n$ nije prost broj, onda možemo pisati $n = ab$, $a, b \in \mathbb{N}$, $a > 1$, $b > 1$. Tada su $a < n$ i $b < n$, pa po pretpostavci indukcije brojevi $a$ i $b$ imaju faktorizacije u proste faktore. Skupimo li te dvije faktorizacije zajedno, dobivamo faktorizaciju broja $n$.

**Dokaz jedinstvenosti u teoremu 1.1.** Pretpostavimo da je

$$n = p_1 \cdots p_r = q_1 \cdots q_s,$$

pri čemu su $p_1, \ldots, p_r, q_1, \ldots, q_s$ prosti brojevi. Možemo pretpostaviti da je $r \leq s$ (ako nije, zamijenimo uloge $p_i$ i $q_j$). Imamo $p_1|n$, tj. $p_1|(q_1 \cdots q_s)$. Sada iz leme 1.1. slijedi da $p_1$ dijeli jedan od faktora, tj. postoji $j \in \{1, \ldots, s\}$ takav da $p_1|q_j$. Numeraciju možemo promijeniti tako da bude $j = 1$, tj. $p_1|q_1$. Budući da je $q_1$ prost broj, slijedi $p_1 = q_1$. Sada gornju jednakost možemo skratiti sa $p_1$, pa dobivamo

$$p_2 \cdots p_r = q_2 \cdots q_s.$$

Jednako rezoniranje pokazuje da možemo numeraciju $q_j$, $2 \leq j \leq s$, promijeniti tako da bude $p_2 = q_2$. Korak po korak zaključujemo da je (uz eventualnu izmjenu numeracije) $p_j = q_j$ za $j = 1, \ldots, r$. Kad bi bilo $s > r$, imali bismo

$$p_1 \cdots p_r = p_1 \cdots p_r q_{r+1} \cdots q_s \qquad \Longrightarrow \qquad 1 = q_{r+1} \cdots q_s$$

a to je nemoguće. Dakle, $s = r$.

U faktorizaciji broja $n$ možemo zajedno grupirati iste faktore. Dakle, prirodan broj $n$ se zapisuje u obliku

$$n = p_1^{k_1} \cdots p_\ell^{k_\ell}$$

pri čemu su prosti brojevi $p_1, \ldots, p_\ell$ međusobno različiti i $k_1, \ldots, k_\ell \in \mathbb{Z}_+$. Takva je faktorizacija jedinstvena do na poredak ako je $k_j > 0$ za svaki $j$. Takav zapis broja $n$ zovemo **prim−faktorizacija** ili **prosta faktorizacija** od $n$.

**Korolar 1.5.** *Ako je $n = p_1^{k_1} \cdots p_\ell^{k_\ell}$ prim−faktorizacija prirodnog broja $n$, onda su svi pozitivni djelitelji broja $n$ točno svi produkti oblika $m = p_1^{j_1} \cdots p_\ell^{j_\ell}$, gdje je $0 \leq j_i \leq k_i$ za $i = 1, \ldots, \ell$.*

**Dokaz:** Očito je svaki takav produkt djelitelj od $n$ :

$$n = mq \qquad \text{za} \quad q = p_1^{k_1 - j_1} \cdots p_\ell^{k_\ell - j_\ell}.$$

Obratno, neka je $m \in \mathbb{N}$ djelitelj od $n$, tj. $n = mx$ za neki $x \in \mathbb{N}$. Primijenimo sada teorem 1.1. na brojeve $m$ i $x$. Pomnožimo li te dvije faktorizacije dobivamo faktorizaciju od $n$, pa zbog jedinstvenosti u teoremu 1.1. vidimo da se u obje faktorizacije mogu pojavljivati samo prosti brojevi $p_1, \ldots, p_\ell$. Dakle,

$$m = p_1^{j_1} \cdots p_\ell^{j_\ell} \qquad \text{i} \qquad x = p_1^{q_1} \cdots p_\ell^{q_\ell}$$

pri čemu su $j_1, \ldots, j_\ell, q_1, \ldots, q_\ell \in \mathbb{Z}_+$. Slijedi

$$n = p_1^{k_1} \cdots p_\ell^{k_\ell} \qquad \text{i} \qquad n = mx = p_1^{j_1 + q_1} \cdots p_\ell^{j_\ell + q_\ell}.$$

Zbog jedinstvenosti u teoremu 1.1. zaključujemo da je $k_i = j_i + q_i$, dakle, $0 \leq j_i \leq k_i$ za $i = 1, \ldots, \ell$.

Ako želimo usporediti prim−faktorizacije za dva prirodna broja, obje možemo dopuniti s nultim potencija nekih primbrojeva tako da se u obje faktorizacije pojavljuju isti primbrojevi. Tada je lako napisati najveću zajedničku mjeru dvaju promatranih brojeva:

**Korolar 1.6.** *Neka su*

$$a = p_1^{k_1} \cdots p_\ell^{k_\ell} \qquad i \qquad a = p_1^{j_1} \cdots p_\ell^{j_\ell}$$

*pri čemu su $p_1, \ldots, p_\ell$ međusobno različiti primbrojevi i $k_1, \ldots, k_\ell, j_1, \ldots, j_\ell \in \mathbb{Z}_+$. Tada je*

$$GCD(a, b) = p_1^{\min(k_1, j_1)} \cdots p_\ell^{\min(k_\ell, j_\ell)}.$$

**Dokaz:** Neka je $d = GCD(a, b)$ i označimo sa $c$ desnu stranu gornje jednakosti koju treba dokazati. Tada je $c \in \mathbb{N}$ i prema korolaru 1.5. $c$ dijeli i $a$ i $b$. Drugim riječima, $c$ je zajednička mjera od $a$ i $b$ pa zaključujemo da je $c \leq d$. S druge strane, kako $d|a$ i $d|b$, dvostruka primjena korolara 1.5. pokazuje da je

$$d = p_1^{m_1} \cdots p_\ell^{m_\ell}, \qquad m_i \leq k_i, \quad m_i \leq j_i, \quad \text{za} \quad i = 1, \ldots, \ell.$$

Slijedi da je $m_i \leq \min(k_i, j_i)$ za $i = 1, \ldots, \ell$, pa zaključujemo da je $d \leq c$. Dvije nejednakosti daju $c = d$.

Iz korolara 1.6. neposredno slijedi:

**Korolar 1.7.** *Cijeli brojevi $a$ i $b$ su relativno prosti ako i samo ako ne postoji primbroj $p$ koji ih oba dijeli.*

Sada možemo dokazati poznati **Kineski teorem o ostacima** (engl. *Chinese Remainder Theorem*):

**Teorem 1.2.** *Neka su $a$ i $b$ relativno prosti prirodni brojevi. Tada za svaki par $(r, s) \in \mathbb{Z}_+ \times \mathbb{Z}_+$ takav da je $r < a$ i $s < b$ postoji jedinstven $n \in \mathbb{Z}_+$ takav da je $n < ab$ i da vrijedi $a|(n-r)$ i $b|(n-s)$. Štoviše, tako definirano preslikavanje $(r, s) \mapsto n$ je bijekcija sa $\{0, 1, \ldots, a-1\} \times \{0, 1, \ldots, b-1\}$ na $\{0, 1, \ldots, ab-1\}$.*

**Dokaz:** (1) Dokažimo najprije egzistenciju takvog broja $n$. Budući da su $a$ i $b$ relativno prosti, prema korolaru 1.1. postoje $u, v \in \mathbb{Z}$ takvi da je $au + bv = 1$. Stavimo li $x = u(s-r)$ i $y = v(r-s)$, slijedi

$$ax - by = s - r.$$

Stavimo $m = ax + r = by + s$. Pomoću propozicije 1.1. zaključujemo da postoje $q, n \in \mathbb{Z}$ takvi da je

$$m = abq + n \qquad \text{i} \qquad 0 \leq n < ab.$$

Slijedi

$$n - r = m - abq - r = ax - abq = a(x - bq) \qquad \text{i} \qquad n - s = m - abq - s = by - abq = b(y - aq),$$

dakle, $a|(n-r)$ i $b|(n-s)$.

(2) Dokažimo sada jedinstvenost. Neka su $n, n' \in \{0, 1, \ldots, ab-1\}$ takvi da vrijedi

$$a|(n-r), \qquad a|(n'-r), \qquad b|(n-s), \qquad b|(n'-s).$$

Kako je

$$n - n' = (n - r) - (n' - r) = (n - s) - (n' - s),$$

vidimo da $a$ i $b$ dijele $n - n'$. Brojevi $a$ i $b$ su relativno prosti, pa iz korolara 1.4. slijedi da i umnožak $ab$ dijeli $n - n'$. Međutim, $|n - n'| < ab$, pa slijedi $n - n' = 0$, odnosno, $n = n'$.

(3) Dokažimo sada injektivnost preslikavanja $(r, s) \mapsto n$. Neka su $r, r' \in \{0, 1, \ldots, a-1\}$ i $s, s' \in \{0, 1, \ldots, b-1\}$ i pretpostavimo da za $n \in \{0, 1, \ldots, ab-1\}$ vrijedi

$$a|(n-r), \qquad a|(n-r'), \qquad b|(n-s), \qquad b|(n-s').$$

Tada vrijedi i

$$a|(r-r') \qquad \text{i} \qquad b|(s-s'),$$

a kako je $|r - r'| < a$ i $|s - s'| < b$, zaključujemo da je $r - r' = s - s' = 0$, tj. $(r, s) = (r', s')$.

(4) Napokon, skupovi $\{0, 1, \ldots, a-1\} \times \{0, 1, \ldots, b-1\}$ i $\{0, 1, \ldots, ab-1\}$ imaju isti broj elemenata: taj broj je umnožak $ab$. Stoga iz injektivnosti preslikavanja $(r, s) \mapsto n$ slijedi njegova surjektivnost, odnosno, bijektivnost.

U cijelom ovom kolegiju ćemo za svaki konačan skup $A$ sa $|A|$ označavati **broj njegovih elemenata**.

Definiramo sada tzv. **Eulerovu funkciju** $\varphi : \mathbb{N} \to \mathbb{Z}_+$ na sljedeći način:

$$\varphi(n) = |\{k \in \mathbb{Z};\ 0 \leq k < n \text{ i } GCD(n, k) = 1\}|.$$

Dakle, $\varphi(n)$ je broj cijelih brojeva $k \in \{0, 1, \ldots, n-1\}$ koji su relativno prosti sa $n$.

**Teorem 1.3.** *Neka je $n \in \mathbb{N}$, $n \geq 2$, i neka je $n = p_1^{k_1} \cdots p_r^{k_r}$ prim−faktorizacija broja $n$ (dakle, $k_j > 0\ \forall j$). Tada je*

$$\varphi(n) = \prod_{j=1}^{r} p_j^{k_j - 1}(p_j - 1).$$

**Dokaz:** Najprije ćemo dokazati da vrijedi:

$$a, b \in \mathbb{N}, \quad GCD(a, b) = 1 \qquad \Longrightarrow \qquad \varphi(ab) = \varphi(a)\varphi(b).$$

Zbog Kineskog teorema o ostacima (teorem 1.2.) dovoljno je dokazati da preslikavanje $(r, s) \mapsto n$ u tom teoremu ima svojstvo

$$GCD(r, a) = GCD(s, b) = 1 \qquad \Longleftrightarrow \qquad GCD(n, ab) = 1. \tag{1.2}$$

Da to dokažemo, pretpostavimo da je $0 \leq n < ab$ i $GCD(n, ab) > 1$. Neka je $p$ prost broj koji dijeli i $n$ i $ab$. Prema lemi 1.1. tada $p|a$ ili $p|b$. Pretpostavimo npr. da $p|a$. Ako je $(r, s)$ par koji po teoremu 1.2. odgovara broju $n$ tada vrijedi $a|(n - r)$. Sada iz $p|a$ i $a|(n - r)$ slijedi $p|(n - r)$. Međutim, $p|n$ pa vrijedi i $p|r$. Dakle, $GCD(r, a) > 1$. Time je u ekvivalenciji (1.2) dokazana implikacija slijeva nadesno.

Dokažimo sada i implikaciju zdesna nalijevo. Pretpostavimo da za neke $a, b \in \mathbb{N}$ i za neki $n < ab$ i za pripadni par $(r, s)$ ne vrijedi $GCD(r, a) = GCD(s, b) = 1$. Možemo uzeti npr. da je $GCD(r, a) > 1$. Tada neki primbroj $p$ dijeli i $r$ i $a$. U skladu s teoremom 1.2. vrijedi $a|(n - r)$, pa slijedi $p|(n - r)$, dakle i $p|n$. Prema tome, vrijedi $p|(ab)$ i $p|n$, pa zaključujemo da $n$ i $ab$ nisu relativno prosti, $GCD(n, ab) > 1$. Time je ekvivalencija (1.2) u potpunosti dokazana.

Preostaje da dokažemo da za svaki primbroj $p$ i za svaki $k \in \mathbb{N}$ vrijedi

$$\varphi\left(p^k\right) = p^{k-1}(p - 1). \tag{1.3}$$

Jedini primbroj koji dijeli $p^k$ je $p$. Stoga, prema korolaru 1.7. za $n \in \{0, 1, \ldots, p^k - 1\}$ vrijedi $GCD(n, p^k) > 1$ ako i samo je $n$ multipl od $p$. To su brojevi

$$0, p, 2p, \ldots, p^k - p,$$

a kako je $p^k - p = \left(p^{k-1} - 1\right) p$, tih brojeva ima $p^{k-1}$. Slijedi

$$\varphi\left(p^k\right) = |\{0, 1, 2, \ldots, p^k - 1\}| - |\{0, p, 2p, \ldots, p^k - p\}| = p^k - p^{k-1} = p^{k-1}(p - 1).$$

Time je (1.3) dokazano.

## 1.2 Definicije osnovnih algebarskih struktura

**Grupoid** je neprazan skup $G$ sa zadanom binarnom operacijom, tj. sa zadanim preslikavanjem $G \times G \to G$. Ta se operacija označava na različite načine, npr. s točkom $(a, b) \mapsto a \cdot b$, ili s plus $(a, b) \mapsto a + b$, ili sa zvjezdicom $(a, b) \mapsto a * b$, ili s kružićem $(a, b) \mapsto a \circ b$, a najčešće bez ikakvoga znaka $(a, b) \mapsto ab$.

**Polugrupa** je grupoid $G$ u kome je operacija asocijativna, tj. u kome vrijedi

$$(ab)c = a(bc) \qquad \forall a, b, c \in G.$$

**Lijeva jedinica** u grupoidu $G$ je svaki element $a \in G$ koji ima svojstvo $ac = c \ \forall c \in G$. Slično, **desna jedinica** u grupoidu $G$ je svaki $b \in G$ takav da je $cb = c \ \forall c \in G$.

**Propozicija 1.3.** *Neka je $G$ grupoid, neka je $\mathfrak{L}(G)$ skup svih lijevih jedinica u $G$ i neka je $\mathfrak{R}(G)$ skup svih desnih jedinica u $G$. Pretpostavimo da je $\mathfrak{L}(G) \neq \emptyset$ i da je $\mathfrak{R}(G) \neq \emptyset$. Tada je $\mathfrak{L}(G) = \mathfrak{R}(G)$ i to je jednočlan skup.*

**Dokaz:** Za bilo koje $a \in \mathfrak{L}(G)$ i $b \in \mathfrak{R}(G)$ imamo $ab = a$ (jer je $b$ desna jedinica) i $ab = b$ (jer je $a$ lijeva jedinica). Dakle, vrijedi $a = b \ \forall a \in \mathfrak{L}(G)$ i $\forall b \in \mathfrak{R}(G)$, a to je upravo tvrdnja propozicije.

Jedini element skupa $\mathfrak{L}(G) = \mathfrak{R}(G)$ iz propozicije 1.3. zove se **jedinica**, ili **jedinični element**, ili **neutralni element** grupoida $G$. Jedinica se obično označava sa $e$ ili sa 1 ili sa $I$, a ako se istovremeno promatraju i drugi grupoidi zbog određenosti pišemo katkada $e_G$ ili $1_G$ ili $I_G$. Ukoliko je oznaka za operaciju $+$ onda se obično neutralni element zove **nula** i označava sa 0 ili sa $0_G$.

Polugrupa s jedinicom zove se **monoid**. Neka je $G$ monoid s jedinicom $e$ i neka je $a \in G$. **Lijevi invers** od $a$ je svaki element $b \in G$ takav da vrijedi $ba = e$. **Desni invers** od $a$ je svaki element $c \in G$ takav da vrijedi $ac = e$.

**Propozicija 1.4.** *Neka je $G$ monoid, $a \in G$, $\mathfrak{L}(a)$ skup svih lijevih inversa od $a$ i $\mathfrak{R}(a)$ skup svih desnih inversa od $a$. Pretpostavimo da je $\mathfrak{L}(a) \neq \emptyset$ i $\mathfrak{R}(a) \neq \emptyset$. Tada je $\mathfrak{L}(a) = \mathfrak{R}(a)$ i to je jednočlan skup.*

**Dokaz:** Za proizvoljne $b \in \mathfrak{L}(a)$ i $c \in \mathfrak{R}(a)$ nalazimo redom $b = be = b(ac) = (ba)c = ec = c$. Time je propozicija dokazana.

Jedini element u $\mathfrak{L}(a) = \mathfrak{R}(a)$ iz propozicije 1.4. zove se **invers** elementa $a$ i označava sa $a^{-1}$. Ako je binarna operacija u $G$ označena sa $+$, onda se invers od $a$ označava sa $-a$, a umjesto $c + -a$ pišemo $c - a$. Element $a \in G$ zove se **invertibilan** ako $a$ ima invers, tj. ako je $\mathfrak{L}(a) \neq \emptyset$ i $\mathfrak{R}(a) \neq \emptyset$. Skup svih invertibilnih elemenata monoida $G$ označavat ćemo sa $G^*$.

**Grupa** je monoid $G$ u kome je svaki element invertibilan, tj. $G^* = G$. Očito vrijedi:

**Propozicija 1.5.** *Neka je $G$ monoid s jedinicom $e$.*

(a) *Za svaki $a \in G^*$ je i $a^{-1} \in G^*$ i vrijedi $(a^{-1})^{-1} = a$.*

(b) *Ako su $a, b \in G^*$ onda je i $ab \in G^*$ i vrijedi $(ab)^{-1} = b^{-1}a^{-1}$.*

(c) *$e \in G^*$ i $e^{-1} = e$.*

*Posebno, $G^*$ je grupa.*

Grupoid, polugrupa, monoid ili grupa $G$ se zove **komutativna (komutativan)** ako je operacija u $G$ komutativna, tj. ako vrijedi $ab = ba\ \forall a, b \in G$. Komutativna grupa zove se i **Abelova** grupa.

Razmotrimo sada neke primjere. Skup $\mathbb{N}$ svih prirodnih brojeva s operacijom zbrajanja je komutativna polugrupa, ali nije monoid. Skup $\mathbb{N}$ s operacijom množenja je komutativni monoid; jedinica je broj 1. Imamo $\mathbb{N}^* = \{1\}$, tj. multiplikativna grupa prirodnih brojeva je trivijalna. Skup $\mathbb{Z}$ svih cijelih brojeva s operacijom zbrajanja je komutativna grupa u kojoj je neutralni element broj 0; ta se grupa zove *aditivna grupa cijelih brojeva* Skup $\mathbb{Z}$ s operacijom množenja je komutativni monoid u kome je jedinica broj 1. U tom monoidu je $\mathbb{Z}^* = \{1, -1\}$. Skup $\mathbb{Q}$ svih racionalnih brojeva je u odnosu na zbrajanje komutativna grupa s jedinicom 0 (*aditivna grupa racionalnih brojeva*), a u odnosu na množenje $\mathbb{Q}$ je komutativni monoid s jedinicom 1; nadalje, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ (*multiplikativna grupa racionalnih brojeva*). Slična je situacija i sa skupom $\mathbb{R}$ svih realnih brojeva i sa skupom $\mathbb{C}$ svih kompleksnih brojeva.

U svim ovim primjerima operacije su bile komutativne. Razmotrimo i neke nekomutativne.

Skup $M_n(\mathbb{R})$ svih realnih kvadratnih matrica $n-$tog reda s operacijom množenja je nekomutativni monoid u kome je jedinica jedinična matrica $I$, koja na glavnoj dijagonali ima jedinice, a svi su joj ostali elementi jednaki nuli. $M_n(\mathbb{R})^*$ je grupa regularnih matrica, koja se obično označava sa $GL_n(\mathbb{R})$ i zove *opća linearna grupa*; ona je nekomutativna ako je $n \geq 2$.

Stavimo $SL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R});\ \det A = 1\}$. To je grupa u odnosu na množenje matrica jer iz $A, B \in SL_n(\mathbb{R})$ slijedi $\det(AB) = (\det A)(\det B) = 1$, dakle $AB \in SL_n(\mathbb{R})$, a također i $\det(A^{-1}) = (\det A)^{-1} = 1$, dakle $A^{-1} \in SL_n(\mathbb{R})$. $SL_n(\mathbb{R})$ se zove *specijalna linearna grupa*. I ta je grupa nekomutativna ako je $n \geq 2$.

Neka je $O_n(\mathbb{R}) = \{A \in M_n(\mathbb{R});\ AA^\tau = A^\tau A = I\}$; pri tome je $A^\tau$ oznaka za transponiranu matricu matrice $A$. $O_n(\mathbb{R})$ je grupa i zove se *ortogonalna grupa*. I ona je nekomutativna, ako je $n \geq 3$.

Neka su sada $T$ i $S$ neprazni skupovi. Sa $S^T$ označavamo skup svih preslikavanja (funkcija) $\varphi : S \to T$. Ako su $f \in S^T$ i $g \in T^U$, definiramo njihovu *kompoziciju* $f \circ g : U \to T$ sa $(f \circ g)(u) = f(g(u))$, $u \in U$. Kompozicija funkcija je asocijativna u sljedećem smislu: ako su $f \in S^T$, $g \in T^U$ i $h \in U^V$ onda je $(f \circ g) \circ h = f \circ (g \circ h)$. Doista, za bilo koji element $v \in V$ imamo:

$$[(f \circ g) \circ h](v) = (f \circ g)(h(v)) = f(g(h(v))) = f((g \circ h)(v)) = [f \circ (g \circ h)](v).$$

Odatle se vidi da je za svaki neprazan skup $T$ skup $T^T$ s operacijom $\circ$ polugrupa. To je monoid jer identiteta $id_T : T \to T$, $id_T(t) = t\ \forall t \in T$, je neutralni element u odnosu na operaciju $\circ$. Grupa $\left(T^T\right)^*$ se sastoji od svih bijekcija sa $T$ na $T$. Takve se funkcije zovu *permutacije skupa* $T$, a $\left(T^T\right)^*$ je tzv. *grupa permutacija* skupa $T$. Inverzni element permutacije $f \in \left(T^T\right)^*$ je upravo inverzna funkcija funkcije $f$. Ako skup $T$ ima barem 3 elementa, grupa $\left(T^T\right)^*$ je nekomutativna. Ako je skup $T$ konačan i ima $n$ članova, npr. $T = \{1, 2, \ldots, n\}$, grupa permutacija skupa $T$ zove se *simetrična grupa $n-$tog reda* i označava sa $S_n$.

Neka je $G$ grupa i $H \subseteq G$. $H$ se zove **podgrupa** grupe $G$, ako je $H$ grupa s obzirom na istu operaciju. Za to je nužno i dovoljno da su ispunjena sljedeća tri uvjeta:

(1) $a, b \in H \ \Rightarrow\ ab \in H$.

(2) $a \in H \ \Rightarrow\ a^{-1} \in H$.

(3) $e \in H$.

Ukoliko je podskup $H$ neprazan, trima uvjetima (1), (2) i (3) ekvivalentan je jedan jedini sljedeći uvjet:

(4) $a, b \in H \;\Rightarrow\; ab^{-1} \in H$.

Doista, očito iz (1) i (2) slijedi (4). Pretpostavimo da vrijedi (4). Za neki $a \in H$ tada imamo $e = aa^{-1} \in H$, dakle vrijedi (3). Nadalje, za $a \in H$ imamo zbog (4) i (3) $a^{-1} = ea^{-1} \in H$, dakle vrijedi i (2). Napokon, ako su $a, b \in H$, tada je zbog (2) $b^{-1} \in H$, pa zbog (4) dobivamo $ab = a(b^{-1})^{-1} \in H$, dakle vrijedi i (1).

Aditivna grupa cijelih brojeva je podgupa aditivne grupe racionalnih brojeva, a ova je opet podgrupa aditivne grupe realnih brojeva. Skup $T_n(\mathbb{R})$ svih gornjetrokutastih matrica u $GL_n(\mathbb{R})$ je podgrupa grupe $GL_n(\mathbb{R})$. Ortogonalna grupa $O_n(\mathbb{R})$ je podgrupa od $GL_n(\mathbb{R})$. Specijalna linearna grupa $SL_n(\mathbb{R})$ je također podgrupa od $GL_n(\mathbb{R})$.

Promatrat ćemo sada preslikavanja s jedne grupe u drugu koja su u skladu s operacijama. Neka su $G_1$ i $G_2$ grupe. Preslikavanje $\varphi : G_1 \to G_2$ zove se **homomorfizam grupa**, ako vrijedi:

$$\varphi(ab) = \varphi(a)\varphi(b) \qquad \forall\ a, b \in G_1.$$

**Propozicija 1.6.** *Neka je $\varphi : G_1 \to G_2$ homomorfizam grupa. Tada vrijedi:*

(*a*) $\varphi(a^{-1}) = [\varphi(a)]^{-1}\ \forall a \in G_1$.

(*b*) $\varphi(e_{G_1}) = e_{G_2}$.

**Dokaz:** (*b*) Imamo $\varphi(e_{G_1}) = \varphi(e_{G_1}e_{G_1}) = \varphi(e_{G_1})\varphi(e_{G_1})$, a odatle je

$$e_{G_2} = [\varphi(e_{G_1})]^{-1}\varphi(e_{G_1}) = [\varphi(e_{G_1})]^{-1}\varphi(e_{G_1})\varphi(e_{G_1}) = e_{G_2}\varphi(e_{G_1}) = \varphi(e_{G_1}).$$

(*a*) Za $a \in G_1$ imamo zbog (*b*)

$$\varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(e_{G_1}) = e_{G_2}$$

i analogno

$$\varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(e_{G_1}) = e_{G_2}.$$

Te dvije jednakosti pokazuju da je $\varphi(a^{-1})$ invers od $\varphi(a)$.

Ako je $\varphi : G_1 \to G_2$ homomorfizam koji je injekcija, onda se $\varphi$ zove **monomorfizam**. Homomorfizam $\varphi$ koji je surjekcija zove se **epimorfizam**.

Ako su $\varphi : G_1 \to G_2$ i $\psi : G_2 \to G_3$ homomorfizmi grupa, onda je i njihova kompozicija $\psi \circ \varphi : G_1 \to G_3$ homomorfizam grupa. Doista, za $a, b \in G_1$ imamo:

$$(\psi \circ \varphi)(ab) = \psi(\varphi(ab)) = \psi(\varphi(a)\varphi(b)) = \psi(\varphi(a))\psi(\varphi(b)) = (\psi \circ \varphi)(a)(\psi \circ \varphi)(b).$$

Ako su $\varphi$ i $\psi$ monomorfizmi (odnosno, epimorfizmi) onda je i njihova kompozicija $\psi \circ \varphi$ monomorfizam (odnosno, epimorfizam).

**Izomorfizam grupa** je homomorfizam koji je bijekcija, dakle i monomorfizam i epimorfizam. Kažemo da je grupa $G_1$ **izomorfna** grupi $G_2$, ako postoji izomorfizam $\varphi : G_1 \to G_2$. U tom slučaju pišemo $G_1 \simeq G_2$. Svojstvo *biti izomorfan*, odnosno relacija $\simeq$, je relacija ekvivalencije među grupama. Doista, identiteta $id_G : G \to G$ je izomorfizam, dakle $G \simeq G$. Nadalje, ako je $G_1 \simeq G_2$ i

ako je $\varphi : G_1 \to G_2$ izomorfizam, onda je i inverzno preslikavanje $\varphi^{-1} : G_2 \to G_1$ izomorfizam, dakle vrijedi $G_2 \simeq G_1$. Napokon, ako su $G_1 \simeq G_2$ i $G_2 \simeq G_3$ i $\varphi : G_1 \to G_2$ i $\psi : G_2 \to G_3$ su izomorfizmi, onda je i njihova kompozicija $\psi \circ \varphi : G_1 \to$ izomorfizam, dakle vrijedi $G_1 \simeq G_3$.

Ako je $\varphi : G_1 \to G_2$ homomorfizam grupa, skup

$$\operatorname{Im}\varphi = \{\varphi(a);\, a \in G_1\} \subseteq G_2$$

zove se **slika** (ili **područje vrijednosti**) homomorfizma $\varphi$, a skup

$$\operatorname{Ker}\varphi = \{a \in G_1;\, \varphi(a) = e_{G_2}\} \subseteq G_1$$

**jezgra** homomorfizma $\varphi$.

Homomorfizam $\varphi : G_1 \to G_2$ je monomorfizam ako i samo ako mu je jezgra trivijalna $\operatorname{Ker}\varphi = \{e_{G_1}\}$. Doista, pretpostavimo da je $\varphi$ monomorfizam. Za bilo koji $a \in \operatorname{Ker}\varphi$ je $\varphi(a) = e_{G_2}$. Također je i $\varphi(e_{G_1}) = e_{G_2}$, pa kako je $\varphi$ injekcija slijedi $a = e_{G_1}$. To pokazuje da je $\operatorname{Ker}\varphi = \{e_{G_1}\}$. Dokažimo i obrnutu implikaciju, pa pretpostavimo da je $\operatorname{Ker}\varphi = \{e_{G_1}\}$. Neka su $a, b \in G_1$ takvi da je $\varphi(a) = \varphi(b)$. Tada je $\varphi(ab^{-1}) = \varphi(a)(\varphi(b))^{-1} = e_{G_2}$, dakle $ab^{-1} \in \operatorname{Ker}\varphi = \{e_{G_1}\}$, pa slijedi $ab^{-1} = e_{G_1}$, tj. $a = b$. Dakle, $\varphi$ je injekcija, odnosno monomorfizam.

Očito je $\varphi$ epimorfizam ako i samo ako je $\operatorname{Im}\varphi = G_2$.

**Propozicija 1.7.** *Neka je $\varphi : G_1 \to G_2$ homomorfizam grupa. Tada je $Im\varphi$ podgrupa od $G_2$, a $Ker\varphi$ je podgrupa od $G_1$.*

**Dokaz:** Neka su $a, b \in \operatorname{Im}\varphi$. Tada postoje $c, d \in G_1$ takvi da je $a = \varphi(c)$ i $b = \varphi(d)$, pa slijedi

$$ab^{-1} = \varphi(c)[\varphi(d)]^{-1} = \varphi(c)\varphi(d^{-1}) = \varphi(cd^{-1}) \in \operatorname{Im}\varphi.$$

To pokazuje da je Im $\varphi$ podgrupa od $G_2$.

Neka su sada $a, b \in \operatorname{Ker}\varphi$. Tada je

$$\varphi(ab^{-1}) = \varphi(a)[\varphi(b)]^{-1} = e_{G_2}[e_{G_2}]^{-1} = e_{G_2},$$

što pokazuje da je $ab^{-1} \in \operatorname{Ker}\varphi$. Dakle, Ker $\varphi$ je podgrupa od $G_1$. Time je propozicija dokazana.

Netrivijalni primjeri homomorfizama su eksponencijalne funkcije: ako je $r > 0$ i $r \neq 1$ onda je sa $\varphi(t) = r^t$ definiran homomorfizam aditivne grupe $\mathbb{R}$ realnih brojeva u multiplikativnu grupu $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. Njegova je jezgra trivijalna Ker $\varphi = \{0\}$, dakle $\varphi$ je monomorfizam. Njegova je slika Im $\varphi$ podgrupa $\mathbb{R}^*_+$ svih pozitivnih realnih brojeva. Eksponencijalna funkcija definirana je i za kompleksnu varijablu, $\varphi(z) = r^z,\ z \in \mathbb{C}$. Tada je $\varphi$ homomorfizam aditivne grupe $\mathbb{C}$ u multiplikativnu grupu $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. Sada je Im $\varphi = \mathbb{C}^*$, dakle $\varphi$ je epimorfizam, ali nije monomorfizam jer je Ker $\varphi = \{\frac{2n\pi i}{\ln r};\, n \in \mathbb{Z}\}$, gdje je $\ln r$ oznaka za prirodni logaritam od $r$.

Drugi netrivijalni primjer homomorfizma je determinanta. Po Binnet−Cauchyjevom teoremu determinanta je homomorfizam grupe $GL_n(\mathbb{R})$ u multiplikativnu grupu $\mathbb{R}^*$. To je epimorfizam, a njegova je jezgra podgrupa $SL_n(\mathbb{R})$.

Definirat ćemo sada još neke algebarske strukture. **Prsten** je neprazan skup $A$ na kome su zadane dvije binarne operacije, *zbrajanje* $(a, b) \mapsto a + b$ i *množenje* $(a, b) \mapsto ab$, sa sljedećim svojstvima:

(a) U odnosu na zbrajanje $A$ je komutativna grupa; neutralni element se označava sa 0 i zove *nula*.

(b) U odnosu na množenje $A$ je polugrupa (odnosno, množenje je asocijativno).

(c) Množenje je i slijeva i zdesna distributivno u odnosu na zbrajanje, tj. vrijedi:

$$a(b+c) = ab + ac \qquad \text{i} \qquad (a+b)c = ac + bc \qquad \forall a, b, c \in A.$$

**Prsten** $A$ je **komutativan** ako je operacija množenja komutativna, tj. $ab = ba\ \forall a, b \in A$. $A$ je **unitalni prsten**, ako je $A$ u odnosu na množenje monoid, tj. postoji $1 \in A$ takav da je $a1 = 1a = a\ \forall a \in A$. Takav element 1 tada je jedinstven i zove se **jedinica prstena** $A$.

U prstenu $A$ za svaki element $a$ vrijedi $0a = a0 = 0$. To slijedi iz jednakosti $0 = 0 + 0$, dakle $0a = (0+0)a = 0a + 0a$. Primijetimo da je $1 = 0$ ako i samo ako je $A = \{0\}$; doista, ako je $1 = 0$ onda za svaki $a \in A$ vrijedi $a = 1a = 0a = 0$. To je tzv. *trivijalan prsten.* U netrivijalnom prstenu unitalnom prstenu $A \neq \{0\}$ je $1 \neq 0$.

Razmotrimo sada nekoliko primjera prstenova.

(*a*) Skup $\mathbb{Z}$ svih cijelih brojeva s običnim operacijama zbrajanja i množenja je komutativni unitalni prsten.

(*b*) Ako u cikličkoj grupi $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ uz zbrajanje modulo $m$ definiramo i množenje modulo $m$ dobivamo komutativni unitalni prsten. Umnožak brojeva $j, k \in \mathbb{Z}_m$ modulo $m$ je jedinstven $n \in Z_m$ takav da je $jk - n$ djeljiv sa $m$.

(*c*) Neka je $S$ neprazan skup. U skupu $\mathbb{Z}^S$ svih funkcija $f : S \to \mathbb{Z}$ definiramo zbrajanje i množenje po točkama:

$$(f+g)(s) = f(s) + g(s), \qquad (fg)(s) = f(s)g(s), \qquad f, g \in \mathbb{Z}^S,\ \ s \in S.$$

S tako definiranim operacijama $\mathbb{Z}^S$ postaje komutativni unitalni prsten. Jedinica je konstantna funkcija $e(s) = 1\ \ \forall s \in S$.

(*d*) Prethodna konstrukcija primjenjiva je i za proizvoljan prsten $A$ i neprazan skup $S$. U skupu $A^S$ svih funkcija $f : S \to A$ zbrajanje i množenje definiramo po točkama:

$$(f+g)(s) = f(s) + g(s), \qquad (fg)(s) = f(s)g(s), \qquad f, g \in A^S,\ \ s \in S.$$

Tada je $A^S$ prsten, koji je komutativan ako i samo ako je prsten $A$ komutativan i unitalan je ako i samo ako je prsten $A$ unitalan.

(*e*) Za beskonačan skup $S$ i prsten $A$ stavimo:

$$A_0^S = \{f \in A^S;\ f(s) \neq 0 \text{ za samo konačno mnogo točaka } s \in S\}.$$

S operacijama po točkama $A_0^S$ je prsten koji je komutativan ako i samo ako je $A$ komutativan. Primijetimo da prsten $A_0^S$ nije unitalan čak ni kad je $A$ unitalan (osim ako je $A$ trivijalan ali tada je i $A_0^S$ trivijalan).

(*f*) Polja racionalnih brojeva $\mathbb{Q}$, realnih brojeva $\mathbb{R}$ i kompleksnih brojeva $\mathbb{C}$ su komutativni prsteni s jedinicom.

(*g*) Skup $M_n(\mathbb{R})$ svih realnih kvadratnih matrica $n-$tog reda uz zbrajanje i množenje matrica je unitalan prsten. Jedinica u tom prstenu je jedinična matrica $I$. Taj je prsten nekomutativan ako je $n \geq 2$.

($h$) Neka je $T_n(\mathbb{R})$ skup svih gornje trokutastih matrica, tj. matrica oblika:

$$\begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & \alpha_{1,3} & \cdots & \alpha_{1,n-1} & \alpha_{1,n} \\ 0 & \alpha_{2,2} & \alpha_{2,3} & \cdots & \alpha_{2,n-1} & \alpha_{2,n} \\ 0 & 0 & \alpha_{3,3} & \cdots & \alpha_{3,n-1} & \alpha_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \alpha_{n-1,n-1} & \alpha_{n-1,n} \\ 0 & 0 & 0 & \cdots & 0 & \alpha_{n,n} \end{bmatrix}$$

S operacijama zbrajanja i množenja matrica $T_n(\mathbb{R})$ je unitalan prsten, koji je nekomutativan ako je $n \geq 2$.

($i$) Neka je $G$ grupa i $A$ prsten. Definiramo skup $A[G]$ isto kao i $A_0^G$ :

$$A[G] = \{f \in A^G;\ f(x) \neq 0 \text{ za samo konačno mnogo } x \in G\}.$$

U skupu $A[G]$ zbrajanje definiramo po točkama:

$$(f+g)(x) = f(x) + g(x), \qquad f, g \in A[G]\ \ x \in G,$$

a množenje koje označavamo sa $*$ i zovemo *konvolucija* definiramo formulom:

$$(f * g)(x) = \sum_{y \in G} f(xy^{-1})g(y), \qquad f, g \in A[G]\ \ x \in G.$$

S tako definiranim operacijama $A[G]$ je prsten. On je komutativan ako su komutativni i grupa $G$ i prsten $A$. Ako je $A$ unitalan prsten s jedinicom 1 onda je i $A[G]$ unitalan prsten; ulogu jedinice ima funkcija $\epsilon$ definirana sa:

$$\epsilon(x) = \begin{cases} 1 & \text{ako je} \quad x = e, \\ \\ 0 & \text{ako je} \quad x \neq e. \end{cases}$$

Pri tome je sa $e$ označena jedinica u grupi $G$.

Neka je $A$ unitalan prsten. U odnosu na množenje tada je $A$ monoid. Prema propoziciji 1.5. skup $A^*$ svih invertibilnih elemenata tog monoida je grupa. Ona se zove **multiplikativna grupa** prstena $A$. Naravno, ako je prsten $A$ netrivijalan, tj. ako je $A \neq \{0\}$, onda $0 \notin A^*$; štoviše, 0 nije ni lijevoinvertibilan ni desnoinvertibilan element od $A$.

Imamo $\mathbb{Z}^* = \{1, -1\}$, $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$, $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ i $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$. $\left(A^S\right)^*$ je skup svih onih $f \in A^S$ za koje je $f(s) \in A^*\ \ \forall s \in S$. Ako je $p$ prost broj onda je $(\mathbb{Z}_p)^* = \{1, 2, \ldots, p-1\} = \mathbb{Z}_p \setminus \{0\}$. Ako broj $m$ nije prost, onda je

$$(\mathbb{Z}_m)^* = \{k \in \{1, 2, \ldots, m-1\};\ GCD(k, m) = 1\}.$$

Neka je $A$ prsten. **Potprsten** je neprazan podskup $B \subseteq A$ koji je i sam prsten s obzirom na iste operacije. Za to je nužno i dovoljno da je $B$ podgrupa od $A$ u odnosu na zbrajanje i potpolugrupa u odnosu na množenje. Neprazan podskup $B \subseteq A$ je potprsten ako i samo ako vrijedi:

$$a, b \in B \qquad \Rightarrow \qquad a - b \in B \ \text{ i } \ ab \in B.$$

Ako je $A$ unitalan prsten s jedinicom 1, potprsten $B$ zove se **unitalan potprsten** ako je $1 \in B$.

Moguće je da potprsten neunitalnog prstena bude unitalan prsten. Npr. uzmimo da je $A$

prsten, $S$ beskonačan skup i $T \subset S$ neki njegov konačan podskup. Tada je $A_0^S$ neunitalan prsten, a $B = \{f \in A_0^S;\ f(s) = 0\ \forall s \in S \setminus T\}$ je njegov potprsten koji je unitalan prsten.

Nadalje, moguće je da potprsten $B$ unitalnog prstena $A$ s jedinicom $1_A$ bude unitalan prsten s jedinicom $1_B$, ali da $B$ nije unitalan potprsten od $A$, tj. da je $1_B \neq 1_A$. Npr. neka je $A = M_n(\mathbb{R})$ i neka je $k < n$. Uočimo skup $B$ svih kvadratnih matrica $n-$tog reda u kojima se zadnjih $n-k$ redaka i zadnjih $n-k$ stupaca sastoji od samih nula. Tj. $B$ je skup svih matrica oblika:

$$\begin{bmatrix} \beta_{11} & \beta_{12} & \cdots & \beta_{1k} & 0 & \cdots & 0 \\ \beta_{21} & \beta_{22} & \cdots & \beta_{2k} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ \beta_{k1} & \beta_{k2} & \cdots & \beta_{kk} & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix}$$

Tada je $A$ unitalan prsten (jedinica je jedinična matrica $I$), a $B$ je neunitalan potprsten od $A$ s jedinicom jer $I \notin B$. Međutim, $B$ je unitalan prsten: jedinica u prstenu B je matrica

$$\begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix}$$

**Tijelo** je unitalan prsten $A$ takav da je $A^* = A \setminus \{0\}$, tj. svaki element različit od nule je invertibilan. Komutativno tijelo zove se **polje**. Primjeri polja su polje racionalnih brojeva $\mathbb{Q}$, polje realnih brojeva $\mathbb{R}$ i polje kompleksnih brojeva $\mathbb{C}$. Još jedan primjer je polje algebarskih brojeva $\mathbb{A}$. To je skup svih $\lambda \in \mathbb{C}$ takvih da postoji prirodan broj $n$ i cijeli brojevi $\alpha_0, \alpha_1, \ldots, \alpha_n$ takvi da vrijedi

$$\alpha_n \lambda^n + \alpha_{n-1}\lambda^{n-1} + \ldots + \alpha_1 \lambda + \alpha_0 = 0 \ \text{ i } \ \alpha_n \neq 0.$$

Kao što ćemo kasnije vidjeti može se dokazati da za $\alpha, \beta \in \mathbb{A}$ vrijedi $\alpha + \beta, \alpha - \beta, \alpha\beta \in \mathbb{A}$, a ako je $\beta \neq 0$, onda je i $\dfrac{\alpha}{\beta} \in \mathbb{A}$. Dakle, $\mathbb{A}$ je stvarno polje.

Ako je $p$ primbroj, onda je $(\mathbb{Z}_p)^* = \mathbb{Z}_p \setminus \{0\}$, dakle, prsten $\mathbb{Z}_p$ je polje.

Navedimo još i jedan primjer tijela koje nije komutativno, tj. koje nije polje. To je **tijelo kvaterniona** $\mathbb{H}$. To je skup svih uređenih četvorki realnih brojeva

$$\mathbb{H} = \{(\alpha, \beta, \gamma, \delta);\ \alpha, \beta, \gamma, \delta \in \mathbb{R}\},$$

u kome je zbrajanje definirano sa

$$(\alpha, \beta, \gamma, \delta) + (\alpha', \beta', \gamma', \delta') = (\alpha + \alpha', \beta + \beta', \gamma + \gamma', \delta + \delta'),$$

a množenje sa

$$(\alpha, \beta, \gamma, \delta) \cdot (\alpha', \beta', \gamma', \delta') =$$
$$= (\alpha\alpha' - \beta\beta' - \gamma\gamma' - \delta\delta', \alpha\beta' + \beta\alpha' + \gamma\delta' - \delta\gamma', \alpha\gamma' + \gamma\alpha' + \delta\beta' - \beta\delta', \alpha\delta' + \delta\alpha' + \beta\gamma' - \gamma\beta').$$

Neposrednim računom provjerava se da je $\mathbb{H}$ unitalan prsten s nulom $0_{\mathbb{H}} = (0,0,0,0)$ i jedinicom $1_{\mathbb{H}} = (1,0,0,0)$. Za $a \in \mathbb{H}$ definiramo tzv. **konjugirani kvaternion**

$$\overline{a} = (\alpha, -\beta, -\gamma, -\delta) \qquad \text{ako je} \quad a = (\alpha, \beta, \gamma, \delta).$$

Primjenom definicije množenja slijedi

$$a\overline{a} = \overline{a}a = (\alpha^2 + \beta^2 + \gamma^2 + \delta^2, 0, 0, 0).$$

Ako je $a \neq 0$, tj. bar jedan od brojeva $\alpha, \beta, \gamma, \delta$ je različit od nule, onda stavimo:

$$b = \frac{\overline{a}}{\alpha^2 + \beta^2 + \gamma^2 + \delta^2} =$$

$$= \left( \frac{\alpha}{\alpha^2+\beta^2+\gamma^2+\delta^2}, -\frac{\beta}{\alpha^2+\beta^2+\gamma^2+\delta^2}, -\frac{\gamma}{\alpha^2+\beta^2+\gamma^2+\delta^2}, -\frac{\delta}{\alpha^2+\beta^2+\gamma^2+\delta^2} \right).$$

Tada iz gornje jednakosti slijedi $ab = ba = (1,0,0,0) = 1_{\mathbb{H}}$, dakle $a$ je invertibilan i $a^{-1} = b$. To pokazuje da je svaki element različit od nule invertibilan, dakle $\mathbb{H}$ je tijelo. To tijelo nije komutativno, dakle to nije polje. $\mathbb{H}$ možemo shvaćati kao četverodimenzionalan vektorski prostor nad poljem $\mathbb{R}$ realnih brojeva s bazom $\{1, i, j, k\}$, gdje su

$$1 = 1_{\mathbb{H}} = (1,0,0,0), \quad i = (0,1,0,0), \quad j = (0,0,1,0), \quad k = (0,0,0,1).$$

Tada je

$$i^2 = j^2 = k^2 = -1, \;\; ij = -ji = k, \;\; jk = -kj = i, \;\; ki = -ik = j.$$

## 1.3 Permutacije

U ovom odjeljku promatrat ćemo simetričnu grupu $S_n$, tj. grupu svih permutacija konačnog skupa $\{1,\dots,n\}$. Ako su $\sigma,\tau\in S_n$, njihovu kompoziciju $\sigma\circ\tau$ ćemo označavati kraće sa $\sigma\tau$ i zvati je **produkt** permutacija $\sigma$ i $\tau$. Dakle, $(\sigma\tau)(j)=\sigma(\tau(j))$ za svaki $j\in\{1,\dots,n\}$. Jedinični element grupe $S_n$ je identiteta na skupu $\{1,\dots,n\}$; označavat ćemo je sa 1, dakle, $1(j)=j\ \ \forall j$. Invers permutacije $\sigma\in S_n$ je inverzna funkcija $\sigma^{-1}:\{1,\dots,n\}\to\{1,\dots,n\}$, jer $\sigma\sigma^{-1}=\sigma^{-1}\sigma=1$ znači da je $\sigma^{-1}(\sigma(j))=j$ i $\sigma(\sigma^{-1}(j))=j$ za svaki $j\in\{1,\dots,n\}$.

Jedan način za označavanje permutacije $\sigma$ jest da napišemo dva retka od $n$ brojeva: u gornji redak napišemo redom brojeve od 1 do $n$ a u donji redak redom slike tih brojeva $\sigma(1),\dots,\sigma(n)$. Dakle, $\sigma=\begin{pmatrix}1&2&3&4&5&6\\2&5&3&6&4&1\end{pmatrix}$ je sljedeća permutacija skupa $\{1,2,3,4,5,6\}$ :

$$\sigma(1)=2,\quad \sigma(2)=5,\quad \sigma(3)=3,\quad \sigma(4)=6,\quad \sigma(5)=4,\quad \sigma(6)=1.$$

Inverzna permutacija dobije se tako da dva retka zamijene mjesta, a zatim poredamo stupce tako da u prvom retku ponovo budu redom brojevi $1,\dots,n$; npr.

$$\sigma=\begin{pmatrix}1&2&3&4&5&6\\2&5&3&6&4&1\end{pmatrix}\qquad\Longrightarrow\qquad\sigma^{-1}=\begin{pmatrix}1&2&3&4&5&6\\6&1&3&5&2&4\end{pmatrix}.$$

$k-$**ciklus**, $2\le k\le n$, je permutacija $\sigma\in S_n$ koja ostavlja fiksnima $n-k$ elemenata skupa $\{1,\dots,n\}$, a preostalih $k$ elemenata poredanih u nekom redoslijedu $c_1,\dots,c_k$ ciklički permutira, tj.

$$\sigma(c_1)=c_2,\ \sigma(c_2)=c_3,\dots,\dots,\sigma(c_{k-1})=c_k,\ \sigma(c_k)=c_1.$$

Taj ćemo ciklus označiti sa $(c_1\ c_2\ \cdots\ c_{k-1}\ c_k)$. Npr. $\sigma=(2\ 4\ 5\ 3)\in S_6$ je $4-$ciklus u prethodno definiranoj oznaci dan sa $\begin{pmatrix}1&2&3&4&5&6\\1&4&2&5&3&6\end{pmatrix}$:

$$\sigma(1)=1,\quad \sigma(2)=4,\quad \sigma(3)=2,\quad \sigma(4)=5,\quad \sigma(5)=3,\quad \sigma(6)=6.$$

Očito oznake (4 5 3 2), (5 3 2 4) i (3 2 4 5) predstavljaju isti taj ciklus. Katkada je zgodno o identiteti 1 govoriti kao o jedinstvenom $1-$ciklusu.

Za cikluse kažemo da su **disjunktni**, ako su podskupovi od $\{1,\dots,n\}$, koje oni ciklički permutiraju, međusobno disjuntni. Npr. (2 4 5 3) i (1 6) su disjunktni, ali (2 4 5 3) i (2 6) nisu. Ako su $\sigma$ i $\tau$ disjunktni ciklusi oni očito komutiraju: $\sigma\tau=\tau\sigma$.

**Propozicija 1.8.** *Svaka permutacija $\sigma\in S_n$ je ili ciklus ili je produkt međusobno disjunktnih ciklusa. Ciklusi koji se pojavljuju u tom prikazu jedinstveno su određeni sa $\sigma$.*

**Dokaz:** Za permutaciju $\sigma\in S_n$ označimo sa $Fix(\sigma)$ skup svih $j\in\{1,\dots,n\}$ koje permutacija $\sigma$ ostavlja fiksnim:

$$Fix(\sigma)=\{j;\ 1\le j\le n,\ \sigma(j)=j\}.$$

Dokaz prve tvrdnje, tj. da je svaka permutacija ili ciklus ili je produkt međusobno disjunktnih ciklusa, provest ćemo silaznom indukcijom u odnosu na $m(\sigma)=|Fix(\sigma)|\le n$.

Baza indukcije: Ako je $m(\sigma)=n$, onda je $\sigma(j)=j\ \ \forall j$, dakle, $\sigma=1$, a to je jedinstveni $1-$ciklus.

Korak indukcije: Pretpostavimo da je $k\le n-1$ i da je tvrdnja dokazana za permutacije $\sigma$ takve da je $m(\sigma)>k$. Neka je $m(\sigma)=k$. Neka je $j\in\{1,\dots,n\}\setminus Fix(\sigma)$. Tada je $\sigma(j)\ne j$. Promatrajmo niz

$$j,\ \sigma(j),\ \sigma^2(j)=\sigma(\sigma(j)),\ \dots\dots,\ \sigma^r(j)=\sigma(\sigma^{r-1}(j)),\ \dots\dots.$$

Svaki član toga niza nalazi se u skupu $\{1,\dots,n\}\setminus Fix(\sigma)$. Doista, pretpostavka $\sigma(\sigma^i(j))=\sigma^i(j)$ bi značila $\sigma^{i+1}(j)=\sigma^i(j)$, a odatle bi primjenom permutacije $(\sigma^{-1})^i$ slijedilo $\sigma(j)=j$, tj. $j\in Fix(\sigma)$, suprotno pretpostavci. Kako je skup $\{1,\dots,n\}\setminus Fix(\sigma)$ konačan, postoji $r\in\mathbb{N}$ takav da je $\sigma^r(j)\in\{j,\sigma(j),\dots,\sigma^{r-1}(j)\}$. Neka je $r$ najmanji takav. Tada je $\sigma^r(j)=\sigma^\ell(j)$ za neki $0\le\ell<r$, pri čemu podrazumijevamo da je $\sigma^0=1$ i $\sigma^1=\sigma$. Kad bi bilo $\ell>0$, primjenom permutacije $(\sigma^{-1})^\ell$ na tu jednakost dobili bismo $\sigma^{r-\ell}(j)=j$, a to je u suprotnosti s minimalnosti $r$. Zaključujemo da je $\ell=0$, tj. $\sigma^r(j)=j$. Nadalje, kako je $j\notin Fix(\sigma)$, vrijedi $r\ge 2$. Brojevi $j,\sigma(j),\dots,\sigma^{r-1}(j)\in\{1,\dots,n\}\setminus Fix(\sigma)$ međusobno su različiti. Formirajmo $r-$ciklus $\gamma=(j\ \sigma(j)\ \cdots\ \sigma^{r-1}(j))$ i neka je $\tau=\gamma^{-1}\sigma$. Za $i\in Fix(\sigma)$ vrijedi $i\notin\{j,\sigma(j),\dots,\sigma^{r-1}(j)\}$, pa je $\gamma(i)=i$, dakle i $\gamma^{-1}(i)=i$. Prema tome je $\tau(i)=i$, odnosno, $i\in Fix(\tau)$. Nadalje, ako je $i\in\{j,\sigma(j),\dots,\sigma^{r-1}(j)\}$, npr. $i=\sigma^p(j)$, onda imamo

$$\tau(i)=\gamma^{-1}(\sigma(\sigma^p(j)))=\gamma^{-1}(\sigma^{p+1}(j))=\sigma^p(j)=i,$$

dakle, $i\in Fix(\tau)$. Time je dokazano da je $Fix(\sigma)\cup\{j,\sigma(j),\dots,\sigma^{r-1}(j)\}\subseteq Fix(\tau)$; ustvari, nije teško vidjeti da su zapravo ti skupovi jednaki. No i bez toga vidimo da je

$$m(\tau)=|Fix(\tau)|\ge|Fix(\sigma)|+|\{j,\sigma(j),\dots,\sigma^{r-1}(j)\}|=k+r>k.$$

Po pretpostavci indukcije $\tau$ je ili ciklus ili produkt međusobno disjunktnih ciklusa i u tim ciklusima pojavljuju se isključivo indeksi iz skupa

$$\{1,\dots,n\}\setminus Fix(\tau)\subseteq\{1,\dots,n\}\setminus(Fix(\sigma)\cup\{j,\sigma(j),\dots,\sigma^{r-1}(j)\}).$$

Posebno, svaki od tih ciklusa disjunktan je s ciklusom $\gamma=(j\ \sigma(j)\cdots\sigma^{r-1}(j))$. Dakle, $\sigma=\gamma\tau$ je produkt međusobno disjunktnih ciklusa. Time je proveden korak indukcije, dakle, dokazana je prva tvrdnja.

Dokažimo sada drugu tvrdnju, tj. jedinstvenost. Iz dokaza prve tvrdnje vidimo da svaki $j\in\{1,\dots,n\}$ generira sasvim određeni $r-$ciklus $\gamma_j=(j\ \sigma(j)\cdots\sigma^{r-1}(j))$ za neki $r\in\mathbb{N}$. Broj $r$ u potpunosti je određen sa $\sigma$ i sa $j$ : to je najmanji prirodan broj takav da vrijedi $\sigma^r(j)\in\{j,\sigma(j),\dots,\sigma^{r-1}(j)\}$. Ako imamo dva prikaza permutacije $\sigma$ kao produkta međusobno disjunktnih ciklusa, onda onaj ciklus u svakom od tih dvaju prikaza koji sadrži $j$ mora biti $\gamma_j$. Dakle, svi ciklusi u dva prikaza podudaraju se.

$2-$ciklus obično se zove **transpozicija**.

**Propozicija 1.9.** *Svaka permutacija $\sigma\in S_n$, $s\ne 1$, je ili transpozicija ili je produkt transpozicija.*

**Dokaz:** Zbog propozicije 1.8. tvrdnja je neposredna posljedica sljedeće leme:

**Lema 1.2.** *Svaki $k-$ciklus $\gamma$, $k>2$, produkt je $k-1$ transpozicija.*

**Dokaz:** Direktna provjera pokazuje da je

$$(c_1\ c_k)(c_1\ c_2\ \cdots\ c_{k-1})=(c_1\ c_2\ \cdots\ c_{k-1}\ c_k)$$

Odatle indukcijom po $k$ slijedi

$$(c_1\ c_2\ \cdots\ c_{k-1}\ c_k)=(c_1\ c_k)(c_1\ c_{k-1})\cdots(c_1\ c_2).$$

Sada ćemo sve permutacije podijeliti u dvije vrste: *parne* i *neparne*. Ekvivalentno, svakoj permutaciji $\sigma$ pridružit ćemo njen *predznak* $\operatorname{sgn}\sigma$.

Za permutaciju $\sigma\in S_n$ skupa $\{1,\dots,n\}$ promatrajmo produkte

$$\Pi(\sigma)=\prod_{1\le j<k\le n}(\sigma(k)-\sigma(j))\qquad\text{i}\qquad|\Pi(\sigma)|=\prod_{1\le j<k\le n}|\sigma(k)-\sigma(j)|.$$

Ako je $(r,s)$ bilo koji par prirodnih brojeva, takav da je $1 \leq r < s \leq n$, onda se faktor $s-r$ pojavljuje točno jedamput u produktu $|\Pi(\sigma)|$. Prema tome, $|\Pi(\sigma)|$ ne ovisi o permutaciji $\sigma$ :

$$|\Pi(\sigma)| = \prod_{1\leq j<k\leq n} (k-j) = 1!2!\cdots(n-1)!.$$

S druge strane, u produktu $\Pi(\sigma)$ pojavljuje se ili faktor $s-r$ ili faktor $r-s=-(s-r)$ ovisno o tome da li je $\sigma(r)<\sigma(s)$ ili je $\sigma(r)>\sigma(s)$. Naravno, produkt $\Pi(\sigma)$ može se od svoje apsolutne vrijednosti razlikovati samo u predznaku i taj predznak označimo sa $\operatorname{sgn}\sigma$ : stavljamo $\operatorname{sgn}\sigma = 1$ ako je $\Pi(\sigma)>0$, a $\operatorname{sgn}\sigma=-1$ ako je $\Pi(\sigma)<0$. Dakle,

$$\Pi(\sigma) = \operatorname{sgn}\sigma \prod_{1\leq j<k\leq n} (k-j)$$

Broj $\operatorname{sgn}\sigma = \pm 1$ zove se **predznak permutacije** $\sigma$. Ako je $\operatorname{sgn}\sigma$=1, kažemo da je $\sigma$ **parna permutacija**, a ako je $\operatorname{sgn}\sigma=-1$, $\sigma$ je **neparna permutacija**. Prema prethodnom razmatranju predznak permutacije jednak je umnošku onoliko faktora $-1$ koliko ima parova $(r,s)$ takvih da je $1\leq r<s\leq n$, ali $\sigma(r)>\sigma(s)$. Dakle, vrijedi

**Propozicija 1.10.** *Za svaku permutaciju $\sigma \in S_n$ vrijedi*

$$sgn\,\sigma = (-1)^{i(\sigma)}, \qquad gdje\ je \quad i(\sigma) = |I(\sigma)| \quad i \quad I(\sigma) = \{(r,s);\ 1\leq r<s\leq n,\ \sigma(r)>\sigma(s)\}.$$

Elementi $(r,s)$ skupa $I(\sigma)$ zovu se **inverzije** u permutaciji $\sigma$, a $i(\sigma)=|I(\sigma)|$ je **broj inverzija** u permutaciji $\sigma$.

**Lema 1.3.** *Neka je $\sigma \in S_n$ i neka je $(a\ b) \in S_n$ transpozicija. Tada je $sgn\,(\sigma(a\ b)) = -sgn\,\sigma$.*

**Dokaz:** Za sve parove $(r,s)$ takve da je $1\leq r<s\leq n$ treba usporediti brojeve $\sigma(s)-\sigma(r)$ i $(\sigma(a\ b))(s)-(\sigma(a\ b))(r)$. Naravno, možemo pretpostavljati da je $a<b$. Podijelit ćemo sve parove $(r,s)$ u pet skupina:

*Skupina* 1. U tu skupinu svrstavamo sve parove $(r,s)$, $1\leq r<s\leq n$ za koje su skupovi $\{r,s\}$ i $\{a,b\}$ disjunktni. Za svaki takav par $(r,s)$ je $(a\ b)(r)=r$ i $(a\ b)(s)=s$, pa imamo $(\sigma(a\ b))(s)-(\sigma(a\ b))(r)=\sigma(s)-\sigma(r)$. Dakle, isti je doprinos svakog para $(r,s)$ iz te skupine predznaku $\operatorname{sgn}\sigma$ i predznaku $\operatorname{sgn}(\sigma(a\ b))$.

*Skupina* 2. U drugu skupinu svrstavamo sve parove $(r,s)$, $1\leq r<s\leq n$, za koje je ili $r=a$ i $s<b$ ili je $r>a$ i $s=b$. Ta je skupina unija dvaju disjunktnih skupova

$$\{(a,t);\ a<t<b\} \qquad \text{i} \qquad \{(t,b);\ a<t<b\}.$$

Promotrimo sada za bilo koji $t$, $a<t<b$, doprinos dvaju parova $(a,t)$ i $(t,b)$ produktima $\Pi(\sigma)$ i $\Pi(\sigma(a\ b))$. Ta dva para doprinose produktu $\Pi(\sigma)$ faktorom $(\sigma(t)-\sigma(a))(\sigma(b)-\sigma(t))$, a produktu $\Pi(\sigma(a\ b))$ faktorom $(\sigma(t)-\sigma(b))(\sigma(a)-\sigma(t))$. Budući da je

$$(\sigma(t)-\sigma(a))(\sigma(b)-\sigma(t)) = (\sigma(t)-\sigma(b))(\sigma(a)-\sigma(t)),$$

ta dva para daju isti doprinos produktu $\Pi(\sigma)$ kao i produktu $\Pi(\sigma(a\ b))$.

*Skupina* 3. U tu skupinu svrstavamo sve parove $(r,s)$, $1\leq r<s\leq n$, za koje je ili $r=a$ i $s>b$ ili je $r=b$ i $s>b$. Ta je skupina unija dvaju disjunktnih skupova

$$\{(a,t);\ b<t\leq n\} \qquad \text{i} \qquad \{(b,t);\ b<t\leq n\}.$$

Promatramo sada za bilo koji $t$, $b < t \leq n$, doprinos dvaju parova $(a,t)$ i $(b,t)$ produktima za dvije permutacije. Oni doprinose produktu $\Pi(\sigma)$ faktorom $(\sigma(t)-\sigma(a))(\sigma(t)-\sigma(b))$, a produktu $\Pi(\sigma(a\ b))$ faktorom $(\sigma(t)-\sigma(b))(\sigma(t)-\sigma(a))$. Kako je

$$(\sigma(t)-\sigma(a))(\sigma(t)-\sigma(b)) = (\sigma(t)-\sigma(b))(\sigma(t)-\sigma(a))$$

ta dva para daju isti ukupni doprinos dvama produktima $\Pi(\sigma)$ i $\Pi(\sigma(a\ b))$.

*Skupina* 4. U ovu skupinu svrstavamo sve parove $(r,s)$, $q \leq r < s \leq n$, za koje je ili $r < a$ i $s = a$ ili je $r < a$ i $s = b$. Ta je skupina unija dvaju disjunktnih skupova

$$\{(t,a);\ 1 \leq t < a\} \qquad \text{i} \qquad \{(t,b);\ 1 \leq t < a\}.$$

Promatramo sada za bilo koji $t$, $1 \leq t < a$, doprinos dvaju parova $(t,a)$ i $(t,b)$ produktima za dvije permutacije. Oni doprinose produktu $\Pi(\sigma)$ faktorom $(\sigma(a)-\sigma(t))(\sigma(b)-\sigma(t))$, a produktu za $\sigma(a\ b)$ faktorom $(\sigma(b)-\sigma(t))(\sigma(a)-\sigma(t))$. Kako je

$$(\sigma(a)-\sigma(t))(\sigma(b)-\sigma(t)) = (\sigma(b)-\sigma(t))(\sigma(a)-\sigma(t))$$

ta dva para daju isti ukupni doprinos dvama produktima $\Pi(\sigma)$ i $\Pi(\sigma(a\ b))$.

*Skupina* 5. Ostaje nam još samo slučaj $\{r,s\} = \{a,b\}$, dakle, par $(r,s) = (a,b)$. Taj par produktu $\Pi(\sigma)$ doprinosi faktorom $\sigma(b)-\sigma(a)$ a produktu $\Pi(\sigma(a\ b))$ faktorom $\sigma(a)-\sigma(b)$.

Zaključujemo da je $\Pi(\sigma) = -\Pi(\sigma(a\ b))$ i time je lema dokazana.

**Propozicija 1.11.** *Predznaci permutacija imaju sljedeća svojstva:*

(*a*) $sgn\, 1 = 1$.

(*b*) *Ako je* $\sigma$ *produkt* $k$ *transpozicija, onda je* $sgn\,\sigma = (-1)^k$.

(*c*) *Za* $\sigma, \tau \in S_n$ *je* $sgn\,\sigma\tau = (sgn\,\sigma)(sgn\,\tau)$.

(*d*) $sgn\,(\sigma^{-1}) = sgn\,\sigma$.

**Dokaz:** Svojstvo (*a*) je očito iz definicije. Za dokaz (*b*) neka je $\sigma = \tau_1 \cdots \tau_k$, pri čemu su $\tau_1, \ldots, \tau_k$ transpozicije. Rekurzivnom primjenom leme 1.3. a na koncu i svojstva (*a*) imamo redom

$$\operatorname{sgn}\sigma = \operatorname{sgn}(\tau_1 \cdots \tau_k) = (-1)\operatorname{sgn}(\tau_1 \cdots \tau_{k-1}) = (-1)^2\operatorname{sgn}(\tau_1 \cdots \tau_{k-2}) =$$

$$= \cdots\cdots = (-1)^{k-1}\operatorname{sgn}\tau_1 = (-1)^k\operatorname{sgn} 1 = (-1)^k.$$

Za dokaz (*c*) koristimo propoziciju 1.9. Ako se $\sigma$ može zapisati kao produkt $k$ transpozicija, a $\tau$ kao produkt $\ell$ transpozicija, onda se očito $\sigma\tau$ može zapisati kao produkt $k+\ell$ transpozicija. Sada prema svojstvu (*b*) imamo

$$\operatorname{sgn}\sigma\tau = (-1)^{k+\ell} = (-1)^k(-1)^\ell = (\operatorname{sgn}\sigma)(\operatorname{sgn}\tau).$$

Napokon, (*d*) slijedi iz (*c*) i (*a*) ako u (*c*) uzmemo $\tau = \sigma^{-1}$.

Napomenimo, da svojstvo (*c*) u propoziciji 1.11. znači da je $\sigma \mapsto \operatorname{sgn}\sigma$ homomorfizam grupe $S_n$ u multiplikativnu grupu $\{1,-1\}$. Taj je homomorfizam surjektivan, a njegovu jezgru čine sve parne permutacije. Posebno, prema propoziciji 1.7. parne permutacije tvore podgrupu od $S_n$. Ta se podgrupa obično označava sa $A_n$.

Predznak permutacije definirali smo samo ako se radi o permutacijama skupa $\{1, \ldots, n\}$. Proširit ćemo sada definiciju i na permutacije proizvoljnog konačnog skupa $T$. Označimo sa $S(T) = \left(T^T\right)^*$ grupu permutacija skupa $T$. Ako je $|T| = n$, postoji bijekcija $\varphi : \{1, \ldots, n\} \to T$. Za svaku permutaciju $\sigma \in S(T)$ tada je $\varphi^{-1}\sigma\varphi \in S_n$. Definiramo

$$\operatorname{sgn}_\varphi \sigma = \operatorname{sgn}(\varphi^{-1}\sigma\varphi), \qquad \sigma \in S(T).$$

Naravno, odmah se postavlja pitanje da li ova definicija ovisi o izboru bijekcije $\varphi : \{1, \ldots, n\} \to T$. Na sreću, ne ovisi. Doista, neka je $\psi : \{1, \ldots, n\} \to T$ također bijekcija. Tada je $\tau = \varphi^{-1}\psi \in S_n$ i $\tau^{-1} = \psi^{-1}\varphi$, pa pomoću svojstava $(c)$ i $(d)$ iz propozicije 1.11. dobivamo za $\sigma \in S(T)$ :

$$\operatorname{sgn}_\psi \sigma = \operatorname{sgn}(\psi^{-1}\sigma\psi) = \operatorname{sgn}(\psi^{-1}\varphi\varphi^{-1}\sigma\varphi\varphi^{-1}\psi) = \operatorname{sgn}(\tau^{-1}\varphi^{-1}\sigma\varphi\tau) =$$

$$= \left(\operatorname{sgn}\left(\tau^{-1}\right)\right)\left(\operatorname{sgn}(\varphi^{-1}\sigma\varphi)\right)(\operatorname{sgn}\tau) = (\operatorname{sgn}\tau)(\operatorname{sgn}_\varphi \sigma)(\operatorname{sgn}\tau) = \operatorname{sgn}_\varphi \sigma.$$

Prema tome, pojam predznaka prenosi se na permutacije bilo kojeg nepraznog konačnog skupa $T$ i definicija ne ovisi o tome na koji način smo numerirali elemente od $T$.

## 1.4 Faktorizacija polinoma

U ovom ćemo odjeljku ustanoviti vjernu analogiju za pojam djeljivosti između cijelih brojeva i polinoma. Promatrat ćemo polinome s koeficijentima iz polja $K$; možemo stalno zamišljati da je $K = \mathbb{C}$ ili $K = \mathbb{R}$ ili $K = \mathbb{Q}$. Pod pojmom *polinom* podrazumijevamo izraze oblika

$$P = \alpha_0 + \alpha_1 X + \cdots + \alpha_{n-1} X^{n-1} + \alpha_n X^n \qquad \text{gdje su} \quad \alpha_0, \alpha_1, \ldots, \alpha_n \in K.$$

Često se polinom $P$ shvaća kao funkcija nezavisne varijable $X$. Međutim, bolje je polinom $P$ identificirati s nizom $(\alpha_0, \alpha_1, \ldots, \alpha_n, 0, 0, \ldots)$ njegovih koeficijenata. Izraz $P = \alpha_0 + \ldots + \alpha_n X^n$ koristimo da se podsjetimo na motivaciju za definiranje raznih računskih operacija s polinomima.

Precizna definicija je sljedeća: **polinom u jednoj varijabli s koeficijentima iz polja** $K$ je beskonačan niz elemenata iz $K$ u kome je samo konačno mnogo članova različito od nule; u tom nizu koeficijente indeksiramo počevši od 0 a ne kao što je s nizovima uobičajeno od 1. Dakle, polinom je niz $(\alpha_k)_{k\in\mathbb{Z}_+}$ takav da za neki $m$ vrijedi $\alpha_k = 0 \ \forall k > m$. Zbrajanje polinoma i množenje polinoma brojem $\lambda \in K$ definiramo *po koordinatama*:

$$(\alpha_k)_{k\in\mathbb{Z}_+} + (\beta_k)_{k\in\mathbb{Z}_+} = (\alpha_k + \beta_k)_{k\in\mathbb{Z}_+}, \qquad \lambda(\alpha_k)_{k\in\mathbb{Z}_+} = (\lambda\alpha_k)_{k\in\mathbb{Z}_+}.$$

Uz te definicije skup svih polinoma postaje vektorski prostor nad poljem $K$. Napomenimo da taj vektorski prostor nije konačnodimenzionalan. Doista, lako se vidi da je beskonačan niz polinoma $(1,0,0,\ldots), (0,1,0,\ldots), (0,0,1,0,\ldots), \ldots$ linearno nezavisan. Štoviše, taj niz tvori bazu vektorskog prostora svih polinoma.

Pored tih dviju operacija definiramo i umnožak dvaju polinoma: ako je $P = (\alpha_k)_{k\in\mathbb{Z}_+}$ i $Q = (\beta_k)_{k\in\mathbb{Z}_+}$, onda je njihov umnožak $PQ$ polinom $(\gamma_k)_{k\in\mathbb{Z}_+}$ čiji su koeficijenti dani sa

$$\gamma_k = \alpha_0\beta_k + \alpha_1\beta_{k-1} + \cdots + \alpha_{k-1}\beta_1 + \alpha_k\beta_0 = \sum_{j=0}^{k} \alpha_j \beta_{k-j}.$$

Uz tako definirane operacije skup svih polinoma u jednoj varijabli s koeficijentima iz $K$ označavamo sa $K[X]$. Lako se vidi da je operacija množenja komutativna, asocijativna i distributivna u odnosu na zbrajanje, tj. ako su $P, Q, R \in K[X]$, onda vrijedi

$$PQ = QP, \qquad P(QR) = (PQ)R, \qquad P(Q+R) = PQ + PR.$$

Dakle, $K[X]$ je komutativan prsten. Taj je prsten unitalan: jedinica je polinom $1 = (1,0,0,\ldots)$. Nula u prstenu $K[X]$ je tzv. *nul−polinom* $0 = (0,0,0,\ldots)$, čiji su svi koeficijenti jednaki nuli.

Ako je $P = (\alpha_k)_{k\in\mathbb{Z}_+} \in K[X]$ i ako je $\alpha_k = 0 \ \forall k > n$ onda pišemo

$$P = \alpha_0 + \alpha_1 X + \alpha_2 X^2 + \cdots + \alpha_{n-1} X^{n-1} + \alpha_n X^n.$$

Takav zapis dobiva precizni smisao, ako svaki element $\lambda \in K$ identificiramo s polinomom $(\lambda, 0, 0, \ldots)$ i stavimo $X = (0,1,0,0,\ldots)$. Doista, tada za svaki prirodan broj $k$ imamo

$$X^k = (\overbrace{0,\ldots,0}^{k}, 1, 0, 0, \ldots).$$

Dakle,

$$\alpha_0 + \alpha_1 X + \alpha_2 X^2 + \cdots + \alpha_{n-1} X^{n-1} + \alpha_n X^n =$$

$$= (\alpha_0,0,0,\ldots) + (0,\alpha_1,0,\ldots) + (0,0,\alpha_2,0,\ldots) + \cdots + (\overbrace{0,\ldots,0}^{n-1}, \alpha_{n-1}, 0, \ldots) + (\overbrace{0,\ldots,0}^{n}, \alpha_n, 0, \ldots) =$$

$$= (\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{n-1}, \alpha_n, 0, 0, \ldots) = P.$$

Ako $P = (\alpha_k)_{k\in\mathbb{Z}_+} \in K[X]$ nije nul−polinom, definiramo **stupanj polinoma** $P$, u oznaci $\deg P$; to je $m \in \mathbb{Z}_+$ takav da je $\alpha_m \neq 0$ i $\alpha_n = 0\ \forall n > m$. **Konstantni polinomi** su po definiciji nul−polinom i polinomi stupnja 0. Uz prije spomenutu identifikaciju $\lambda = (\lambda, 0, 0, \ldots)$ za $\lambda \in K$ konstantni polinomi su upravo elementi polja $K$. Formalno stavljamo $\deg 0 = -\infty$. Uz dogovor

$$m + (-\infty) = (-\infty) + m = (-\infty) + (-\infty) = -\infty, \qquad m \in \mathbb{Z}_+,$$

za $P, Q \in K[X]$ očito vrijedi:

$$\deg (P + Q) \leq \max \{\deg\ P, \deg\ Q\};$$

$$\deg (\lambda P) = \deg\ P \qquad \text{ako je} \quad \lambda \in K, \quad \lambda \neq 0;$$

$$\deg (PQ) = \deg\ P + \deg\ Q.$$

U prvoj od tih formula vrijedi znak jednakosti ako je $\deg P \neq \deg Q$. U trećoj od gornjih formula implicitno je sadržano da za $P, Q \in K[X]$ vrijedi $PQ = 0$ ako i samo ako je ili $P = 0$ ili $Q = 0$. Neposredna posljedica te činjenice je *mogućnost skraćivanja*: ako su $P, Q, R \in K[X]$, $R \neq 0$ i $PR = QR$ onda je $P = Q$. Doista, iz $PR = QR$ slijedi $(P - Q)R = 0$, pa iz $R \neq 0$ slijedi $P - Q = 0$, tj. $P = Q$.

Svaki polinom $P = (\alpha_k)_{k\in\mathbb{Z}_+} = \alpha_0 + \alpha_1 X + \cdots + \alpha_m X^m$ definira funkciju sa $K$ u $K$, koju označavamo istim znakom $P$. Ona je definirana tako da formalnu varijablu $X$ zamijenimo s varijablom iz $K$ :

$$P(\lambda) = \alpha_0 + \alpha_1\lambda + \alpha_2\lambda^2 + \cdots + \alpha_m\lambda^m, \qquad \lambda \in K.$$

Aritmetičke operacije s polinomima definirane su upravo tako da pridruživanje $P \mapsto P(\,\cdot\,)$ poštuje te operacije, tj. za $P, Q \in K[X]$ i za $\alpha, \lambda \in K$ vrijedi

$$(P + Q)(\lambda) = P(\lambda) + Q(\lambda), \qquad (P - Q)(\lambda) = P(\lambda) - Q(\lambda),$$

$$(\alpha P)(\lambda) = \alpha P(\lambda), \qquad (PQ)(\lambda) = P(\lambda)Q(\lambda).$$

Element $\lambda_0 \in K$ zove se **nultočka** ili **korijen polinoma** $P \in K[X]$ ako je $P(\lambda_0) = 0$.

U analogiji s cijelim brojevima definirat ćemo sada pojmove vezane uz djeljivost polinoma. **Djelitelj**, **divizor**, **faktor** ili **mjera** polinoma $A$ je svaki polinom $B$ takav da vrijedi $A = BQ$ za neki $Q \in K[X]$. Tada kažemo i da je $A$ **djeljiv** sa $B$, a također da $B$ **dijeli** $A$. Tu relaciju zapisujemo kao i kod cijelih brojeva: $B|A$. Djeljivost polinoma ima potpuno analogna svojstva kao i djeljivost cijelih brojeva. Prije svega imamo tzv. *dijeljenje s ostatkom*:

**Propozicija 1.12.** *Neka su $A, B \in K[X]$ i $B \neq 0$. Tada postoje jedinstveni $Q, R \in K[X]$ takvi da je $A = BQ + R$ i $\deg R < \deg B$.*

**Dokaz:** Dokažimo najprije egzistenciju takvih polinoma $Q$ i $R$. U slučaju da je $\deg A < \deg B$ egzistencija je evidentna: $Q = 0$, $R = P$.

Ako je $\deg A \geq \deg B$ egzistenciju $Q$ i $R$ dokazujemo matematičkom indukcijom u odnosu na $\deg A \geq \deg B$.

Baza indukcije: Neka je $\deg A = \deg B = m$, tj.

$$A = \alpha_0 + \alpha_1 X + \ldots + \alpha_m X^m, \qquad B = \beta_0 + \beta_1 X + \ldots + \beta_m X^m, \qquad \alpha_m\beta_m \neq 0.$$

Stavimo $Q = \dfrac{\alpha_m}{\beta_m}$ i $R = A - BQ$. Tada vrijedi $A = BQ + R$, a koeficijent od $R$ uz $X^m$ je 0, dakle $\deg R \leq m - 1 < m = \deg B$.

Korak indukcije: Neka je $n > \deg B = m \geq 0$ i pretpostavimo da je egzistencija dokazana u slučaju da je $\deg A \leq n-1$. Neka je $\deg A = n$. Dakle,

$$B = \beta_0 + \beta_1 X + \ldots + \beta_m X^m, \qquad A = \alpha_0 + \alpha_1 X + \ldots + \alpha_n X^n, \qquad \alpha_n \beta_m \neq 0.$$

Stavimo $A' = A - \dfrac{\alpha_n}{\beta_m} X^{n-m} B$. Tada je $\deg A' \leq n-1 < n$, pa po pretpostavci indukcije postoje $Q', R \in K[X]$ takvi da je $A' = BQ' + R$ i da je $\deg R < m$. Stavimo li $Q = \dfrac{\alpha_n}{\beta_m} X^{n-m} + Q'$, slijedi $A = BQ + R$ i $\deg R < m$.

Time je dokazana egzistencija polinoma $Q$ i $R$ takvih da je $A = BQ + R$ i $\deg R < \deg B$. Dokažimo još jedinstvenost takvih polinoma $Q$ i $R$. Neka su $Q'$ i $R'$ polinomi takvi da je $A = BQ' + R'$ i $\deg R' < \deg B$. Sada iz $BQ + R = = BQ' + R'$ slijedi $(Q - Q')B = R' - R$, pa je $\deg (R' - R) = \deg (Q - Q') + \deg B$. Kada bi bilo $\deg (S - S') \geq 0$, slijedilo bi $\deg (R' - R) \geq \deg B$, a to je nemoguće zbog $\deg R < \deg B$ i $\deg R' < \deg B$. Stoga mora biti $\deg (Q - Q') = -\infty$, tj. $Q - Q' = 0$ ili $Q = Q'$. Slijedi $R' - R = (Q - Q')B = 0$, tj. $R = R'$. Posebno, ako su polinomi $P$ i $Q$ različiti od nule onda je i polinom $PQ$ različit od nule.

**Propozicija 1.13.** *Neka je $\lambda_0 \in K$ nultočka polinoma $P \in K[X]$. Tada je polinom $P$ djeljiv s polinomom $X - \lambda_0$, tj. postoji $Q \in K[X]$ takav da je $P = (X - \lambda_0)Q$. Ako je $P \neq 0$, vrijedi* $\deg Q = \deg P - 1$.

**Dokaz:** Prema propoziciji 1.12. postoje polinomi $Q, R \in K[X]$ takvi da je

$$P = (X - \lambda_0)Q + R \qquad \text{i} \qquad \deg R < \deg (X - \lambda_0) = 1.$$

Dakle, stupanj polinoma $R$ je ili 0 ili $-\infty$, što znači da je $R$ konstantni polinom, odnosno, $R = \alpha \in K$. Sada imamo $P = (X - \lambda_0)Q + \alpha$, a kako je $\lambda_0$ nultočka polinoma $P$, nalazimo:

$$0 = P(\lambda_0) = (\lambda_0 - \lambda_0)Q(\lambda_0) + \alpha = \alpha \qquad \Longrightarrow \qquad \alpha = 0 \qquad \Longrightarrow \qquad P = (T - \lambda_0)Q.$$

Napokon, kako je stupanj produkta polinoma jednak sumi stupnjeva tih polinoma, imamo

$$\deg P = \deg ((X - \lambda_0)Q) = \deg (X - \lambda_0) + \deg Q = 1 + \deg Q,$$

dakle, $\deg Q = \deg P - 1$.

Propozicija 1.13. ima sljedeću dalekosežnu posljedicu:

**Teorem 1.4.** *Neka je $P \in K[X]$ i neka su $\lambda_1, \lambda_2, \ldots, \lambda_n \in K$ međusobno različite nultočke polinoma $P$. Tada je polinom $P$ djeljiv s polinomom $(X - \lambda_1)(X - \lambda_2) \cdots (X - \lambda_n)$. Posebno, ako je $P \neq 0$ i ako je $m = \deg P$, polinom $P$ ima u polju $K$ najviše $m$ nultočaka.*

**Dokaz:** Tvrdnju ćemo dokazati matematičkom indukcijom u odnosu na $n$. Baza indukcije $n = 1$ je upravo tvrdnja propozicije 1.13. Provedimo sada korak indukcije i pretpostavimo da je $n \geq 2$ i da je već dokazano da je polinom $P$ djeljiv s polinomom $(X - \lambda_1)(X - \lambda_2) \cdots (X - \lambda_{n-1})$. Neka je $S \in K[X]$ takav da je

$$P = (X - \lambda_1)(X - \lambda_2) \cdots (X - \lambda_{n-1})S. \tag{1.4}$$

Uvrstimo sada u tu jednakost dvaju polinoma $\lambda_n$ umjesto formalne varijable $X$. Kako je $\lambda_n$ nultočka polinoma $P$, slijedi:

$$(\lambda_n - \lambda_1)(\lambda_n - \lambda_2) \cdots (\lambda_n - \lambda_{n-1})S(\lambda_n) = 0.$$

Po pretpostavci su nultočke $\lambda_1, \lambda_2, \ldots, \lambda_{n-1}, \lambda_n$ međusobno različite, pa imamo $\lambda_n - \lambda_1 \neq 0$, $\lambda_n - \lambda_2 \neq 0$, $\ldots$ , $\lambda_n - \lambda_{n-1} \neq 0$. Stoga iz gornje jednakosti slijedi da je $S(\lambda_n) = 0$, tj. $\lambda_n$ je nultočka polinoma $S$. Sada iz propozicije 1.13. slijedi da je polinom $S$ djeljiv s polinomom $X - \lambda_n$, tj. postoji polinom $Q \in K[X]$ takav da je $S = (X - \lambda_n)Q$. Odatle i iz (1.4) slijedi

$$P = (X - \lambda_1)(X - \lambda_2) \cdots (X - \lambda_{n-1})(X - \lambda_n)Q.$$

Ako je $m = \deg P$, odavde je $m = n + \deg Q$, dakle $n \leq m$. Time je teorem 1.4. dokazan.

Sada možemo pobliže razmotriti vezu između polinoma i polinomijalnih funkcija. Svakom polinomu $P \in K[X]$ je uvrštavanjem varijable $\lambda \in K$ umjesto formalne varijable $X$ pridružena polinomijalna funkcija $\lambda \mapsto P(\lambda)$. Postavlja se pitanje: Da li polinomijalna funkcija $\lambda \mapsto P(\lambda)$ u potpunosti određuje polinom $P$? Drugim riječima, postoje li međusobno različiti polinomi $P_1$ i $P_2$ takvi da je $P_1(\lambda) = P_2(\lambda)\ \forall \lambda \in K$? Stavimo li $P = P_1 - P_2$, vidimo da se isto pitanje može postaviti na sljedeći način: Postoji li polinom $P \in K[X]$, $P \neq 0$, takav da je $P(\lambda) = 0\ \forall \lambda \in K$?

Isto pitanje možemo formulirati i kao pitanje da li je određeni homomorfizam prstenova injektivan ili nije. Naime, polinomi u jednoj varijabli s koeficijentima iz polja $K$ čine prsten $K[X]$, a skup svih funkcija $K^K$ sa $K$ u $K$ je također prsten u odnosu na operacije zbrajanja i množenja definirane *po točkama*:

$$(f + g)(\lambda) = f(\lambda) + g(\lambda), \qquad (fg)(\lambda) = f(\lambda)g(\lambda), \qquad f, g \in K^K,\ \lambda \in K.$$

Pridruživanje polnomijalnih funkcija polinomima je zapravo preslikavanje $\Phi : K[X] \to K^K$ :

$$(\Phi(P))(\lambda) = \alpha_0 + \alpha_1\lambda + \cdots + \alpha_m\lambda^m, \qquad \text{za} \quad P = \alpha_0 + \alpha_1 X + \cdots + \alpha_m X^m \in K[X], \quad \lambda \in K.$$

Poznate jednakosti $(P + Q)(\lambda) = P(\lambda) + Q(\lambda)$ i $(PQ)(\lambda) = P(\lambda)Q(\lambda)$ znače da je $\Phi(P + Q) = \Phi(P) + \Phi(Q)$ i $\Phi(PQ) = \Phi(P)\Phi(Q)$, dakle $\Phi$ je homomorfizam prstenova. Prema tome postavljeno pitanje može se i ovako formulirati: Da li je homomorfizam $\Phi$ prstena $K[X]$ u prsten $K^K$ injektivan?

**Teorem 1.5.** *Neka je $K$ polje. Homomorfizam $\Phi$ prstena polinoma $K[X]$ u prsten funkcija $K^K$, koji polinomu $P$ pridružuje polinomijalnu funkciju $\lambda \mapsto P(\lambda)$, je injektivan ako i samo ako je polje $K$ beskonačno. Ako je polje $K$ konačno i ima $m$ elemenata, $K = \{\lambda_1, \lambda_2, \ldots, \lambda_m\}$, onda je jezgra homomorfizma $\Phi$ skup svih polinoma koji su djeljivi s polinomom $(X - \lambda_1)(X - \lambda_2) \cdots (X - \lambda_m)$ :*

$$\ker \Phi = \{(X - \lambda_1)(X - \lambda_2) \cdots (X - \lambda_m)Q;\ \ Q \in K[X]\}.$$

**Dokaz:** Pretpostavimo prvo da je polje $K$ beskonačno i neka je $P \in \ker \Phi$. Tada je $P(\lambda) = 0$ $\forall \lambda \in K$, dakle, polinom $P$ ima beskonačno mnogo nultočaka. Prema teoremu 1.4. zaključujemo da mora biti $P = 0$. Time je dokazano da je $\ker \Phi = \{0\}$, tj. homomorfizam $\Phi$ je injektivan.

Pretpostavimo sada da je polje $K$ konačno i da ima $m$ elemenata: $K = \{\lambda_1, \lambda_2, \ldots, \lambda_m\}$. Stavimo

$$P = (T - \lambda_1)(T - \lambda_2) \cdots (T - \lambda_m).$$

Tada je svaka točka iz $K$ nultočka polinoma $P$, a to znači da je $P \in \ker \Phi$. Odatle slijedi da je $\{PQ;\ \ Q \in K[X]\} \subseteq \ker\ \Phi$. Obrnuta inkluzija je posljedica teorema 1.4. Doista, neka je $R \in \ker \Phi$. Tada je $R(\lambda_j) = 0$ za $j = 1, 2, \ldots, m$, tj. $\lambda_1, \lambda_2, \ldots, \lambda_m$ su nultočke polinoma $R$. Sada po teoremu 1.4. slijedi da je polinom $R$ djeljiv s polinomom $P$, tj. $R = PQ$ za neki $Q \in K[X]$. Dakle, vrijedi i inkluzija $\ker\ \Phi \subseteq \{PQ;\ \ Q \in K[X]\}$. Time je dokazana jednakost $\ker \Phi = \{PQ;\ \ Q \in K[X]\}$.

Analogno kao za cijele brojeve definiramo najveću zajedničku mjeru i za polinome. U ovom će se slučaju riječ *najveći* odnositi na stupanj polinoma. Definicija je sljedeća: Neka su $P, Q \in K[X]$ polinomi koji nisu oba jednaki nuli. **Najveća zajednička mjera** polinoma $P$ i $Q$ je polinom $M$ koji je mjera polinoma $P$ i $Q$, tj. $M|P$ i $M|Q$, koja među svim zajedničkim mjerama tih dvaju polinoma ima najveći stupanj. Dakle, $M$ ima svojstvo da iz $N|P$ i $N|Q$ slijedi $\deg N \leq \deg M$.

Sasvim analogno kao što u slučaju cijelih brojeva iz propozicije 1.1. o dijeljenju s ostatkom dobivamo Euklidov algoritam, tako i u slučaju polinoma iz propozicije 1.12. o dijeljenju polinoma s ostatkom dobivamo **Euklidov algoritam za polinoma**. Taj se algoritam ponovo sastoji od uzastopne primjene dijeljenja s ostatkom sve dok ostatak ne iščezne. Dakle, ako su $A, B \in K[X]$ i $B \neq 0$ (tj. $\deg B \geq 0$) onda imamo

$$\begin{array}{rcll} A & = & BQ_1 + R_1 & 0 \leq \deg R_1 < \deg B \\ B & = & R_1Q_2 + R_2, & 0 \leq \deg R_2 < \deg R_1, \\ R_1 & = & R_2Q_3 + R_3, & 0 \leq \deg R_3 < \deg R_2, \\ & \vdots & & \\ R_{n-2} & = & R_{n-1}Q_n + R_n, & 0 \leq \deg R_n < \deg R_{n-1}, \\ R_{n-1} & = & R_nQ_{n+1}. & \end{array}$$

Pri svakom dijeljenju ostatak ima stupanj striktno manji od ostatka pri prethodnom dijeljenju. Stoga i u ovom slučaju Euklidov algoritam sigurno završava: nakon konačno mnogo dijeljenja s ostatkom doći ćemo do djeljivosti tj. do dijeljenja bez ostatka. Naravno, opet u slučaju $B|A$ Euklidov algoritam završava u prvom koraku, tj. $n = 0$ :

$$A = BQ_1.$$

Ako je $n = 1$, tj. ako $B \nmid A$, ali $R_1|B$, onda Euklidov algoritam završava u drugom koraku:

$$\begin{array}{rcll} A & = & BQ_1 + R_1, & 0 \leq \deg R_1 < \deg B, \\ B & = & R_1Q_2. & \end{array}$$

Kao i kod cijelih brojeva imamo

**Propozicija 1.14.** *Neka su $A, B \in K[X]$ i $B \neq 0$.*

(a) *$R_n$ je najveća zajednička mjera polinoma $A$ i $B$.*

(b) *Ako je $D \in K[X]$ zajednička mjera od $A$ i $B$, tj. $D|A$ i $D|B$, onda vrijedi $D|R_n$.*

(c) *Najveća zajednička mjera polinoma $A$ i $B$ jedinstvena je do na umnožak elementom iz $K$ različitim od nule; preciznije, ako je $M$ najveća zajednička mjera od $A$ i $B$ onda je i $D \in K[X]$ najveća zajednička mjera od $A$ i $B$ ako i samo ako vrijedi $D = \lambda M$ za neki $\lambda \in K \setminus \{0\}$.*

(d) *Za svaku najveću zajedničku mjeru $D$ od $A$ i $B$ postoje polinomi $P, Q \in K[X]$ takvi da je $AP + BQ = D$.*

**Dokaz:** Dokaz je analogan dokazu propozicije 1.2.:

(1) Najprije se potpuno analogno koraku (1) u dokazu propozicije 1.2. dokazuje da iz Euklidovog algoritma slijedi $R_n|A$ i $R_n|B$, dakle, $R_n$ je zajednička mjera od $A$ i $B$.

(2) Zatim se potpuno analogno koraku (2) u dokazu propozicije 1.2. dokazuje da postoje $P, Q \in K[X]$ takvi da je $R_n = AP + BQ$.

(3) Ako je $D \in K[X]$ zajednička mjera mjera od $A$ i $B$, tj. $D|A$ i $D|B$, onda pomoću (2) nalazimo da $D|R_n$. Time je dokazano $(b)$. Nadalje, tada je $\deg D \leq \deg R_n$, pa zaključujemo da je $R_n$ najveća zajednička mjera od $A$ i $B$, tj. dokazano je $(a)$.

(4) Tvrdnja $(c)$ slijedi iz očigledne činjenice da za polinome $R, S \in K[X]$ jednakog stupnja vrijedi $R|S$ ako i samo ako je $S = \lambda R$ za neki $\lambda \in K \setminus \{0\}$. Odatle i iz (2) slijedi i tvrdnja $(d)$.

Može nas smetati da kod polinoma najveća zajednička mjera nije jedinstvena kao što je to bilo kod cijelih brojeva. Radi se o tome što smo kod cijelih brojeva najveću zajedničku mjeru definirali kao *prirodan broj* a ne samo kao *cijeli broj*. Skup prirodnih brojeva $\mathbb{N}$ ima svojstvo da za $m, n \in \mathbb{N}$ vrijedi $m|n$ i $n|m$ ako i samo ako je $n = m$, dok za cijele brojeve imamo samo jedinstvenost do na predznak: za $n, m \in \mathbb{Z} \setminus \{0\}$ vrijedi $n|m$ i $m|n$ ako i samo ako je $m = \pm n$. U pozadini tog svojstva je činjenica da je multiplikativna grupa $\mathbb{Z}^* = \{1, -1\}$ i da za svaki $m \in \mathbb{Z} \setminus \{0\}$ postoji jedinstven $n \in \mathbb{N}$ i $q \in \mathbb{Z}^*$ takvi da je $m = qn$; naravno, $n = |m|$, a $q = 1$ ako je $m > 0$ i $q = -1$ ako je $m < 0$.

Potpuno analognu ulogu koju prirodni brojevi $\mathbb{N}$ igraju u prstenu $\mathbb{Z}$ u slučaju polinoma igraju tzv. normirani polinomi. **Polinom** $P = (\alpha_n)_{n\geq 0}$ zove se **normiran**, ako je $P \neq 0$, tj. $m = \deg P \geq 0$, i ako je $\alpha_m = 1$. Dakle,

$$P = X^m + \alpha_{m-1}X^{m-1} + \ldots + \alpha_1 X + \alpha_0.$$

Skup svih normiranih polinoma označavat ćemo sa $K_1[X]$.

Multiplikativna grupa u prstenu polinoma je $K[X]^* = K^* = K \setminus \{0\}$ pa stvarno imamo analogiju s cijelim brojevima: za svaki polinom $P \neq 0$ postoje jedinstven $N \in K_1[X]$ i jedinstven $\lambda \in K[X]^* = K \setminus \{0\}$ takvi da je $P = \lambda N$. Naime, ako je $n = \deg P$ i

$$P = \alpha_0 + \alpha_1 X + \cdots + \alpha_{n-1}X^{n-1} + \alpha_n X^n, \qquad \alpha_n \neq 0,$$

tada je

$$\lambda = \alpha_n \qquad \text{i} \qquad N = X^n + \frac{\alpha_{n-1}}{\alpha_n}X^{n-1} + \cdots + \frac{\alpha_1}{\alpha_n}X + \frac{\alpha_0}{\alpha_n}.$$

Naravno, i za polinome vrijedi kao i za cijele brojeve:

$$P, Q \in K[X] \setminus \{0\}, \qquad P|Q \quad \text{i} \quad Q|P \qquad \Longleftrightarrow \qquad Q = \lambda P \quad \text{za neki} \quad \lambda \in K[X]^* = K \setminus \{0\},$$

$$P, Q \in K_1[X], \qquad P|Q \quad \text{i} \quad Q|P \qquad \Longleftrightarrow \qquad P = Q.$$

Stoga je i za polinome najveća zajednička mjera jedinstvena, ako zahtijevamo da se radi o normiranom polinomu. Jedinstvenu najveću zajedničku mjeru polinoma $A$ i $B$ koja je normirana označavat ćemo sa $GCD(A, B)$.

Analogon prostih brojeva u prstenu polinoma $K[X]$ igraju tzv. ireducibilni polinomi. Pri tome se $P \in K[X]$ zove **ireducibilan polinom**, ako je je $\deg P > 0$ i ako ne postoje nekonstantni polinomi $A$ i $B$ takvi da je $P = AB$. Skup svih ireducibilnih normiranih polinoma označavat ćemo sa $K_i[X]$. Nadalje, za polinome $A$ i $B$ kažemo da su **relativno prosti** ako je $GCD(A, B) = 1$. Sasvim analogno kao i za cijele brojeve dokazuju se sljedeće četiri posljedice propozicije 1.14.:

**Korolar 1.8.** *Polinomi $A, B \in K[X]$ su relativno prosti ako i samo ako postoje $P, Q \in K[X]$ takvi da je $AP + BQ = 1$.*

**Dokaz:** Ako su $A$ i $B$ relativno prosti, tj. ako je $GCD(A, B) = 1$, onda prema tvrdnji $(d)$ propozicije 1.14. postoje polinomi $P, Q \in K[X]$ takvi da je $AP+BQ = 1$. Obratno, pretpostavimo da je $AP + BQ = 1$ za neke polinome $P, Q \in K[X]$. Tada svaka zajednička mjera od $A$ i $B$ dijeli 1. To znači da je 1 jedina normirana zajednička mjera od $A$ i $B$, tj. $GCD(A, B) = 1$.

**Korolar 1.9.** *Neka su polinomi $A, B, C \in K[X]$ takvi da su $A$ i $B$ relativno prosti i da su $A$ i $C$ relativno prosti. Tada su $A$ i umnožak $BC$ relativno prosti.*

**Dokaz:** Prema tvrdnji $(d)$ propozicije 1.14. postoje $P, Q, R, S \in K[X]$ takvi da je

$$AP + BQ = 1 \qquad \text{i} \qquad AR + CS = 1.$$

Tada za $U = APR + CPS + BQR$ i $V = QS$ nalazimo

$$AU + (BC)V = A^2PR + ACPS + ABQR + BCQS = (AP + BQ)(AR + CS) = 1.$$

Prema korolaru 1.8. slijedi $GCD(A, BC) = 1$, tj. $A$ i $BC$ su relativno prosti.

**Korolar 1.10.** *Neka su $A, B \in K[X]$ relativno prosti i neka je $C \in K[X]$ takav da $A|BC$. Tada $A|C$.*

**Dokaz:** Prema korolaru 1.8. postoje $P, Q \in K[X]$ takvi da je $AP + BQ = 1$. Odatle je $C = CAP + CBQ$, pa ako $A|(BC)$, tj. $BC = AS$ za neki $S \in K[X]$, tada je

$$C = CAP + CBQ = CAP + ASQ = A(CP + SQ).$$

Dakle, $A|C$.

**Korolar 1.11.** *Neka su $A, B \in K[X]$ relativno prosti i neka je $C \in K[X]$ takav da $A|C$ i $B|C$. Tada $(AB)|C$.*

**Dokaz:** Prema korolaru 1.8. postoje $P, Q \in K[X]$ takvi da je $AP + BQ = 1$. Neka su $R, S \in K[X]$ takvi da je $C = AR = BS$. Tada nalazimo

$$C = CAP + CBQ = BSAP + ARBQ = AB(SP + RQ).$$

Dakle, $(AB)|C$.

Nadalje, za polinome pomoću korolara 1.10. dobivamo sljedeći analogon leme 1.1.:

**Lema 1.4.** *Ako su $A_1, \ldots, A_s \in K[X]$, $s \geq 2$, i ako za $P \in K_i[X]$ vrijedi $P|(A_1 \cdots A_s)$, onda $P|A_i$ za neki $i$.*

**Dokaz** provodimo matematičkom indukcijom u odnosu na $s \geq 2$.

(1) Pretpostavimo najprije da je $s = 2$, dakle, $P|(A_1A_2)$ i $P \nmid A_1$. Budući da su $P$ i 1 jedini normirani djelitelji od $P$, slijedi $GCD(A_1, P) = 1$. Sada iz korolara 1.10. (za $A = P$, $B = A_1$ i $C = A_2$) slijedi $P|A_2$.

(2) Provedimo sada i korak indukcije. Neka je $s \geq 3$ i pretpostavimo da je lema dokazana za slučaj umnoška od $s-1$ faktora. Ako $P$ dijeli umnožak $A_1A_2 \cdots A_s) = A_1(A_2 \cdots A_s)$, onda prema (1) vrijedi $P|A_1$ ili $P|(A_2 \cdots A_s)$. U ovom drugom slučaju iz pretpostavke indukcije slijedi $P|A_i$ za neki $i \in \{2, \ldots, s\}$.

Vrlo slično kao što se iz leme 1.1. dokazuje teorem 1.1. iz leme 1.4. se dokazuje teorem o jedinstvenoj faktorizaciji u prstenu polinoma:

**Teorem 1.6.** *Neka je $P \in K[X]$, $\deg P \geq 1$. Tada postoje $r \in \mathbb{N}$, $\lambda \in K^*$ i $P_1, \ldots, P_r \in K_i[X]$ takvi da je*

$$P = \lambda P_1 \cdots P_r.$$

*Ako su i $s \in \mathbb{N}$, $\mu \in K^*$ i $Q_1, \ldots, Q_s \in K_i[X]$ takvi da je*

$$P = \mu Q_1 \cdots Q_s,$$

*tada je $s = r$, $\mu = \lambda$ i postoji permutacija $\sigma \in S_r$ takva da je $P_i = Q_{\sigma(i)}$ za $i = 1, \ldots, r$.*

**Dokaz:** Prije svega, za svaki $P \in K[X]$ stupnja $\geq 1$ postoji jedinstven $\lambda \in K^*$ i jedinstven $P' \in K_1[X]$ takvi da je $P = \lambda P'$. Stoga u daljnjem možemo pretpostavljati da je polinom $P$ normiran.

Dokaz egzistencije faktorizacije tada dokazujemo indukcijom po $\deg P \geq 1$. Ako je $\deg P = 1$, tada je polinom $P$ ireducibilan, pa možemo uzeti $r = 1$ i $P_1 = P$. Pretpostavimo sada da je $n \geq 2$ i da je egzistencija faktorizacije dokazana za polinome stupnja manjeg od $n$. Neka je $\deg P = n$. Ako je polinom $P$ ireducibilan, opet imamo faktorizaciju sa samo jednim faktorom: $r = 1$ i $P_1 = P$. Ako polinom $P$ nije ireducibilan, onda postoje $A, B \in K_1[X]$ takvi da je $P = AB$, $\deg A \geq 1$ i $\deg B \geq 1$. Tada su $\deg A < n$ i $\deg B < n$, pa po pretpostavci indukcije polinomi $A$ i $B$ imaju faktorizacije u ireducibilne faktore. Skupimo li te dvije faktorizacije zajedno, dobivamo faktorizaciju umnoška $AB = P$.

Dokažimo sada jedinstvenost. Pretpostavimo da je

$$P = P_1 \cdots P_r = Q_1 \cdots Q_s,$$

pri čemu su $P_1, \ldots, P_r, Q_1, \ldots, Q_s \in K_i[X]$. Možemo pretpostaviti da je $r \leq s$ (ako nije, zamijenimo uloge $P_i$ i $Q_j$). Imamo $P_1 | P$, tj. $P_1 | (Q_1 \cdots Q_s)$. Sada iz leme 1.4. slijedi da $P_1$ dijeli jedan od faktora, tj. postoji $j \in \{1, \ldots, s\}$ takav da $P_1 | Q_j$. Budući da su $P_1$ i $Q_j$ ireducibilni i normirani, slijedi $P_1 = Q_j$. Stavimo tada $j = \sigma(1)$. Gornju jednakost možemo skratiti sa $P_1$, pa dobivamo

$$P_2 \cdots P_r = \prod_{1 \leq i \leq s,\, i \neq j} Q_i.$$

Jednako rezoniranje pokazuje da postoji $i \in \{1, \ldots, s\} \setminus \{j\}$ takav da je $P_2 = Q_i$. Tada stavljamo $s(2) = i$. Korak po korak dolazimo do injekcije $\{1, \ldots, r\} \to \{1, \ldots, s\}$ takve da vrijedi $P_k = Q_{\sigma(k)}$ za $k = 1, \ldots, r$. Kad bi bilo $s > r$, imali bismo

$$P_1 \cdots P_r = P_1 \cdots P_r Q \qquad \Longrightarrow \qquad 1 = Q,$$

gdje je $Q$ umnožak svih polinoma $Q_j$ za $j \in \{1, \ldots, s\} \setminus \{\sigma(1), \ldots, \sigma(r)\}$. No to je nemoguće jer je $\deg Q_j \geq 1 \ \forall j$, dakle, $\deg Q \geq s - r > 0$. Ova kontradikcija pokazuje da je $s = r$, dakle,

$$\sigma \in S_r \qquad \text{i} \qquad P_i = Q_{\sigma(i)} \quad \forall i \in \{1, \ldots, r\}$$

i time je dokazana tvrdnja o jedinstvenosti.

Skup ireducibilnih normiranih polinoma vrlo je jednostavno opisati ako je polje $K$ algebarski zatvoreno. Pri tome kažemo da je **polje $K$ algebarski zatvoreno** ako svaki nekonstantni polinom $P \in K[X]$ ima u polju $K$ nultočku:

$$P \in K[X], \quad \deg P \geq 1 \qquad \Longrightarrow \qquad \exists \alpha \in K \quad \text{takav da je} \quad P(\alpha) = 0.$$

Primjer algebarski zatvorenog polja je polje $\mathbb{C}$ kompleksnih brojeva; to je tvrdnja tzv. *Fundamentalnog teorema algebre* koji je tema sljedećeg odjeljka.

**Propozicija 1.15.** *Ako je polje $K$ algebarski zatvoreno onda je*

$$K_i[X] = \{X - \alpha;\ \alpha \in K\}.$$

**Dokaz:** Primijetimo najprije da je za svako polje $K$ i za svaki $\alpha \in K$ polinom $X - \alpha$ ireducibilan:

$$\{X - \alpha;\ \alpha \in K\} \subseteq K_i[X].$$

Doista, svaki takav polinom je stupnja 1, pa ne može biti prikazan kao umnožak nekonstantnih polinoma.

Neka je $P \in K_i[X]$. Neka je $\alpha \in K$ takav da je $P(\alpha) = 0$. Po propoziciji 1.13. polinom $P$ djeljiv je s polinomom $X - \alpha$, tj. postoji $Q \in K[X]$ takav da je $P = (X - \alpha)Q$. Kako je polinom $P$ ireducibilan slijedi $Q = 1$, odnosno $P = X - \alpha$. Time je dokazana i obrnuta inkluzija $K_i[X] \subseteq \{X - \alpha;\ \alpha \in K\}$, dakle vrijedi jednakost:

$$K_i[X] = \{X - \alpha;\ \alpha \in K\}.$$

## 1.5 Fundamentalni teorem algebre

Polinom $P = X^2 + 1 \in \mathbb{R}[X]$ nema nultočki u polju $\mathbb{R}$ realnih brojeva. Međutim, ako polje $\mathbb{R}$ proširimo do polja $\mathbb{C}$ kompleksnih brojeva, dolazimo do dvije nultočke $i$ i $-i$. U stvari, korak po korak postupno smo proširenjem brojevnih sustava

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

omogućavali rješivost sve općenitijih i općenitijih jednadžbi. Važnost polja $\mathbb{C}$ kompleksnih brojeva jest u tome da nam nisu potrebna daljnja proširenja: u polju $\mathbb{C}$ svaka polinomijalna jednadžba ima rješenje. Upravo to se zove **Fundamentalni teorem algebre**:

**Teorem 1.7.** *Neka je $P$ polinom jedne varijable s koeficijentima iz polja $\mathbb{C}$ koji je nekonstantan, tj.* $\deg P \geq 1$. *Tada postoji $\alpha \in \mathbb{C}$ takav da je $P(\alpha) = 0$.*

Prvi potpun dokaz ovog teorema sadržan je u Gaussovoj doktorskoj disertaciji 1799. godine. Kasnije je Gauss pronašao još tri dokaza tog teorema, svaki baziran na različitim idejama i argumentima. Mi ćemo prikazati vjerojatno najjednostavniji dokaz Fundamentalnog teorema algebra, koji se bazira na teoriji analitičkih funkcija kompleksne varijable. Iskoristit ćemo tzv. **Liouvilleov teorem**:

**Teorem 1.8.** *Neka je $f : \mathbb{C} \to \mathbb{C}$ funkcija koja je analitička na cijeloj kompleksnoj ravnini $\mathbb{C}$ i koja je ograničena, tj. takva da postoji $M > 0$ takav da je $|f(\lambda)| \leq M \ \ \forall \lambda \in \mathbb{C}$. Tada je funkcija $f$ konstantna.*

**Dokaz teorema 1.7.:** Dokazujemo metodom suprotnpog. Dakle, pretpostavimo da je $P \in \mathbb{C}[X]$ nekonstantni polinom i da je $P(\alpha) \neq 0 \ \ \forall \alpha \in \mathbb{C}$. Možemo pretpostaviti da je polinom $P$ normiran:

$$P = X^m + \alpha_1 X^{m-1} + \cdots + \alpha_{m-1} X + \alpha_m.$$

Budući da se analitička funkcija $\lambda \mapsto P(\lambda)$ nigdje ne poništava, to je i njena recipročna vrijednost

$$f(\lambda) = \frac{1}{P(\lambda)}, \qquad \lambda \in \mathbb{C},$$

funkcija koja je analitička na cijeloj kompleksnoj ravnini.

Dokazat ćemo da je funkcija $f$ ograničena. Prije svega, neka je

$$N = \max \left\{ \sqrt[j]{|\alpha_j|};\ j = 1, 2, \ldots, m \right\}.$$

Ako je $\lambda \in \mathbb{C}$ i $|\lambda| > 2mN$, onda za svaki $j \in \{1, \ldots, m\}$ vrijedi

$$|\lambda| \geq 2m\sqrt[j]{|\alpha_j|} \qquad \Longrightarrow \qquad |\lambda^j| \geq (2m)^j |\alpha_j| \qquad \Longrightarrow \qquad \frac{|\alpha_j|}{|\lambda^j|} \leq \frac{1}{(2m)^j} \leq \frac{1}{2m},$$

pa slijedi

$$\left| \frac{\alpha_1}{\lambda} + \frac{\alpha_2}{\lambda^2} + \cdots + \frac{\alpha_m}{\lambda^m} \right| \leq \frac{|\alpha_1|}{|\lambda|} + \frac{|\alpha_2|}{|\lambda^2|} + \cdots + \frac{|\alpha_m|}{|\lambda^m|} \leq \frac{m}{2m} = \frac{1}{2}.$$

Stoga za svaki takav $\lambda$ vrijedi

$$\left| 1 + \frac{\alpha_1}{\lambda} + \frac{\alpha_2}{\lambda^2} + \cdots + \frac{\alpha_m}{\lambda^m} \right| \geq 1 - \left| \frac{\alpha_1}{\lambda} + \frac{\alpha_2}{\lambda^2} + \cdots + \frac{\alpha_m}{\lambda^m} \right| \geq 1 - \frac{1}{2} = \frac{1}{2},$$

a odatle nalazimo

$$|f(\lambda)| = \frac{1}{|\lambda^m + \alpha_1\lambda^{m-1} + \cdots + \alpha_m|} = \frac{\frac{1}{|\lambda|^m}}{\left|1 + \frac{\alpha_1}{\lambda} + \frac{\alpha_2}{\lambda^2} + \cdots + \frac{\alpha_m}{\lambda^m}\right|} \leq \frac{\frac{1}{(2mN)^m}}{\frac{1}{2}} = \frac{2}{(2mN)^m}.$$

Dakle, vrijedi

$$|\lambda| > 2mN \qquad \Longrightarrow \qquad |f(\lambda)| \leq \frac{2}{(2mN)^m}. \tag{1.5}$$

S druge strane, neprekidna funkcija $f$ na zatvorenom krugu $\{\lambda \in \mathbb{C};\ |\lambda| \leq 2mN\}$ je ograničena, tj.

$$R = \sup\{|f(\lambda)|;\ \lambda \in \mathbb{C},\ |\lambda| \leq 2mN\} < +\infty$$

Stoga vrijedi

$$|\lambda| \leq 2mN \qquad \Longrightarrow \qquad |f(\lambda)| \leq R. \tag{1.6}$$

Ako stavimo $M = \max\left\{\frac{2}{(2mN)^m}, R\right\}$, iz (1.5) i (1.6) vidimo da vrijedi

$$|f(\lambda| \leq M \qquad \forall \lambda \in \mathbb{C}.$$

Sada iz Liouvilleovog teorema 1.7. slijedi da je funkcija $f$ konstantna. No to nije moguće, jer je $P$ po pretpostavci nekonstantan polinom. Ova kontradikcija pokazuje da je pretpostavka bila pogrešna: nije moguće da nekonstantan polinom $P \in \mathbb{C}[X]$ nema nijednu nultočku u polju $\mathbb{C}$. Time je Fundamentalni teorem algebre dokazan.

Prema propoziciji 1.15. skup svih normiranih ireducibilnih polinoma s kompleksnim koeficijentima je

$$\mathbb{C}_i[X] = \{X - \lambda;\ \lambda \in \mathbb{C}\}.$$

Odatle možemo odrediti i skup svih normiranih ireducibilnih polinoma s realnim koeficijentima:

**Propozicija 1.16.** *Za polje $\mathbb{R}$ realnih brojeva je*

$$\mathbb{R}_i[X] = \{X - \lambda;\ \lambda \in \mathbb{R}\} \cup \{X^2 + \alpha X + \beta;\ \alpha, \beta \in \mathbb{R},\ \alpha^2 < 4\beta\}.$$

**Dokaz:** Prema početku dokaza propozicije 1.15. imamo $X - \lambda \in \mathbb{R}_i[X]$ za svaki $\lambda \in \mathbb{R}$. Neka je

$$P \in \mathbb{R}_i[X] \setminus \{X - \lambda;\ \lambda \in \mathbb{R}\}.$$

Tada $P$ nema realne nultočke; doista, inače bismo kao u dokazu propozicije 1.15. mogli zaključiti da je $P = X - \lambda$ za neki $\lambda \in \mathbb{R}$. Zbog Fundamentalnog teorema algebre tada postoji $\lambda \in \mathbb{C}\setminus\mathbb{R}$ takav da je $P(\lambda) = 0$. Budući da polinom $P$ ima realne koeficijente odatle slijedi da je $P\left(\overline{\lambda}\right) = \overline{P(\lambda)} = 0$. Budući da je $\lambda \neq \overline{\lambda}$, iz teorema 1.4. slijedi da je u prstenu $\mathbb{C}[X]$ polinom $P$ djeljiv s polinomom $(X - \lambda)(X - \overline{\lambda})$. Međutim,

$$(X - \lambda)(X - \overline{\lambda}) = X^2 - 2(Re\lambda)X + |\lambda|^2 \in \mathbb{R}[X],$$

dakle $(X - \lambda)(X - \overline{\lambda})$ dijeli polinom $P$ i u prstenu $\mathbb{R}[X]$. Zbog ireducibilnosti polinoma $P$ u $\mathbb{R}[X]$ zaključujemo da je $P = (X - \lambda)(X - \overline{\lambda})$. Stavimo li $\alpha = -2\operatorname{Re}\lambda$ i $\beta = |\lambda|^2$, dobivamo $P = X^2 + \alpha X + \beta$, a kako je $\lambda \neq \overline{\lambda}$, to je $|\operatorname{Re}\lambda| < |\lambda|$, dakle $\alpha^2 = 4(\operatorname{Re}\lambda)^2 < 4|\lambda|^2 = 4\beta$. Time je dokazano da vrijedi

$$\mathbb{R}_i[X] \setminus \{X - \lambda;\ \lambda \in \mathbb{R}\} \subseteq \{X^2 + \alpha X + \beta;\ \alpha, \beta \in \mathbb{R},\ \alpha^2 < 4\beta\},$$

odnosno,

$$\mathbb{R}_i[X] \subseteq \{X-\lambda;\ \lambda\in\mathbb{R}\} \cup \{X^2+\alpha X+\beta;\ \alpha,\beta\in\mathbb{R},\ \alpha^2<4\beta\}.$$

Vrijedi i obrnuta inkluzija. Doista, već znamo da je $\{X-\lambda;\ \lambda\in\mathbb{R}\}\subseteq\mathbb{R}_i[X]$. Nadalje, ako su $\alpha,\beta\in\mathbb{R}$ takvi da je $\alpha^2<4\beta$, onda se polinom $X^2+\alpha X+\beta$ ne može napisati kao produkt dvaju nekonstantnih polinoma iz $K_1[X]$. Doista, pretpostavimo suprotno da je

$$X^2+\alpha X+\beta = PQ, \qquad P,Q\in K_1[X],\quad \deg P\geq 1,\ \deg Q\geq 1.$$

Tada je $\deg P+\deg Q=2$ pa slijedi da su normirani polinomi $P$ i $Q$ nužno stupnja 1. Drugim riječima, postoje $\lambda,\mu\in\mathbb{R}$ takvi da je $P=X-\lambda$ i $Q=X-\mu$. Slijedi

$$X^2+\alpha X+\beta=(X-\lambda)(X-\mu)=X^2-(\lambda+\mu)X+\lambda\mu.$$

No tada je

$$\alpha=-\lambda-\mu \quad \text{i} \quad \beta=\lambda\mu,$$

a odatle nalazimo

$$\alpha^2-4\beta=\lambda^2+2\lambda\mu+\mu^2-4\lambda\mu=\lambda^2-2\lambda\mu+\mu^2=(\lambda-\mu)^2\geq 0.$$

To je u suprotnosti s pretpostavkom $\alpha^2<4\beta$. Ova kontradikcija pokazuje da je pretpostavka o reducibilnosti polinoma $X^2+\alpha X+\beta$ bila pogrešna. Time je dokazana inkluzija

$$\{X^2+\alpha X+\beta;\ \alpha,\beta\in\mathbb{R},\ \alpha^2<4\beta\}\subseteq\mathbb{R}_i[X],$$

tj.

$$\{X-\lambda;\ \lambda\in\mathbb{R}\}\cup\{X^2+\alpha X+\beta;\ \alpha,\beta\in\mathbb{R},\ \alpha^2<4\beta\}\subseteq\mathbb{R}_i[X].$$

Iz dvije suprotne inkluzije slijedi jednakost u tvrdnji propozicije.

# Poglavlje 2

# Grupe

## 2.1 Normalne podgrupe. Kvocijentne grupe

Neka je $G$ grupa i $H$ podgrupa od $G$. Za $a, b \in G$ pišemo $a \sim^H b$ ako je $b^{-1}a \in H$. Na taj način definirana je relacija ekvivalencije na skupu $G$, odnosno, vrijedi:

($a$) *refleksivnost*: $a \sim^H a \ \ \forall a \in G$;

($b$) *simetričnost*: za $a, b \in G$ iz $a \sim^H b$ slijedi $b \sim^H a$;

($c$) *tranzitivnost*: za $a, b, c \in G$ iz $a \sim^H b$ i $b \sim^H c$ slijedi $a \sim^H c$.

Doista, za svaki $a \in G$ je $a^{-1}a = e \in H$, dakle vrijedi $a \sim^H a$. Nadalje, pretpostavimo da je $a \sim^H b$. Tada je $b^{-1}a \in H$, pa slijedi da je i $a^{-1}b = (b^{-1}a)^{-1} \in H$, dakle vrijedi $b \sim^H a$. Napokon, neka vrijedi $a \sim^H b$ i $b \sim^H c$, tj. $b^{-1}a, c^{-1}b \in H$. Tada nalazimo da je i $c^{-1}a = (c^{-1}b)(b^{-1}a) \in H$, dakle vrijedi $a \sim^H c$.

Kao što je uvijek kad je zadana relacija ekvivalencije, grupa $G$ je disjunktna unija svih svojih klasa ekvivalencije u odnosu na relaciju $\sim^H$ . Za $a \in G$ označit ćemo sa $[a]$ klasu ekvivalencije u odnosu na relaciju $\sim^H$ u kojoj se nalazi element $a$ :

$$[a] = \{b \in G;\ b \sim^H a\} = \{b \in G;\ a^{-1}b \in H\}.$$

**Lema 2.1.** *Neka je $G$ grupa, $H$ njena podgrupa i $a \in G$. Tada je*

$$[a] = aH = \{ah;\ h \in H\}.$$

**Dokaz:** Neka je $b \in [a]$. Tada je $h = a^{-1}b \in H$. Odatle množenjem slijeva sa $a$ dobivamo $b = ah$. Time je dokazana inkuzija $[a] \subseteq aH$. Za dokaz obrnute inkluzije uzmimo da je $b \in aH$. Po definiciji skupa $aH$ to znači da je $b = ah$ za neki $h \in H$. No tada je $a^{-1}b = h \in H$, dakle $b \sim^H a$, odnosno $b \in [a]$. Time je dokazana i obrnuta inkluzija $[a] \supseteq aH$, dakle jednakost.

Klase ekvivalencije $[a] = aH,\ a \in G$, zovu se **desne klase** u grupi $G$ u odnosu na podgrupu $H$, ili kraće **desne $H-$klase** u $G$.

Sasvim analogno relaciji $\sim^H$ definira se relacija ${}^H\!\sim$:

$$a \ {}^H\!\sim b \qquad \Longleftrightarrow \qquad ab^{-1} \in H.$$

Naravno, ${}^{H}\!\sim$ je također relacija ekvivalencije u grupi $G$, a klasa ekvivalencije koja sadrži element $a \in G$ jednaka je

$$Ha = \{ha;\ h \in H\} = \{b \in G;\ b\ {}^{H}\!\sim a\}.$$

$Ha$ se zove **lijeva klasa** u grupi $G$ u odnosu na podgrupu $H$, ili kraće **lijeva $H-$klasa** u $G$.

Između bilo kojih dviju $H-$klasa u grupi $G$ postoji bijekcija. Doista, za element $c$ grupe $G$ definiramo preslikavanja $\varphi_c, \psi_c, \chi_c : G \to G$ :

$$\varphi_c(a) = cac^{-1}, \qquad \psi_c(a) = ac, \qquad \chi_c(a) = ca, \qquad a \in G.$$

**Propozicija 2.1.** *Neka je $G$ grupa, $H$ podgrupa i $c \in G$. Tada vrijedi:*

(a) *$\varphi_c$ je izomorfizam grupe $G$ na samu sebe; restrikcija $\varphi_c|Hc$ je bijekcija lijeve $H-$klase $Hc$ na desnu $H-$klasu $cH$.*

(b) *$\psi_c$ je bijekcija sa $G$ na $G$; za $a, b \in G$ restrikcija $\psi_{a^{-1}b}|Ha$ je bijekcija sa $Ha$ na $Hb$.*

(c) *$\chi_c$ je bijekcija sa $G$ na $G$; za $a, b \in G$ restrikcija $\chi_{ba^{-1}}|aH$ je bijekcija sa $aH$ na $bH$.*

**Dokaz:** $(a)$ $\varphi_c$ je homomorfizam jer

$$\varphi_c(ab) = cabc^{-1} = cac^{-1}cbc^{-1} = \varphi_c(a)\varphi_c(b).$$

$\varphi_c$ je injekcija. Doista, pretpostavimo da su $a, b \in G$ takvi da je $\varphi_c(a) = \varphi_c(b)$. To znači da je $cac^{-1} = cbc^{-1}$, a množenjem te jednakosti slijeva sa $c^{-1}$ i zdesna sa $c$ slijedi $a = b$. $\varphi_c$ je i surjekcija sa $G$ na $G$. Doista, za bilo koji $a \in G$ imamo $\varphi_c(c^{-1}ac) = cc^{-1}acc^{-1} = a$. Prema tome, $\varphi_c$ je izomorfizam grupe $G$ na samu sebe.

Napokon, očito je $\varphi_c(Hc) = cHcc^{-1} = cH$.

$(b)$ $\psi_c$ je injekcija:

$$\psi_c(a) = \psi_c(b) \qquad \Longrightarrow \qquad ac = bc \ / \cdot c^{-1} \qquad \Longrightarrow \qquad a = b.$$

$\psi_c$ je i surjekcija, jer je $\psi_c(ac^{-1}) = ac^{-1}c = a$. Napokon,

$$\psi_{a^{-1}b}(Ha) = Haa^{-1}b = Hb.$$

Sasvim analogno dokazuje se i $(c)$.

Prema tome, sve $H-$klase u grupi $G$ (i lijeve i desne) međusobno su bijektivne. Posebno, u konačnoj grupi $G$ sve one imaju isti broj elemenata i to je upravo broj elemenata podgrupe $H = He = eH$.

Za konačnu grupu $G$ sa $|G|$ćemo označavati njezin broj elemenata. $|G|$ se obično zove **red grupe** $G$. Općenitije, sa $|S|$ ćemo označavati broj elemenata bilo kojeg konačnog skupa $S$.

**Teorem 2.1 (Lagrangeov teorem).** *Neka je $G$ konačna grupa i $H$ njena podgrupa. Tada je red $|G|$ grupe $G$ djeljiv s redom $|H|$ grupe $H$. Preciznije, ako je $|G| = n$, $|H| = k$ i ako je $p$ broj desnih $H-$klasa u $G$, onda je $n = pk$; $p$ je ujedno broj lijevih $H-$klasa u grupi $G$.*

**Dokaz:** Neka su $a_1, a_2, \ldots, a_p$ predstavnici svih desnih $H-$klasa u $G$. Tada imamo disjunktnu uniju

$$G = a_1H \cup a_2H \cup \ldots \cup a_pH.$$

Prema propoziciji 2.1. broj elemenata u svakoj od klasa $a_jH$ jednak je $|H| = k$. Iz gornjeg rastava u disjunktnu uniju slijedi $n = pk$.

Za podgrupu $H$ grupe $G$ kažemo da je **konačnog indeksa** u grupi $G$ ako ima samo konačno mnogo različitih desnih $H-$klasa u grupi $G$. Taj se broj označava sa $(G:H)$ i zove **indeks** podgrupe $H$ u grupi $G$. Očito je $(G:H)$ ujedno i broj različitih lijevih $H-$klasa u $G$. Prema Lagrangeovom teoremu za konačnu grupu $G$ i za bilo koju njenu podgrupu $H$ vrijedi:

$$(G:H) = \frac{|G|}{|H|}.$$

Podgrupa $H$ grupe $G$ zove se **normalna podgrupa** ako je $Hc = cH\ \forall c \in G$. Činjenicu da je $H$ normalna podgrupa od $G$ zapisujemo ovako: $H \trianglelefteq G$. Pomnožimo li jednakost $Hc = cH$ zdesna sa $c^{-1}$ dobivamo $H = cHc^{-1}$. Dakle, podgrupa $H$ je normalna u grupi $G$ ako i samo ako vrijedi

$$cHc^{-1} = H \qquad \forall c \in G,$$

odnosno, uz prije uvedenu oznaku $\varphi_c$ ako i samo ako je $\varphi_c(H) = H\ \ \forall c \in G$.

Neka je $H$ normalna podgrupa grupe $G$. Sa $G/H$ ćemo označavati skup svih $H-$klasa u $G$. U taj skup uvodimo binarnu operaciju sa:

$$(aH)(bH) = abH, \qquad aH, bH \in G/H, \quad \text{t.j.} \quad a, b \in G.$$

Činjenica da je podgrupa $H$ normalna osigurava smislenost ove definicije, tj. da rezultat $abH$ ne ovisi o izboru predstavnika $a$ i $b$ dviju $H-$klasa. Doista, neka su $a'$ i $b'$ druga dva predstavnika istih $H-$klasa, tj. $aH = a'H$ i $bH = b'H$. To znači da je $a \sim^H a'$ i $b \sim^H b'$, tj. vrijedi $h = a^{-1}a' \in H$ i $k = b^{-1}b' \in H$. Dakle, $a' = ah$ i $b' = bk$ pa imamo

$$a'b' = ahbk = abb^{-1}hbk.$$

Dakle, vrijedi $a'b' = abg$, uz oznaku $g = b^{-1}hbk$. Imamo $b^{-1}hb = \varphi_{b^{-1}}(h) \in \varphi_{b^{-1}}(H) = H$, jer je $H$ normalna podgrupa. Stoga je $g = b^{-1}hbk \in H$, dakle $a'b' = abg \in abH$, odnosno, $a'b' \sim^H ab$ ili $a'b'H = abH$.

S tako definiranom operacijom skup $H-$klasa $G/H$ postaje grupa. Doista, operacija je asocijativna:

$$((aH)(bH))(cH) = (abH)(cH) = abcH = (aH)(bcH) = (aH((bH)(cH)).$$

Klasa $H = eH$ je neutralna (jedinični element iz $G/H$) u odnosu na tu operaciju:

$$(eH)(aH) = (aH)(eH) = aH \qquad aH \in G/H.$$

Napokon, za $aH \in G/H$ imamo

$$(a^{-1}H)(aH) = (aH)(a^{-1}H) = eH,$$

dakle $a^{-1}H \in G/H$ je invers od $aH$. $G/H$ se zove **kvocijentna grupa** grupe $G$ po normalnoj podgrupi $H$.

Sada možemo poboljšati tvrdnje propozicije 1.7.:

**Teorem 2.2.** *Neka je $\varphi : G_1 \to G_2$ homomorfizam grupa.*

(a) *$H = Ker\ \varphi$ je normalna podgrupa od $G_1$.*

(b) *Preslikavanje $\Phi : G_1/H \to Im\ \varphi$ definirano sa $\Phi(aH) = \varphi(a)$, $a \in G_1$, je izomorfizam kvocijentne grupe $G_1/H$ na grupu $Im\ \varphi$.*

**Dokaz:** (a) Neka je $h \in H$. Tada je $h \in$ Ker $\varphi$, dakle $\varphi(h) = e_{G_2}$. Stoga za svaki $a \in G_1$ imamo

$$\varphi(aha^{-1}) = \varphi(a)\varphi(h)\varphi(a)^{-1} = \varphi(a)\varphi(a)^{-1} = e_{G_2},$$

dakle, $aha^{-1} \in$ Ker $\varphi = H$. Time smo dokazali inkluziju $aHa^{-1} \subseteq H,\ \forall a \in G_1$. Zamjenom $a$ sa $a^{-1}$ dobivamo i $a^{-1}Ha \subseteq H\ \forall a \in G_1$. Množenjem te inkluzije slijeva sa $a$ i zdesna sa $a^{-1}$ slijedi $aHa^{-1} \supseteq H\ \forall a \in G_1$. Iz dvije inkluzije zaključujemo da je $aHa^{-1} = H\ \forall a \in G_1$, dakle, $H$ je normalna podgrupa grupe $G_1$.

(b) Prije svega dokažimo da je definicija preslikavanja $\Phi$ smislena, tj. da ne ovisi o izboru predstavnika $H-$klase. Neka su $a, a' \in G_1$ takvi da vrijedi $aH = a'H$, odnosno $a \sim^H a'$, što znači da je $a'^{-1}a \in H =$ Ker $\varphi$. Dakle, imamo $\varphi(a'^{-1}a) = e_{G_2}$, a odatle $\varphi(a')^{-1}\varphi(a) = e_{G_2}$. Množenjem ove jednakosti slijeva sa $\varphi(a')$ dobivamo $\varphi(a) = \varphi(a')$, a to smo i željeli dokazati.

$\Phi$ je homomorfizam, jer

$$\Phi((aH)(bH)) = \Phi(abH) = \varphi(ab) = \varphi(a)\varphi(b) = \Phi(aH)\Phi(bH).$$

$\Phi$ je injekcija, jer

$$\Phi(aH) = \Phi(bH) \quad \Longrightarrow \quad \varphi(a) = \varphi(b) \quad \Longrightarrow \quad \varphi(b^{-1}a) = \varphi(b)^{-1}\varphi(a) = e_{G_2} \quad \Longrightarrow$$

$$\Longrightarrow \quad b^{-1}a \in \text{Ker } \varphi = H \quad \Longrightarrow \quad a \sim^H b \quad \Longrightarrow \quad aH = bH.$$

Napokon, treba još dokazati da je $\Phi$ surjekcija na Im $\varphi$. Neka je $c \in$ Im $\varphi$. Tada postoji $a \in G_1$ takav da je $c = \varphi(a)$. No tada po definiciji preslikavanja $\Phi$ vrijedi $c = \Phi(aH)$.

Neka je $G$ grupa. Podskup $Z(G) = \{x \in G;\ xa = ax\ \forall a \in G\}$ zove se **centar** grupe $G$. To je normalna komutativna podgrupa od $G$. Doista, očito je $e \in Z(G)$. Nadalje, ako je $x \in Z(G)$, množenjem jednakosti $ax = xa$ slijeva i zdesna sa $x^{-1}$ slijedi $x^{-1}a = ax^{-1}\ \forall a \in G$, dakle $x^{-1} \in Z(G)$. Napokon, ako su $x, y \in Z(G)$, za bilo koji $a \in G$ imamo $xya = xay = axy$, što pokazuje da je $xy \in Z(G)$. Time smo dokazali da je $Z(G)$ podgrupa od $G$. Ona je očito komutativna. Ta je podgrupa normalna, jer za $x \in Z(G)$ i $a \in G$ imamo $axa^{-1} = x$, što pokazuje da je $aZ(G)a^{-1} = Z(G)\ \forall a \in G$.

Primijetimo da ako je $K$ podgrupa od $G$, koja je sadržana u $Z(G)$, onda $\forall a \in G$ vrijedi $aKa^{-1} = K$. Dakle, svaka je takva podgrupa normalna. Takva se podgrupa zove **centralna**.

Imamo $Z(GL_n(\mathbb{R})) = \{\lambda I; \lambda \in \mathbb{R}^*\}$, gdje je $I$ oznaka za jediničnu matricu. Za parni $n \in \mathbb{N}$ je $Z(SL_n(\mathbb{R})) = \{I, -I\}$, a za neparni $n$ je $Z(SL_n(\mathbb{R})) = \{I\}$. Za simetričnu grupu $S_n$ imamo $Z(S_2) = S_2$ i $Z(S_n) = \{e\}$ za $n \geq 3$.

## 2.2 Cikličke grupe

Neka je $G$ grupa i $a \in G$. Stavimo $a^0 = e$, $a^1 = a$, a za $n \geq 2$ definiramo induktivno $a^n = a \cdot a^{n-1}$. Dakle, $a^n = a \cdot a \cdots a$ ($n$ faktora). Nadalje, za $n \in \mathbb{N}$ stavljamo $a^{-n} = (a^{-1})^n$. Na taj način za svaki $a \in G$ i za svaki $n \in \mathbb{Z}$ definirali smo $a^n$. Dakle, za svaki $a \in G$ imamo preslikavanje

$$\Phi_a : \mathbb{Z} \to G, \qquad \Phi_a(n) = a^n, \quad n \in \mathbb{Z}.$$

Lako se vidi da za bilo koje $n, m \in \mathbb{Z}$ vrijedi $a^{n+m} = a^n a^m$. Drugim riječima, $\Phi_a$ je homomorphizam aditivne grupe $\mathbb{Z}$ u grupu $G$. Njegovu sliku označimo sa

$$\langle a \rangle = \text{Im } \Phi_a = \{a^n;\ n \in \mathbb{Z}\}.$$

$\langle a \rangle$ je najmanja podgrupa od $G$ koja sadrži element $a$. Općenito, za bilo koji podskup $S$ grupe $G$ za najmanju podgrupu koja sadrži skup $S$ kažemo da je **generirana** sa $S$ i označavamo je sa $\langle S \rangle$. Grupa generirana jednim elementom zove se **ciklička**. Prema teoremu 2.2. ciklička podgrupa $\langle a \rangle$ generirana nekim elementom $a \in G$ izomorfna je kvocijentnoj grupi $\mathbb{Z}/\text{Ker } \Phi_a$ aditivne grupe cijelih brojeva po jezgri Ker $\Phi_a$ homomorfizma $\Phi_a : n \mapsto a^n$ :

$$\text{Ker } \Phi_a = \{n \in \mathbb{Z};\ a^n = e\}.$$

**Lema 2.2.** *Neka je $K$ podgrupa aditivne grupe $\mathbb{Z}$. Tada je ili $K = \{0\}$ ili postoji $m \in \mathbb{N}$ takav da je*

$$K = m\mathbb{Z} = \{km;\ k \in \mathbb{Z}\} = \{n \in \mathbb{Z};\ n \text{ je djeljiv sa } m\}.$$

**Dokaz:** Pretpostavimo da je $K \neq \{0\}$. Tada je $K \cap \mathbb{N} \neq \emptyset$. Neka je $m$ najmanji broj iz skupa $K \cap \mathbb{N}$. Tada je $km \in K$ za svaki prirodan broj $k$, jer je $km = m + m + \ldots + m$ ($k$ sumanada). I suprotan element $-km$ je sadržan u $K$. Time smo dokazali inkluziju $K \supseteq m\mathbb{Z}$. Dokažimo i obrnutu inkluziju. Neka je $n \in K$. Možemo pisati $n = km + p$, pri čemu je $k \in \mathbb{Z}$ i $p \in \{0, 1, \ldots, m-1\}$. Tada je $km \in K$, dakle i $p = n - km \in K$. Kako je $p < m$, zbog izbora broja $m$ slijedi da mora biti $p = 0$. Dakle, $n = km$ i time je dokazana obrnuta inkluzija $K \subseteq m\mathbb{Z}$. Stoga imamo jednakost $K = m\mathbb{Z}$.

Za prirodan broj $m$ kvocijentnu grupu $\mathbb{Z}/m\mathbb{Z}$ označavamo sa $\mathbb{Z}_m$. To je **ciklička grupa $m-$tog reda**. Kao skup ona se može identificirati sa skupom $\{0, 1, \ldots, m-1\}$, a operacija je *zbrajanje modulo $m$* : zbroj brojeva $j$ i $k$ modulo $m$ je jedinstven broj $n \in \{0, 1, \ldots m-1\}$ takav da je $j + k - n$ djeljiv sa $m$. U stvari, $n = j + k$, ako je $j + k < m$, a $n = j + k - m$, ako je $j + k \geq m$. Ova razmatranja pokazuju da vrijedi:

**Propozicija 2.2.** *Neka je $G$ grupa i $a \in G$. Za cikličku grupu $\langle a \rangle$ generiranu elementom $a$ ispunjena je jedna od sljedeće dvije mogućnosti:*

(a) *$\langle a \rangle$ je beskonačna grupa. To je ispunjeno točno onda kad je $\Phi_a$ monomorfizam, tj. kad je $a^n \neq a^m$ za $n \neq m$. Tada je $n \mapsto a^n$ izomorfizam aditivne grupe $\mathbb{Z}$ na grupu $\langle a \rangle$.*

(b) *$\langle a \rangle$ je konačna grupa. Tada je $\langle a \rangle = \{e, a, a^2, \ldots, a^{m-1}\}$ za neki prirodan broj $m$ i preslikavanje $n \mapsto a^n$ je izomorfizam grupe $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ na grupu $\langle a \rangle$.*

Neka je $G$ konačna grupa reda $|G| = n$ s jediničnim elementom $e$ i neka je $a \in G$. Prema propoziciji 2.2. tada je podgrupa $\langle a \rangle$ generirana elementom $a$ izomorfna cikličkoj grupi $\mathbb{Z}_m$ za neki prirodan broj $m$. Red $m = |\langle a \rangle|$ grupe $\langle a \rangle$ zove se **period** elementa $a$ i to je najmanji prirodan broj $k$ za kojeg je $a^k = e$. Tada je $a^m = e$ i za međusobno različite $i, j \in \{0, 1, \ldots, m-1\}$

je $a^i \neq a^j$. Prema Lagrangeovom teoremu (teorem 2.1.) period svakog elementa $a \in G$ je djelitelj reda $n$ grupe $G$. Jedinica $e$ je jedini element grupe $G$ reda 1. Ako je red $n$ grupe $G$ prost broj onda je period svakog elementa $a \neq e$ grupe $G$ jednak $n$. To znači da $\langle a \rangle$ podgrupa reda $n$ dakle jednaka je čitavoj grupi $G$. Tim razmatranjem dokazali smo:

**Propozicija 2.3.** *Neka je $G$ konačna grupa reda $n$. Period svakog elementa $a \in G$ je djelitelj od $n$. Ako je $n$ prost broj i $a \neq e$ onda je $\langle a \rangle = G$, tj. element $a$ je generator grupe $G$.*

Neka je $G$ konačna grupa reda $n$ i neka je $m$ period elementa $a \in G$, dakle $a^m = e$. Prema prethodnoj propoziciji je $n = mq$ za neki prirodan broj $q$. Imamo $a^n = a^{mq} = (a^m)^q = e^q = e$. Dakle, vrijedi $a^n = e \ \forall a \in G$. Najmanji prirodan broj $k$ takav da je $a^k = e \ \forall a \in G$ zove se **eksponent grupe** $G$.

**Propozicija 2.4.** *Neka je $G$ konačna grupa reda $n$ i eksponenta $k$. Broj $n$ djeljiv je s brojem $k$.*

**Dokaz:** Neka su $a_1, a_2, \ldots, a_n$ svi elementi grupe $G$ i neka su redom $m_1, m_2, \ldots, m_n$ periodi tih elemenata. Za $q \in \mathbb{N}$ i $j \in \{1, 2, \ldots, n\}$ vrijedi $a_j^q = e$ ako i samo ako je $q$ višekratnik broja $m_j$. To znači da je eksponent $k$ grupe $G$ višekratnik svakog od brojeva $m_1, m_2, \ldots, m_n$. Prema tome, $k$ je najmanji zajednički višekratnik brojeva $m_1, m_2, \ldots, m_n$. Prema propoziciji 2.3. red $n$ grupe $G$ je višekratnik svakog od brojeva $m_1, m_2, \ldots, m_n$. No, svaki zajednički višekratnik djeljiv je s najmanjim zajedničkim višekratnikom. Dakle, $n$ je djeljiv s $k$.

Razmotrimo sada posebno Abelove konačne grupe. Sjetimo se da je svaka podgrupa Abelove grupe normalna, dakle po svakoj se podgrupi može formirati kvocijentna grupa.

**Propozicija 2.5.** *Neka je $G$ Abelova grupa reda $n$ i eksponenta $k$. Tada je neka potencija broja $k$ djeljiva sa $n$. Drugim riječima, ako je $n$ djeljiv s prostim brojem $p$ onda je i $k$ djeljiv s $p$.*

**Dokaz** ćemo provesti indukcijom u odnosu na red grupe $G$. Baza indukcije $|G| = 1$, tj. $G = \{e\}$, je trivijalna. Provedimo korak indukcije. Neka je $|G| = n \geq 2$ i pretpostavimo da je tvrdnja dokazana za Abelove grupe reda manjeg od $n$. Neka je $a \in G, \ a \neq e$. Označimo sa $q$ period elementa $a$. Tada je $k$ djeljiv sa $q$, tj. $k = qj$ za neki $j \in \mathbb{N}$. Neka je $H = \langle a \rangle$. Tada je $|H| = q$. Označimo sa $r$ eksponent kvocijentne grupe $G/H$. Očito za svaki element $a \in G$ vrijedi $(aH)^k = a^k H = eH$, a to je jedinica u kvocijentnoj grupi $G/H$. Prema tome, $k$ je djeljiv sa $r$ tj. $k = rs$, za neki $s \in \mathbb{N}$. Neka je $m$ red kvocijentne grupe $G/H$. Naravno, po Lagrangeovom teoremu je $n = mq$. Kako je $m < n$, po pretpostavci indukcije neka potencija od $r$ djeljiva je sa $m$. Dakle, postoje $i, p \in \mathbb{N}$ takvi da je $r^i = mp$. Prema tome, imamo sljedeće jednakosti:

$$n = mq, \qquad k = qj, \qquad k = rs, \qquad r^i = mp.$$

Odatle slijedi:

$$k^{i+1} = k \cdot k^i = kr^i s^i = qjmps^i = njps^i.$$

Dakle, potencija $k^{i+1}$ je djeljiva sa $n$.

Posebnu ulogu među Abelovim grupama igraju cikličke grupe, tj. grupe generirane jednim elementom.

**Propozicija 2.6.** *Neka je $G$ ciklička grupa.*

(a) *Svaka podgrupa od $G$ je ciklička.*

(b) *Za svaku podgrupu $H$ od $G$ kvocijentna grupa $G/H$ je ciklička.*

**Dokaz:** Ako je grupa $G$ beskonačna onda je $G$ izomorfna aditivnoj grupi $\mathbb{Z}$. Prema lemi 2.2. svaka netrivijalna podgrupa od $\mathbb{Z}$ je oblika

$$m\mathbb{Z} = \{km;\ k \in \mathbb{Z}\} = \{0, m, -m, 2m, -2m, \ldots\}$$

za neki prirodan broj $m$. Ta je podgrupa ciklička: generator joj je $m$. Nadalje, i kvocijentna grupa $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ je ciklička. Dakle, propozicija je dokazana ako je grupa $G$ beskonačna.

Pretpostavimo sada da je grupa $G$ konačna reda $n$ i neka je $a$ generator grupe $G$ :

$$G = \langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}.$$

Neka je $H \neq \{e\}$ podgrupa od $G$. Stavimo

$$m = \min\{k \in \mathbb{N};\ a^k \in H\}.$$

Tvrdimo da je tada $a^m$ generator grupe $H$. Doista, neka je $b \in H$ proizvoljan. Tada je $b = a^k$ za neki $k \in \{0, 1, \ldots, n-1\}$. Možemo pisati $k = ms + j$ za jedinstvene cijele brojeve $s$ i $j$ takve da je $s \geq 0$ i $0 \leq j < m$. Tada je $b = a^{ms+j} = (a^m)^s a^j$. Imamo $a^m \in H$, pa slijedi $a^j = b\,(a^m)^{-s} \in H$. Kako je $0 \leq j < m$ iz definicije broja $m$ slijedi $j = 0$. Dakle, $k = ms$ pa slijedi $b = (a^m)^s \in \langle a^m \rangle$. Time je dokazana inkuzija $H \subseteq \langle a^m \rangle$. Kako je $a^m \in H$, obrnuta inkluzija $\langle a^m \rangle \subseteq H$ je očigledna. Dakle, vrijedi jednakost $H = \langle a^m \rangle$ i time je dokazano da je grupa $H$ ciklička.

Napokon, ako $a \in G$ generira grupu $G$, onda njegova $H-$klasa $aH$ generira kvocijentnu grupu $G/H$, dakle i kvocijentna grupa $G/H$ je ciklička.

## 2.3 Grupe transformacija

I u matematici i u primjenama grupe koje se prirodno pojavljuju najčešće *djeluju na nekom skupu*. Neka je $G$ grupa i $S$ neprazan skup. Kažemo da **grupa** $G$ **djeluje na skupu** $S$ ako je zadan homomorfizam grupe $G$ u grupu permutacija skupa $S$. To znači da je za svaki $a \in G$ zadana bijekcija $\varphi_a : S \to S$ i da vrijedi $\varphi_a \circ \varphi_b = \varphi_{ab}$. Vrlo često se zadano djelovanje grupe $G$ na skupu $S$ zapisuje bez posebnih oznaka za permutacije $\varphi_a$ skupa $S$. Naime, definiramo li $ax = \varphi_a(x)$, $a \in G,\ x \in S$, vidimo da se djelovanje grupe $G$ na skupu $S$ može opisati zadavanjem preslikavanja $G \times S \to S,\ (a, x) \mapsto ax$, sa sljedećim svojstvima:

(a) $x \mapsto ax$ je bijekcija sa $S$ na $S\ \ \forall a \in G$;

(b) $a(bx) = (ab)x\ \ \forall a, b \in G$ i $\forall x \in S$.

Djelovanje grupe $G$ na skupu $S$ zadaje na prirodan način relaciju ekvivalencije na $S$ : za $x, y \in S$ stavljamo $x \sim y$ ako i samo ako postoji $a \in G$ takav da je $y = ax$. To je doista relacija ekvivalencije na $S$ :

za svaki $s \in S$ je $s = es$, dakle $s \sim s$;

ako su $x, y \in S$ takvi da je $x \sim y$, tj. ako vrijedi $y = ax$ za neki $a \in G$, onda je $x = a^{-1}y$, dakle, vrijedi i $y \sim x$;

napokon, ako za $x, y, z \in S$ vrijedi $x \sim y$ i $y \sim z$, tj. ako za neke $a, b \in G$ vrijedi $y = ax$ i $z = by$, onda je $(ab)x = a(bx) = ay = z$, dakle vrijedi i $x \sim z$.

Klase ekvivalencije u skupu $S$ zovu se $G-$**orbite**. $G-$orbita elementa $x \in S$ je skup

$$\mathcal{O}(x) = \{y \in S;\ x \sim y\} = Gx = \{ax;\ a \in G\}.$$

Za točku $x \in S$ definiramo

$$G_x = \{a \in G;\ ax = x\}.$$

$G_x$ je podgrupa od $G$ koja se zove **stabilizator** točke $x$ u grupi $G$.

**Propozicija 2.7.** *Neka je zadano djelovanje grupe $G$ na skupu $S$ i neka je $x \in S$. Tada je $aG_x \mapsto ax$ bijekcija sa skupa $G/G_x$ svih desnih $G_x-$klasa u grupi $G$ na $G-$orbitu $\mathcal{O}(x)$ elementa $x$ u skupu $S$. Posebno, ako je grupa $G$ konačna onda je broj elemenata $G-$orbite $\mathcal{O}(x)$ jednak indeksu $(G:G_x)$ stabilizatora $G_x$ točke $x$ u grupi $G$.*

**Dokaz:** Prije svega, uočimo da je defnicija preslikavanja $aG_x \mapsto ax$ sa skupa $G/G_x$ svih desnih $G_x-$klasa u skup $S$ smislena, tj. da ne ovisi o izboru predstavnika $G_x-$klase. Doista, neka su $a, b \in G$ takvi da je $aG_x = bG_x$. Tada je $b^{-1}a \in G_x$, dakle vrijedi $b^{-1}ax = x$, a odatle je $ax = bx$, što dokazuje smislenost definicije preslikavanja iz tvrdnje propozicije. Po samoj definiciji $G-$orbite očito je $aG_x \mapsto ax$ surjekcija sa $G/G_x$ na $\mathcal{O}(x)$. Treba još dokazati da je to i injekcija. Neka su $aG_x, bG_x \in G/G_x$ takvi da je $ax = bx$. Tada je $b^{-1}ax = x$, dakle $b^{-1}a \in G_x$, a to pokazuje da je $a \sim^{G_x} b$, odnosno $aG_x = bG_x$. Time je dokazana i injektivnost preslikavanja $aG_x \mapsto ax$.

Promatrat ćemo sada djelovanje grupe $G$ na samoj sebi koje se zove **konjugiranje**. Za svaki $a \in G$ bijekcija $\varphi_a : G \to G$ zadana je sa

$$\varphi_a(x) = axa^{-1}, \qquad x \in G.$$

To je doista djelovanje grupe $G$ na skupu $G$, jer je

$$\varphi_a\left(\varphi_b(x)\right) = \varphi_a\left(bxb^{-1}\right) = a\left(bxb^{-1}\right)a^{-1} = (ab)x(ab)^{-1} = \varphi_{ab}(x).$$

Elementi $x, y \in G$ koji su ekvivalentni u odnosu na to djelovanje zovu se $G-$**konjugirani** ili **konjugirani u grupi** $G$ :

$$\text{postoji} \quad a \in G \quad \text{takav da je} \quad y = axa^{-1}.$$

$G-$orbita elementa $x \in G$ zove se **klasa konjugiranosti** tog elementa:

$$\mathcal{O}(x) = \{axa^{-1};\ a \in G\}.$$

Stabilizator elementa $x \in G$ označava se sa $C_G(x)$ i zove **centralizator** elementa $x$ u grupi $G$ :

$$C_G(x) = \{a \in G;\ axa^{-1} = x\} = \{a \in G;\ ax = xa\}.$$

Dakle, centralizator $C_G(x)$ elementa $x$ je podgrupa koja se sastoji od svih elemenata grupe $G$ koji komutiraju sa $x$.

Presjek svih centralizatora $C_G(x)$, $x \in G$, je upravo **centar grupe** $G$ :

$$Z(G) = \bigcap_{x \in G} C_G(x) = \{a \in G;\ ax = xa\ \ \forall x \in G\}.$$

Već smo spomenuli da je $Z(G)$ je komutativna normalna podgrupa od $G$. Štoviše, svaka podgrupa od $Z(G)$ je normalna podgrupa od $G$.

Razmotrimo još jedno djelovanje grupe $G$ To je opet konjugiranje, ali ovaj puta na skupu $\mathcal{G}$ svih podgrupa od $G$. Za $a \in G$ i $H \in \mathcal{G}$ stavimo

$$\Phi_a(H) = aHa^{-1} = \{aha^{-1};\ h \in H\}.$$

Tada je $\Phi_a(H) \in \mathcal{G}$ i na taj način definirano je djelovanje grupe $G$ na skupu $\mathcal{G}$, tj. $\Phi_a \circ \Phi_b = \Phi_{ab}$ i $\Phi_e = id_{\mathcal{G}}$. Za **podgrupe** $H, K \in \mathcal{G}$ grupe $G$ kažemo da su **konjugirane** u grupi $G$ ako postoji $a \in G$ takav da je $K = \Phi_a(H) = aHa^{-1}$. Stabilizator podgrupe $H \in \mathcal{G}$ u odnosu na to djelovanje je podgrupa

$$N_G(H) = \{a \in G;\ aHa^{-1} = H\}$$

grupe $G$ koja se zove **normalizator** podgupe $H$ u grupi $G$. To je najveća među svim podgrupama grupe $G$ koje sadrže $H$ i u kojima je $H$ normalna podgrupa. Drugim riječima, vrijedi $H \trianglelefteq N_G(H)$ i ako je $K \in \mathcal{G}$ takva da je $H \trianglelefteq K$, onda je $K \subseteq N_G(H)$. $G-$orbite u skupu $\mathcal{G}$ zovu se **klase konjugiranosti podgrupa** grupe $G$. Naravno, vrijedi $N_G(H) = G$ ako i samo ako je $H \trianglelefteq G$.

## 2.4 Rješive i proste grupe

Neka je $G$ grupa. Definiramo tada

$$C(G) = \langle aba^{-1}b^{-1};\ a, b \in G\rangle.$$

Ako su $a, b \in G$, onda se element $aba^{-1}b^{-1}$ zove **komutator** elemenata $a$ i $b$. Primijetimo da je $aba^{-1}b^{-1} = e$ ako i samo ako je $ab = ba$, tj. ako i samo ako $a$ i $b$ komutiraju. Dakle, $C(G)$ je podgrupa od $G$ generirana svim komutatorima elemenata. $C(G)$ se zove **komutatorska podgrupa** grupe $G$. Očito je $C(G) = \{e\}$ ako i samo ako je grupa $G$ komutativna.

**Propozicija 2.8.** *Neka je $G$ grupa. Tada je $C(G) \trianglelefteq G$ i kvocijentna grupa $G/C(G)$ je komutativna. Nadalje, ako je $H \trianglelefteq G$ takva da je kvocijentna grupa $G/H$ komutativna, onda je $C(G) \subseteq H$.*

**Dokaz:** Označimo sa $S$ skup svih komutatora u grupi $G$ :

$$S = \{aba^{-1}b^{-1};\ a, b \in G\}.$$

Za bilo koje $a, b, c \in G$ imamo

$$c(aba^{-1}b^{-1})c^{-1} = (cac^{-1})(cbc^{-1})\left(cac^{-1}\right)^{-1}\left(cbc^{-1}\right)^{-1}.$$

Odatle se vidi da je $cSc^{-1} \subseteq S$, a iz $c^{-1}Sc \subseteq S$ slijedi i $S \subseteq cSc^{-1}$. Dakle, vrijedi jednakost $cSc^{-1} = S$ za svaki $c \in G$. Kako $S$ generira podgrupu $C(G)$ i $cSc^{-1}$ generira podgrupu $cC(G)c^{-1}$, slijedi da je $cC(G)c^{-1} = C(G)$ za svaki $c \in G$. Dakle, $C(G) \trianglelefteq G$.

Označimo sada sa $\pi$ epimorfizam grupe $G$ na kvocijentnu grupu $G/C(G)$ koji svakom elemenu pridružuje njegovu klasu:

$$\pi(a) = aC(G), \qquad a \in G.$$

Tada je $Ker\,\pi = C(G)$, pa za bilo koje $a, b \in G$ nalazimo

$$\pi(a)\pi(b)\pi(a)^{-1}\pi(b)^{-1} = \pi\left(aba^{-1}b^{-1}\right) = e_{G/C(G)} \qquad \text{(jedinica u kvocijentnoj grupi } G/C(G))$$

jer je $aba^{-1}b^{-1} \in S \subseteq C(G)$. Slijedi $\pi(a)\pi(b) = \pi(b)\pi(a)\ \forall a, b \in G$, dakle, kvocijentna grupa $G/C(G)$ je komutativna.

Napokon, pretpostavimo da je $H \trianglelefteq G$ takva da je $G/H$ komutativna. Za bilo koje $a, b \in H$ je tada $abH = (aH)(bH) = (bH)(aH) = baH$. Budući da se lijeve i desne $H-$klase u grupi $G$ podudaraju, ta se jednakost može pisati i ovako: $Hab = Hba$. Odatle je $Haba^{-1}b^{-1} = H$, pa slijedi $aba^{-1}b^{-1} \in H$. Dakle, $S \subseteq H$, a kako je $C(G)$ najmanja podgrupa od $G$ koja sadrži skup $S$, zaključujemo da je $C(G) \subseteq H$.

Naravno, za svaku podgrupu $H \leq G$ možemo definirati $C(H)$: to je podgrupa generirana skupom $\{hkh^{-1}k^{-1};\ h, k \in H\}$ svih komutatora elemenata iz $H$. Posebno, induktivno definiramo podgrupe $C^k(G)$, $k \in \mathbb{N}$ :

$$C^1(G) = C(G), \qquad C^k(G) = C(C^{k-1}(G)) \quad k \geq 2.$$

Kažemo da je $G$ **rješiva grupa**, ako postoji prirodan broj $n$ takav da je $C^n(G) = \{e\}$. Naravno, ako je grupa $G$ komutativna onda je $C^1(G) = C(G) = \{e\}$. Dakle, svaka komutativna grupa je rješiva.

**Teorem 2.3.** *Grupa $G$ je rješiva ako i samo ako postoji konačan rastući niz podgrupa*

$$\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_{n-1} \subseteq G_n = G$$

*takvih da vrijedi*

(a) $G_i \trianglelefteq G_{i+1}$ *za* $i = 0, 1, 2, \ldots, n-1$.

(b) *Kvocijentna grupa* $G_{i+1}/G_i$ *je komutativna za* $i = 0, 1, 2, \ldots, n-1$.

**Dokaz:** Pretpostavimo da je grupa $G$ rješiva i neka je $n \in \mathbb{N}$ takav da je $C^n(G) = \{e\}$. Stavimo tada $G_i = C^{n-i}(G)$ za $i = 0, 1, 2, \ldots, n-1$ i $G_n = G$. Kako je

$$G_i = C^{n-i}(G) = C(C^{n-i-1}(G)) = C(G_{i+1}),$$

imamo rastući niz podgrupa

$$\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_{n-1} \subseteq G_n = G$$

Prema propoziciji 2.8 tada za $i \in \{0, 1, \ldots, n-1\}$ vrijedi $G_i = C(G_{i+1}) \trianglelefteq G_{i+1}$. Nadalje, grupa $G_{i+1}/G_i = G_{i+1}/C(G_{i+1})$ je komutativna. Dakle, uvjet iz teorema je nužan da bi grupa $G$ bila rješiva.

Dokažimo sada dovoljnost tog uvjeta i pretpostavimo da imamo rastući konačan niz podgrupa kao u iskazu teorema. Kako je tada grupa $G_{i+1}/G_i$ komutativna, prema posljednjoj tvrdnji u propoziciji 2.8 slijedi da je $C(G_{i+1}) \subseteq G_i$. Indukcijom po $k$ dokazat ćemo sada da za svaki $k$ vrijedi $C^k(G) \subseteq G_{n-k}$. Doista, baza indukcije je trivijalna, jer je $C^1(G) = C(G) = C(G_n) \subseteq G_{n-1}$. Za dokaz koraka indukcije, pretpostavimo da je $k \geq 2$ i da je dokazano da je $C^{k-1}(G) \subseteq G_{n-k+1}$. Slijedi

$$C^k(G) = C(C^{k-1}(G)) \subseteq C(G_{n-k+1}) \subseteq G_{n-k}$$

i time je dokaz koraka indukcije proveden. Posebno, za $k = n$ dobivamo $C^n(G) \subseteq G_0 = \{e\}$, dakle, grupa $G$ je rješiva.

**Teorem 2.4.** *Neka je $G$ grupa, $H$ podgrupa od $G$ i $N$ normalna podgrupa od $G$.*

(a) *Ako je grupa $G$ rješiva, tada je i grupa $H$ rješiva.*

(b) *Ako je grupa $G$ rješiva, tada je i grupa $G/N$ rješiva.*

(c) *Ako su grupe $G/N$ i $N$ rješive, tada je i grupa $G$ rješiva.*

**Dokaz:** Tvrdnja $(a)$ slijedi iz evidentne činjenice da je $C^k(H) \subseteq C^k(G)$ za svaki $k$.

$(b)$ Označimo sa $\pi : G \to G/N$ epimorfizam koji svakom elementu grupe $G$ pridružuje njegovu $N-$klasu:

$$\pi(a) = aN, \qquad a \in G.$$

Tada je $\pi\left(aba^{-1}b^{-1}\right) = \pi(a)\pi(b)\pi(a)^{-1}\pi(b)^{-1}$, pa slijedi da je

$$\left\{\pi\left(aba^{-1}b^{-1}\right);\ a, b \in G\right\}$$

skup svih komutatora u kvocijentnoj grupi $G/N$. Odatle slijedi $C(G/N) = \pi(C(G))$, a odatle indukcijom po $k$ nalazimo da je $C^k(G/N) = \pi(C^k(G))$. Ako je $n \in \mathbb{N}$ takav da je $C^n(G) = \{e\}$, tada slijedi $C^n(G/N) = \pi(\{e\}) = \{e_{G/N}\}$. Dakle, grupa $G/N$ je rješiva.

$(c)$ Pretpostavimo da su $n, m \in \mathbb{N}$ takvi da je $C^n(G/N) = \{e_{G/N}\}$ i $C^m(N) = \{e\}$. Označimo ponovo sa $\pi$ epimorfizam $G \to G/N$. U dokazu tvrdnje $(b)$ vidjeli smo da je $C^k(G/N) = \pi(C^k(G))$

za svaki $k$. Posebno je $\pi(C^n(G)) = C^n(G/N) = \{e_{G/N}\}$, dakle je $C^n(G) \subseteq Ker\pi = N$. Sada slijedi $C^{n+m}(G) \subseteq C^m(N) = \{e\}$, dakle, grupa $G$ je rješiva.

**Grupa** $G$ zove se **prosta** ako su jedine njene normalne podgrupe $\{e\}$ i $G$. To se drugim riječima kaže da grupa $G$ nema netrivijalnih normalnih podgrupa.

**Teorem 2.5.** *Rješiva grupa je prosta ako i samo ako je ciklička i red $|G|$ joj je prost broj.*

**Dokaz:** Neka je grupa $G$ rješiva i prosta. Tada je za neki $n \in \mathbb{N}$ $C^n(G) = \{e\}$, pa slijedi da je $C(G) \neq G$; doista, iz $C(G) = G$ slijedi da je $C^k(G) = G$ za svaki $k$. No prema propoziciji 2.8 je $C(G) \trianglelefteq G$. Kako je grupa $G$ prosta, slijedi $C(G) = \{e\}$, a to znači da je grupa $G$ komutativna. U komutativnoj grupi svaka je podgrupa normalna. Dakle, ako je $a \neq e$, onda mora biti $\langle a \rangle = G$. Dakle, grupa $G$ je ciklička. Kad bi $G$ bila beskonačna, ona bi bila izomorfna aditivnoj grupi $\mathbb{Z}$, a ta grupa ima mnoštvo podgrupa. Dakle, $|G| = n \in \mathbb{N}$ i za $a \in G$, $a \neq e$, imamo $G = \{e, a, a^2, \ldots, a^{n-1}\}$. Kad bi bilo $n = mk$ za neke $m, k \in \mathbb{N}$, $m \geq 2$, $k \geq 2$, onda bi $H = \langle a^k \rangle$ bila netrivijalna podgrupa od $G$, što je nemoguće, jer je grupa $G$ prosta. Dakle, $n$ je prost broj.

Obratno, ako je $p$ prost broj i $|G| = p$, onda je grupa $G$ ciklička, dakle, komutativna, dakle, rješiva, a također zbog Lagrangeovog teorema 2.1 grupa $G$ nema nikakvih a ne samo normalnih netrivijalnih podgrupa, dakle je prosta.

Kao obično sa $S_n$ ćemo označiti grupu permutacija skupa $\{1, 2, \ldots, n\}$, a sa $A_n$ podgrupu svih parnih permutacija. Grupa $A_n$ zove se **alternirajuća grupa**. Ako je $\sigma \in A_n$ onda je $\tau \circ \sigma \circ \tau^{-1}$ parna permutacija za svaku permutaciju $\tau \in S_n$. Prema tome, $A_n$ je normalna podgrupa od $S_n$, $A_n \trianglelefteq S_n$.

**Propozicija 2.9.** *Grupa $A_n$ generirana je svim $3-$ciklusima, odnosno svim permutacijama $\tau = (i\, j\, k)$, pri čemu su $i, j, k$ međusobno različiti brojevi iz $\{1, 2, \ldots, n\}$, i $\tau$ preslikava na sljedeći način:*

$$\tau(i) = j, \qquad \tau(j) = k, \qquad \tau(k) = i, \qquad \tau(m) = m \quad \forall m \in \{1, 2, \ldots, n\} \setminus \{i, j, k\}.$$

**Dokaz:** Označimo sa $H$ podgrupu od $S_n$ generiranu svim $3-$ciklusima. Kako je svaki $3-$ciklus parna permutacija, vrijedi $H \subseteq A_n$.

Prema propoziciji 1.9. i prema tvrdnji $(b)$ propozicije 1.11. svaka parna permutacija produkt je parnog broja transpozicija. Pokazat ćemo sada da je produkt dviju transpozicija ili jedinični element $e$ ili $3-$ciklus ili produkt dvaju $3-$ciklusa. Promatrajmo najprije produkt disjunktnih transpozicija $(i\, j)(k\, \ell)$, $\{i, j\} \cap \{k, \ell\} = \emptyset$. Vrijedi

$$[(i\, j)(k\, \ell)](i) = (i\, j)(i) = j, \qquad [(i\, j)(k\, \ell)](j) = (i\, j)(j) = i,$$

$$[(i\, j)(k\, \ell)](k) = (i\, j)(\ell) = \ell, \qquad [(i\, j)(k\, \ell)](\ell) = (i\, j)(k) = k.$$

S druge strane je

$$[(i\, j\, k)(j\, k\, \ell)](i) = (i\, j\, k)(i) = j, \qquad [(i\, j\, k)(j\, k\, \ell)](j) = (i\, j\, k)(k) = i,$$

$$[(i\, j\, k)(j\, k\, \ell)](k) = (i\, j\, k)(\ell) = \ell, \qquad [(i\, j\, k)(j\, k\, \ell)](\ell) = (i\, j\, k)(j) = k.$$

Dakle,

$$(i\, j)(k\, \ell) = (i\, j\, k)(j\, k\, \ell).$$

Nadalje, produkt dviju jednakih transpozicija je jedinični element $e$ grupe $S_n$ :

$$(i\, j)(i\, j) = e.$$

Napokon, promotrimo produkt dvije transpozicije koje nisu niti jednake niti disjunktne. To je produkt $(i\,j)(j\,k)$ za neke međusobno različite brojeve $i, j, k \in \{1, 2, \ldots, n\}$. Tada imamo

$$(j\,k)(i) = i, \qquad (j\,k)(j) = k, \qquad (j\,k)(k) = j,$$

dakle,

$$[(i\,j)(j\,k)](i) = (i\,j)(i) = j, \qquad [(i\,j)(j\,k)](j) = (i\,j)(k) = k, \qquad [(i\,j)(j\,k)](k) = (i\,j)(j) = i,$$

što pokazuje da je

$$(i\,j)(j\,k) = (i\,j\,k).$$

Zaključujemo da je produkt parnog broja transpozicija ili jedinica $e$ ili $3-$ciklus ili produkt $3-$ciklusa. Odatle slijedi i obrnuta inkluzija $A_n \subseteq H$.

Očito je $A_2 = \{e\}$, a $A_3 = \{e, (123), (132)\}$ je komutativna grupa izomorfna sa $\mathbb{Z}_3$. Pokazuje se da je $A_4 = \{e, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$ i da je $H = \{e, (12)(34), (13)(24), (14)(23)\}$ komutativna normalna podgrupa od $A_4$. Red kvocijentne grupe $A_4/H$ jednak je $12/4 = 3$, dakle, ta je kvocijentna grupa izomorfna sa $Z_3$. Posebno, kvocijentna grupa $A_4/H$ je komutativna. Dakle, ako stavimo $G_0 = \{e\}$, $G_1 = H$ i $G_2 = A_4$, vidimo da vrijedi:

$$G_0 \trianglelefteq G_1 \trianglelefteq G_2, \quad G_0 = \{e\}, \quad G_2 = A_4, \quad \text{i grupe} \quad G_1/G_0 \simeq G_1 \quad \text{i} \quad G_2/G_1 \quad \text{su komutativne.}$$

To pokazuje da je grupa $A_4$ rješiva.

**Teorem 2.6.** *Ako je $n \geq 5$, alternirajuća grupa $A_n$ je prosta.*

**Dokaz:** Pretpostavimo da je $N \neq \{e\}$ normalna podgrupa od $A_n$. Treba dokazati da je tada $N = A_n$.

(1) Prvo ćemo dokazati da grupa $N$ sadrži neki $3-$ciklus. Proučit ćemo nekoliko mogućnosti.

($a$) Pretpostavimo da $N$ sadrži neki element oblika $x = abc\cdots$, gdje su $a, b, c, \ldots$ međusobno disjunktni ciklusi i gdje je $a$ $m-$ciklus za neki $m \geq 4$ :

$$a = (a_1 a_2 \ldots a_m), \qquad m \geq 4.$$

Stavimo $t = (a_1 a_2 a_3) \in A_n$. Tada je $z = t^{-1}xt \in N$. Budući da je $m-$ciklus $a$ disjunktan s ostalim ciklusima $b, c, \ldots$ u prikazu elementa $x$, to $3-$ciklus $t$ komutira s tim ostalim ciklusima. Stoga, ako sa $y$ označimo umnožak tih ostalih ciklusa, imamo

$$z = t^{-1}xt = \left(t^{-1}at\right) bc\cdots = \left(t^{-1}at\right) y.$$

Kako je $x = ay$, to je $x^{-1} = y^{-1}a^{-1}$, pa slijedi

$$zx^{-1} = t^{-1}atyy^{-1}a^{-1} = t^{-1}ata^{-1}.$$

Međutim, $t^{-1} = (a_3 a_2 a_1)$, $a^{-1} = (a_m a_{m-1} \ldots a_2 a_1)$, pa direktno izračunavanje djelovanja elementa $zx^{-1} = t^{-1}ata^{-1}$ na skup $\{1, 2, \ldots, n\}$ pokazuje da taj element djeluje ovako:

$$zx^{-1}(a_1) = a_3, \quad zx^{-1}(a_3) = a_4, \quad zx^{-1}(a_4) = a_1,$$

$$zx^{-1}(a_j) = a_j \quad \text{za} \quad j = 2 \quad \text{i za} \quad 5 \leq j \leq m.$$

Budući da očito ta permutacija ostavlja fiksnima sve $p \in \{1, 2, \ldots, n\} \setminus \{a_1, a_2, \ldots, a_m\}$, vidimo da je

$$zx^{-1} = (a_1 a_3 a_m)$$

3−ciklus. No kako su $z, x \in N$ to je i $zx^{-1} \in N$. Dakle, u ovom slučaju podgrupa $N \trianglelefteq A_n$ sadrži bar jedan 3−ciklus.

($b$) Pretpostavimo sada da $N$ sadrži element koji u rastavu u produkt međusobno disjunktnih ciklusa ima barem dva 3−ciklusa. Bez smanjenja općenitosti možemo pretpostaviti da podgrupa $N$ sadrži element

$$x = (123)(456)y$$

pri čemu je $y$ permutacija koja ostavlja fiksnima $1, 2, 3, 4, 5$ i $6$. Neka je $t = (234) \in A_n$. Tada $N$ sadrži element

$$\left(t^{-1}xt\right) x^{-1} = (12436).$$

Prema razmotrenom slučaju ($a$) tada $N$ sadrži neki 3−ciklus.

($c$) Pretpostavimo sada da $N$ sadrži element $x$ oblika $(ijk)p$, gdje je $p$ produkt 2−ciklusa, koji su disjuntni međusobno i svi su disjunktni sa $(ijk)$. Tada $N$ sadrži $x^2 = (ikj)$, a to je 3−ciklus.

($d$) Preostaje još samo slučaj kad je svaki element od $N \setminus \{e\}$ umnožak međusobno disjunktnih 2−ciklusa. Kao što smo vidjeli prije ovoga teorema, to se stvarno može dogoditi ako je $n = 4$; naime takva je upravo podgrupa koju smo označili sa $H$. Međutim, kako je $n \geq 5$, možemo pretpostaviti da $N$ sadrži element

$$x = (12)(34)p$$

pri čemu je $p$ permutacija koja ostavlja fiksnima $1, 2, 3$ i $4$. Stavimo $t = (234)$. Tada $N$ sadrži element

$$\left(t^{-1}xt\right) x^{-1} = (14)(23).$$

Nadalje, za $u = (145)$, normalna podgrupa $N$ sadrži element

$$u^{-1}\left(t^{-1}xtx^{-1}\right) u = (45)(23).$$

Slijedi da $N$ sadrži i element

$$(45)(23)(14)(23) = (154)$$

suprotno pretpostavci da je svaki element od $N \setminus \{e\}$ umnožak međusobno disjuntnih 2−ciklusa. Dakle, slučaj ($d$) nije moguć, ako je $n \geq 5$.

Time je dokazano da normalna podgrupa $N$ sadrži neki 3−ciklus.

(2) Pretpostavimo da je $(ijk) \in N$ i da je $m \in \{1, 2, \ldots, n\} \setminus \{i, j, k\}$. Tada je

$$(mk)(ijk)(mk)^{-1} = (mk)(ijk)(mk) = (ijm).$$

Odatle očito slijedi da $N$ sadrži sve 3−cikluse. No kako je prema propoziciji 2.9. grupa $A_n$ generirana 3−ciklusima, slijedi $N = A_n$.

Time je teorem dokazan.

Budući da je prema tvrdnji ($a$) teorema 2.4 svaka podgrupa rješive grupe rješiva, iz teorema 2.6 neposredno slijedi:

**Korolar 2.1.** *Ako je $n \geq 5$, grupa permutacija $S_n$ nije rješiva.*

## 2.5 Sylowljevi teoremi

Prema Lagrangeovom teoremu 2.1. ako je $H$ podgrupa konačne grupe $G$ onda je red grupe $G$ djeljiv s redom grupe $G$. U ovom odjeljku dokazat ćemo da za svaki djelitelj od $|G|$ oblika $p^k$, gdje je $p$ prost broj, postoji podgrupa od $G$ reda $p^k$. Najprije dokazujemo tu tvrdnju za $k = 1$ :

**Teorem 2.7.** (**Cauchyjev teorem**) *Neka je $G$ konačna grupa i neka je $p$ prost broj koji dijeli red grupe $G$. Tada grupa $G$ sadrži podgrupu reda $p$. Drugim riječima, grupa $G$ sadrži element $a$ čiji je period $p$.*

**Dokaz:** ($a$) Dokažimo najprije taj teorem u slučaju da je grupa $G$ komutativna. Dokaz provodimo indukcijom u odnosu na red $|G|$ grupe $G$. Baza indukcije je trivijalna, jer ako je $|G|$ prost broj, onda je $|G| = p$, dakle, sama $G$ je svoja podgrupa reda $p$. Provedimo sada korak indukcije i pretpostavimo da je tvrdnja dokazana za grupe reda manjeg od $|G|$. Neka je $M$ podgrupa od $G$ koja je različita od $G$ i koja među svim podgrupama od $G$ različitim od $G$ ima najveći red. Stavimo $|M| = m$.

Ako $p \mid m$, po pretpostavci indukcije grupa $M$ ima podgrupu $H$ koja je reda $p$. Kako je tada $H$ podgrupa od $G$, tvrdnja je u tom slučaju dokazana.

Pretpostavimo sada da $p \nmid m$. Neka je $b \in G \setminus M$ i označimo sa $B$ cikličku podgrupu $\langle b \rangle$ generiranu s elementom $b$. Tada je $MB = \{xy;\ x \in M,\, y \in B\}$ podgrupa od $G$ koja sadrži $M$ i $MB \neq M$, jer $b \in MB$, ali $b \notin M$. Prema izboru podgrupe $M$ slijedi da je $MB = G$.

Promatrajmo sada Kartezijev produkt

$$M \times B = \{(x, y);\ x \in M,\, y \in B\}.$$

Ako operaciju množenja definiramo po komponentama

$$(x_1, y_1)(x_2, y_2) = (x_1y_1, x_2y_2), \qquad x_1, x_2 \in M, \quad y_1, y_2 \in B,$$

onda $M \times B$ postaje grupa. Definiramo sada preslikavanje $\varphi : M \times B \to G$ na sljedeći način:

$$\varphi((x, y)) = xy, \qquad x \in M, \quad y \in B.$$

Tada je zbog jednakosti $MB = G$ preslikavanje $\varphi$ surjekcija. Nadalje, zbog komutativnosti grupe $G$ preslikavanje $\varphi$ je homomorfizam grupa:

$$\varphi((x_1, y_1)(x_2, y_2)) = \varphi((x_1x_2, y_1y_2)) = x_1x_2y_1y_2 = x_1y_1x_2y_2 = \varphi((x_1, y_1))\varphi((x_2, y_2)).$$

Dakle, $\varphi$ je epimorfizam grupe $M \times B$ na grupu $G$. Prema teoremu 2.2 grupa $G$ izomorfna je kvocijentnoj grupi $(M \times B)/(\operatorname{Ker}\varphi)$. Posebno je

$$|G| = \frac{|M \times B|}{|\operatorname{Ker}\varphi|}.$$

Međutim, očito je $|M \times B| = |M| \cdot |B|$. Nadalje,

$$\operatorname{Ker}\varphi = \{(x, y);\ x \in M,\, y \in B,\, xy = e\} = \left\{\left(x, x^{-1}\right);\ x \in M \cap B\right\}.$$

Dakle, $|\operatorname{Ker}\varphi| = |M \cap B|$. Prema tome je

$$|G| = \frac{|M| \cdot |B|}{|M \cap B|}.$$

Stavimo $|B| = r$. Tada je $B = \{e, b, b^2, \ldots, b^{r-1}\}$. Nadalje, budući da je $p$ prost broj, iz gornje formule za red $|G|$ grupe $G$ i iz pretpostavke da $p \nmid m$ slijedi da $p \mid r$. Stavimo li $q = r/p$, nalazimo da je $A = \langle b^q \rangle = \{e, b^q, b^{2q}, \ldots, b^{(p-1)q}\}$ podgrupa od $G$ reda $p$. Time je proveden korak indukcije, dakle, teorem je dokazan u slučaju da je grupa $G$ komutativna.

($b$) Dokažimo sada teorem u općem slučaju, tj. bez pretpostavke da je grupa $G$ komutativna. I taj dokaz provodimo indukcijom u odnosu na red $|G|$ grupe $G$. Baza indukcije je ponovo trivijalna, jer je trivijalna tvrdnja teorema ako je red $|G|$ grupe $G$ prost broj. Provedimo sada korak indukcije i pretpostavimo da je teorem dokazan za grupe manjeg reda od $|G|$. Neka su sada $C_1, C_2, \ldots, C_r$ sve klase konjugiranosti u grupi $G$. Uzmimo da je $C_1$ klasa konjugiranosti jedinice, $C_1 = \{e\}$. Tada je $|C_1| = 1$, pa imamo

$$|G| = 1 + |C_2| + \cdots + |C_r|.$$

Budući da prost broj $p$ dijeli red $|G|$ grupe $G$, iz ove jednakosti slijedi da za neko $j \geq 2$ broj $|C_j|$ nije djeljiv sa $p$. Neka je $x \in C_j$. Tada je $|G| = |C_j| \cdot |C_G(x)|$, pa slijedi da je red $|C_G(x)|$ centralizatora $C_G(x)$ elementa $x$ djeljiv sa $p$.

Ako je $C_G(x) \neq G$, iz pretpostavke indukcije slijedi da grupa $C_G(x)$ ima podgrupu $H$ reda $p$. No $H$ je tada podgrupa od $G$, pa je teorem u tom slučaju dokazan.

Pretpostavimo sada da je $C_G(x) = G$. To znači da je $x \in Z(G)$. Po pretpostavci je $x \neq e$, dakle, možemo zaključiti da je u tom slučaju $Z(G) \neq \{e\}$. Razmotrimo sada dvije mogućnosti:

(1) Pretpostavimo da je red $|Z(G)|$ centra $Z(G)$ grupe $G$ djeljiv sa $p$. Kako je grupa $Z(G)$ komutativna, iz dokazanog u ($a$) slijedi da $Z(G)$ ima podgrupu $H$ reda $p$. Tada je $H$ podgrupa od $G$, pa je i u tom slučaju teorem dokazan.

(2) Pretpostavimo sada da $|Z(G)|$ nije djeljiv sa $p$. Budući da je $|G| = |Z(G)| \cdot |G/Z(G)|$, zaključujemo da je red kvocijentne grupe $G/Z(G)$ djeljiv sa $p$. Kako je $Z(G) \neq \{e\}$, to je $|G/Z(G)| < |G|$, pa po pretpostavci indukcije kvocijentna grupa $G/Z(G)$ ima podgrupu reda $p$, odnosno, u postoji element $\eta \in G/Z(G)$ čiji je period jednak $p$. Neka je $\pi : G \to G/Z(G)$ epimorfizam koji elementu iz $G$ pridružuje njegovu $Z(G)-$klasu i neka je $y \in G$ takav da je $\eta = \pi(y)$. Sada iz $\eta \neq e_{G/Z(G)}$ i $\eta^p = e_{G/Z(G)}$ slijedi da je $y \notin Z(G)$ i $y^p \in Z(G)$. Neka je $Y = \langle y \rangle$ podgrupa od $G$ generirana sa $y$. Tada je $YZ(G) = \{ab;\ a \in Y,\ b \in Z(G)\}$ komutativna podgrupa od $G$ i imamo sljedeću disjunktnu uniju

$$YZ(G) = Z(G) \cup yZ(G) \cup y^2Z(G) \cup \cdots \cup y^{p-1}Z(G).$$

Odatle je $|YZ(G)| = p \cdot |Z(G)|$. Dakle, red komutativne grupe $YZ(G)$ djeljiv je sa $p$ pa opet iz dokazanog u ($a$) slijedi da grupa $YZ(G)$ sadrži podgrupu $H$ reda $p$. Kako je tada $H$ podgrupa od $G$, i u ovom je slučaju teorem dokazan.

Neka je $p$ prost broj. $p-$**grupa** je konačna grupa $G$ reda $|G| = p^n$ za neki prirodan broj $n$. Podgrupa $H$ konačne grupe $G$ zove se $p-$**podgrupa** ako je $H$ $p-$grupa. Naravno, da bi konačna grupa $G$ uopće imala netrivijalnu $p-$podgrupu nužno je da je njen red $|G|$ djeljiv sa $p$. Iz Cauchyjevog teorema 2.7 slijedi da je to i dovoljno. Podgrupa $H$ konačne grupe $G$ zove se **Sylowljeva** $p-$**podgrupa** od $G$ ako je $H$ $p-$podgrupa i ako indeks $(G : H)$ podgrupe $H$ u grupi $G$ nije djeljiv s $p$. Kako je prema Lagrangeovom teoremu $(G : H) = \frac{|G|}{|H|}$ to znači da je $|H| = p^n$ i $|G| = p^n m$, pri čemu $m$ nije djeljiv sa $p$.

Iz ove definicije nije jasno da li za neki prost broj $p$ konačna grupa čiji je red djeljiva sa $p$ uopće ima Sylowljevih $p-$podgrupa. Cilj je ovog poglavlja da dokažemo izuzetno značajne strukturne teoreme o konačnim grupama, tzv. *Sylowljeve teoreme*, koji govore o egzistenciji i opisu Sylowljevih podgrupa.

**Teorem 2.8.** (**Prvi Sylowljev teorem**) *Neka je $G$ konačna grupa reda $n$ i neka je $p$ prost broj koji dijeli $n$. Tada postoji Sylowljeva $p-$podgrupa grupe $G$.*

**Dokaz** ćemo provesti indukcijom u odnosu na red grupe. Pretpostavka teorema može biti ispunjena samo ako je $|G| \geq p$, dakle baza indukcije je $|G| = p$. U tom slučaju tvrdnja je trivijalna, jer je tada sama grupa $G$ svoja Sylowljeva $p-$podgrupa.

Provedimo sada korak indukcije i pretpostavimo da je $n > p$ djeljiv sa $p$ i da je tvrdnja dokazana za sve grupe čiji je red manji od $n$ i djeljiv sa $p$. Neka je $|G| = n$. Imamo dvije mogućnosti:

$(a)$ Postoji podgrupa $H \lneq G$ čiji indeks $(G : H)$ u grupi $G$ nije djeljiv sa $p$. Tada za neki prirodan broj $s$ vrijedi

$$|G| = p^s m \qquad \text{i} \qquad |H| = p^s q, \qquad m, q \in \mathbb{N}, \quad p \not| m, \quad p \not| q.$$

Imamo $|H| < n$ pa po pretpostavci indukcije grupa $H$ ima barem jednu Sylowljevu $p-$podgrupu. Ta je podgrupa reda $p^s$, dakle to je ujedno Sylowljeva $p-$podgrupa od $G$.

$(b)$ Druga je mogućnost da takva podgrupa $H$ ne postoji. To znači da je za svaku podgrupu $H \lneq G$ njen indeks $(G : H)$ djeljiv sa $p$. Neka je $Z = Z(G)$ centar grupe $G$. Definiramo djelovanje grupe $G$ na samoj sebi konjugiranjem: elementu $a \in G$ pridružujemo bijekciju $\varphi_a : G \to G$ definiranu sa $\varphi_a(x) = axa^{-1}$, $x \in G$. Orbita i stabilizator elementa $x \in G$ s obzirom na to djelovanje su

$$\mathcal{O}(x) = \{axa^{-1};\ a \in G\}, \qquad C_G(x) = \{a \in G;\ ax = xa\}.$$

Imamo $Z \subseteq C_G(x)\ \forall x \in G$. Nadalje, orbita $\mathcal{O}(x)$ je jednočlan skup ako i samo ako je $C_G(x) = G$, odnosno, ako i samo ako je $x \in Z$. Neka je $S \subset G$ skup predstavnika svih višečlanih $G-$orbita u $G$. Tada imamo

$$G = Z \cup \bigcup_{x \in S} \mathcal{O}(x)$$

i to je disjunktna unija. Dakle, vrijedi

$$n = |Z| + \sum_{x \in S} |\mathcal{O}(x)|.$$

Prema propoziciji 2.7 broj $|\mathcal{O}(x)|$ elemenata orbite $\mathcal{O}(x)$ jednak je indeksu $(G : C_G(x))$ centralizatora $C_G(x)$ elementa $x$ u grupi $G$, pa imamo

$$n = |Z| + \sum_{x \in S} (G : C_G(x)).$$

Za svaki $x \in S$ je $C_G(x) \lneq G$, pa je po pretpostavci (b) indeks $(G : C_G(x))$ djeljiv sa $p$. Po pretpostavci je i $n$ djeljiv sa $p$, dakle, prema gornjoj jednakosti red $|Z|$ centra $Z$ grupe $G$ djeljiv je sa $p$. Prema Cauchyjevom teoremu 2.7 $Z$ ima cikličku podgrupu $H$ reda $p$. Kako je $H$ centralna podgrupa od $G$, ona je normalna podgrupa od $G$, pa možemo formirati kvocijentnu grupu $G/H$. Neka je $p^m$ najveća potencija od $p$ koja dijeli $n = |G|$. Budući da je $|G/H| = \frac{n}{p}$, to je $p^{m-1}$ najveća potencija koja dijeli $|G/H| = (G : H)$. Po pretpostavci indukcije grupa $G/H$ ima Sylowljevu $p-$podgrupu, dakle postoji podgrupa $X$ grupe $G/H$ kojoj je red $p^{m-1}$. Neka je $\pi : G \to G/H$ kanonski epimorfizam koji svakom elementu grupe $G$ pridružuje njegovu $H-$klasu: $\pi(a) = aH,\ a \in G$. Stavimo

$$Y = \pi^{-1}(X) = \{a \in G;\ \pi(a) \in X\}.$$

Uočimo da je $Y$ podgrupa od $G$. Doista, ako su $a, b \in Y$, tada je $\pi(a), \pi(b) \in X$, dakle i $\pi(ab^{-1}) = \pi(a)\pi(b)^{-1} \in X$, jer je $X$ podgrupa od $G/H$. To pokazuje da je $ab^{-1} \in Y$, dakle $Y$ je stvarno podgrupa od $G$. Napokon, $Y$ je unija svih $H-$klasa koje čine grupu $X$. Budući da svaka $H-$klasa u $G$ ima $p$ elemenata, to je red od $Y$ jednak $p \cdot |X| = p \cdot p^{m-1} = p^m$. Dakle, $Y$ je

podgrupa od $G$ reda $p^m$, što znači da je $Y$ Sylowljeva $p-$podgrupa od $G$.

Time je teorem u potpunosti dokazan.

I dalje promatramo konjugiranje u grupi $G$, tj. djelovanje izomorfizama $\varphi_a : G \to G$, $a \in G$. Ako je $H$ podgrupa od $G$ i $a \in G$, onda je i $\varphi_a(H) = aHa^{-1}$ podgrupa od $G$. **Podgrupe** $H$ i $K$ zovu se **konjugirane** ako postoji $a \in G$ takav da je $K = aHa^{-1}$. Konjugirane podgrupe imaju isti broj elemenata, dakle ako je $H$ Sylowljeva $p-$podgrupa od $G$ onda je i $aHa^{-1}$ Sylowljeva $p-$podgrupa od $G$ $\forall a \in G$.

U daljnjem za grupu $G$ reda $n$ koji je djeljiv s prostim brojem $p$ označimo sa $\mathcal{S}$ skup svih Sylowljevih $p-$podgrupa od $G$. Grupa $G$ djeluje konjugacijama na skupu $\mathcal{S}$. Orbita i stabilizator Sylowljeve podgrupe $P$ su:

$$\mathcal{O}(P) = \{aPa^{-1};\ a \in G\}, \qquad G_P = \{a \in G;\ aPa^{-1} = P\}.$$

**Teorem 2.9.** (**Drugi Sylowljev teorem**) *Neka je $G$ konačna grupa i neka je njen red $n$ djeljiv s prostim brojem $p$.*

*(a) Svaka $p-$podgrupa grupe $G$ sadržana je u nekoj Sylowljevoj $p-$podgrupi grupe $G$.*

*(b) Sve Sylowljeve $p-$podgrupe od $G$ međusobno su konjugirane. Dakle, ako su $P$ i $Q$ Sylowljeve $p-$podgrupe od $G$ onda postoji $a \in G$ takav da je $Q = aPa^{-1}$.*

**Dokaz:** Dokazat ćemo najprije sljedeću tvrdnju:

*Neka je $H$ $p-$podgrupa grupe $G$ i neka je $P$ Sylowljeva $p-$podgrupa grupe $G$. Postoji $a \in G$ takav da je $H \subseteq aPa^{-1}$.*

Kao prije iskaza teorema sa $\mathcal{S}$ označavamo skup svih Sylowljevih $p-$podgrupa od $G$. Na skupu $\mathcal{S}$ grupa $G$ djeluje konjugacijama. Neka je $\mathcal{O}(P) \subseteq \mathcal{S}$ $G-$orbita od $P$ :

$$\mathcal{O}(P) = \{aPa^{-1};\ a \in G\}.$$

Promatrajmo sada djelovanje grupe $H$. Za $Q \in \mathcal{O}(P)$ i $x \in H$ očito je i $xQx^{-1} \in \mathcal{O}(P)$, dakle grupa $H$ djeluje konjugacijama na skupu $\mathcal{O}(P)$. U odnosu na to djelovanje $G-$orbita $\mathcal{O}(P)$ raspada se u disjunktnu uniju $H-$orbita. Neka je $\mathcal{T}$ skup predstavnika svih $H-$orbita u $\mathcal{O}(P)$. Za $Q \in \mathcal{T}$ stavimo

$$\mathcal{O}_H(Q) = \{xQx^{-1};\ x \in H\}, \qquad H_Q = \{x \in H;\ xQx^{-1} = Q\}, \qquad Q \in \mathcal{T}.$$

Imamo disjunktnu uniju

$$\mathcal{O}(P) = \bigcup_{Q \in \mathcal{T}} \mathcal{O}_H(Q),$$

dakle broj elemenata u $G-$orbiti $\mathcal{O}(P)$ jednak je zbroju broja elemenata u $H-$orbitama:

$$|\mathcal{O}(P)| = \sum_{Q \in \mathcal{T}} |\mathcal{O}_H(Q)|.$$

$H$ je $p-$podgrupa od $G$ dakle njen red je neka potencija $p^s$ prostog broja $p$. Budući da je red podgrupe djelitelj reda grupe, red bilo koje podgrupe $K$ od $H$ je neka potencija $p^r$ prostog broja $p$; indeks $(H : K)$ od $K$ u $H$ je kvocijent $\frac{|H|}{|K|}$, dakle $(H : K) = p^m$ za neki nenegativan cijeli broj $m$. Posebno, to vrijedi za svaki stabilizator $H_Q$ točke $Q \in \mathcal{T}$ u grupi $H$. Prema propoziciji 2.7 broj elemenata $H-$orbite $\mathcal{O}_H(Q)$ jednak je indeksu $(H : H_Q)$ stabilizatora $H_Q$ u grupi $H$. Za

svaki $Q \in \mathcal{T}$ označimo sa $m(Q)$ nenegativan cijeli broj takav da je $(H : H_Q) = p^{m(Q)}$. Iz gornje jednakosti stoga slijedi:

$$|\mathcal{O}(P)| = \sum_{Q \in \mathcal{T}} p^{m(Q)}.$$

Imamo $|\mathcal{O}(P)| = (G : G_P)$ pri čemu je $G_P = \{a \in G;\ aPa^{-1} = P\}$. Očito je $P \subseteq G_P$, to je indeks $(G : G_P)$ djelitelj indeksa $(G : P)$. No po definiciji Sylowljeve $p-$podgrupe indeks $(G : P)$ nije djeljiv sa $p$. Slijedi da ni $(G : G_P)$ nije djeljiv sa $p$. Dakle, broj $|\mathcal{O}(P)|$ elemenata $G-$orbite od $P$ nije djeljiv sa $p$. Sada iz gornje jednakosti slijedi da mora biti $m(Q) = 0$ za barem jednu $Q \in \mathcal{T}$.

Neka je $Q \in \mathcal{T}$ takva podgrupa, tj. $m(Q) = 0$. Tada je $(H : H_Q) = 1$, dakle $H_Q = H$. To znači da je $xQx^{-1} = Q\ \ \forall x \in H$. Stavimo

$$HQ = \{xa;\ x \in H,\ a \in Q\}.$$

Iz utvrđene činjenice $xQx^{-1} = Q\ \ \forall x \in H$ slijedi da je $HQ$ podgrupa grupe $G$ i da je $Q$ normalna podgrupa od $HQ$. Dakle, možemo formirati kvocijentnu grupu $HQ/Q$.

Očito je $H \cap Q$ podgrupa od $H$. Nadalje, za $x \in H$ imamo $xHx^{-1} = H$ i $xQx^{-1} = Q$, dakle $x(H \cap Q)x^{-1} \subseteq H \cap Q$. Budući da konačni skupovi $x(H \cap Q)x^{-1}$ i $H \cap Q$ imaju isti broj elemenata, iz dokazane inkluzije slijedi jednakost:

$$x(H \cap Q)x^{-1} = H \cap Q, \qquad \forall x \in H.$$

Dakle, $H \cap Q$ je normalna podgrupa od $H$.

Definiramo sada preslikavanje $\Phi : H/(H \cap Q) \to (HQ)/Q$ s kvocijentne grupe $H/(H \cap Q)$ u kvocijentnu grupu $(HQ)/Q$ :

$$\Phi(x(H \cap Q)) = xQ, \qquad x \in H.$$

Definicija ima smisla, jer ako za neke $x, y \in H$ vrijedi $x(H \cap Q) = y(H \cap Q)$, onda je $y^{-1}x \in H \cap Q \subseteq Q$, dakle, $xQ = yQ$. Dokažimo da je $\Phi$ izomorfizam grupa. Budući da je množenje u kvocijentnoj grupi definirano preko množenja predstavnika, očito je $\Phi$ homomorfizam grupa. Pretpostavimo da su $x, y \in H$ takvi da je $\Phi(x(H \cap Q)) = \Phi(y(H \cap Q))$. To znači da je $xQ = yQ$. Odatle slijedi $y^{-1}x \in Q$, a kako su $x, y \in H$ to je i $y^{-1}x \in H$. Dakle je $y^{-1}x \in H \cap Q$, što znači da je $x(H \cap Q) = y(H \cap Q)$. Time smo dokazali da je $\Phi$ injekcija. $\Phi$ je i surjekcija. Doista, neka je $yQ$, $y \in HQ$, proizvoljan element kvocijentne grupe $(HQ)/Q$. Tada je $y = xa$ za neke $x \in H$ i $a \in Q$. Slijedi $x^{-1}y = a \in Q$, dakle $yQ = xQ = \Phi(x(H \cap Q))$. Prema tome, $\Phi$ je i surjekcija. Time je dokazano da je $\Phi : H/(H \cap Q) \to (HQ)/Q$ izomorfizam grupa.

Red kvocijentne grupe $H/(H \cap Q)$ je djelitelj reda grupe $H$, dakle to je potencija broja $p$. Prema tome, red njoj izomorfne kvocijentne grupe $(HQ)/Q$ je potencija od $p$, a kako je $Q$ $p-$grupa, to je prema Lagrangeovom teoremu (teorem 2.1) i $HQ$ $p-$grupa. Dakle, $HQ$ je $p-$podgrupa koja sadrži $Q$. Ali $Q$ je maksimalna $p-$podgrupa, pa slijedi $HQ = Q$, odnosno, $H \subseteq Q$. Time je iskazana tvrdnja u potpunosti dokazana.

Iz dokazane tvrdnje odmah slijedi tvrdnja $(a)$ teorema, jer podgrupa konjugirana Sylowljevoj $p-$podgrupi i sama je Sylowljeva $p-$podgrupa. Nadalje, ako su $Q$ i $P$ Sylowljeve $p-$podgrupe od $G$, prema dokazanoj tvrdnji postoji $a \in G$ takav da je $Q \subseteq aPa^{-1}$. Međutim, $Q$ i $aPa^{-1}$ su podgrupe istoga reda, jer su obje te podgrupe Sylowljeve $p-$podgrupe. Dakle, iz inkluzije slijedi jednakost $Q = aPa^{-1}$, pa je time dokazana i tvrdnja $(b)$ teorema.

Time je drugi Sylowljev teorem u potpunosti dokazan.

**Teorem 2.10.** (**Treći Sylowljev teorem**) *Neka je $G$ konačna grupa i neka je njen red $n$ djeljiv s prostim brojem $p$. Broj Sylowljevih $p-$podgrupa od $G$ umanjen za 1 djeljiv je sa $p$. Preciznije, ako je $k$ broj Sylowljevih $p-$podgrupa od $G$ onda je za neki $s \in \mathbb{N}$ i za neke $k_1, \ldots, k_s \in \mathbb{N}$ :*

$$k = 1 + \sum_{j=1}^{s} p^{k_j}.$$

**Dokaz:** Neka je $\mathcal{S}$ skup svih Sylowljevih $p-$podgrupa grupe $G$ i neka je $P \in \mathcal{S}$. Prema tvrdnji $(b)$ teorema 2.9 $\mathcal{S} = \{aPa^{-1};\ a \in G\}$. Promatrajmo sada djelovanje grupe $P$ na skupu $\mathcal{S}$ pomoću konjugacija. Za $Q \in \mathcal{S}$ označimo sa $\mathcal{O}_P(Q)$ njenu $P-$orbitu i sa $P_Q$ njen stabilizator u $P$ :

$$\mathcal{O}_P(Q) = \{xQx^{-1};\ x \in P\}, \qquad P_Q = \{x \in P;\ xQx^{-1} = Q\}.$$

Očito je $P_P = P$, odnosno $\mathcal{O}_P(P) = \{P\}$. Posebno, $|\mathcal{O}_P(P)| = 1$. Pretpostavimo da je za neku podgrupu $Q \in \mathcal{S}$ njena $P-$orbita jednočlan skup: $|\mathcal{O}_P(Q)| = 1$. To znači da je $xQx^{-1} = Q\ \ \forall x \in P$. Odatle kao u dokazu teorema 2.9 slijedi $PQ = Q$, dakle $P \subseteq Q$, a odatle je $P = Q$. Prema tome, ako je $Q \in \mathcal{S}$ i $Q \neq P$ onda je $|\mathcal{O}_P(Q)| > 1$. Međutim, $|\mathcal{O}_P(Q)| = (P : P_Q)$, a to je neka potencija $p^{m(Q)}$ broja $p$. Dakle, ako sa $\mathcal{R}$ označimo skup predstavnika svih $P-$orbita u $\mathcal{S}$ osim $\{P\}$, onda je

$$|\mathcal{S}| = 1 + \sum_{Q \in \mathcal{R}} p^{m(Q)}.$$

Time je teorem dokazan.

# Poglavlje 3

# Komutativni prsteni

## 3.1 Prsteni i moduli

Podsjetimo se osnovnih definicija iz teorije prstenova. **Prsten** je neprazan skup $R$ na kome su zadane dvije binarne operacije, *zbrajanje* $(a, b) \mapsto a + b$ i *množenje* $(a, b) \mapsto ab$, sa sljedećim svojstvima:

(a) U odnosu na zbrajanje $R$ je komutativna grupa; neutralni element se označava sa 0 i zove *nula*.

(b) U odnosu na množenje $R$ je polugrupa (odnosno, množenje je asocijativno).

(c) Množenje je i slijeva i zdesna distributivno u odnosu na zbrajanje, tj. vrijedi:

$$a(b + c) = ab + ac \qquad \text{i} \qquad (a + b)c = ac + bc \qquad \forall a, b, c \in R.$$

Znamo da u prstenu $R$ za svaki element $a$ vrijedi $0a = a0 = 0$. $R$ se zove **unitalni prsten**, ako je $R$ u odnosu na množenje monoid, tj. postoji (nužno jedinstven) element $1 \in R$ takav da je $a1 = 1a = a\ \forall a \in R$; taj se element 1 zove **jedinica prstena** $R$. U unitalnom prstenu $R$ je $1 = 0$ ako i samo ako je $R = \{0\}$; to je tzv. *trivijalan prsten*. U netrivijalnom unitalnom prstenu $R \neq \{0\}$ je $1 \neq 0$.

Potprsten prstena $R$ je podskup $S$ koji je i sam prsten u odnosu na zadane operacije. To znači da je $S \neq \emptyset$ i da iz $a, b \in S$ vrijedi $a - b \in S$ i $ab \in S$. Ako je prsten $R$ unitalan s jedinicom 1 *potprsten* $S$ se zove **unitalan** ako je $1 \in S$.

Neka su $R$ i $S$ prstenovi. Preslikavanje $\varphi : R \to S$ se zove **homomorfizam prstenova** ako vrijedi

$$\varphi(a + b) = \varphi(a) + \varphi(b) \qquad \text{i} \qquad \varphi(ab) = \varphi(a)\varphi(b) \qquad \forall a, b \in R.$$

Iz propozicije 1.6. slijedi da je tada $\varphi(0) = 0$ i $\varphi(-a) = -\varphi(a)$, $a \in R$. Ako su $R$ i $S$ unitalni prstenovi s jedinicama $1_R$ i $1_S$, **homomorfizam prstenova** $\varphi : R \to S$ zove se **unitalan** ako je $\varphi(1_R) = 1_S$. Injektivni homomorfizam zove se **monomorfizam prstenova**, surjektivni homomorfizam je **epimorfizam prstenova**, a bijektivni homomorfizam je **izomorfizam prstenova**. Inverzno preslikavanje izomorfizma prstenova očito je također izomorfizam prstenova. Nadalje, kompozicija $\psi \circ \varphi : R \to T$ izomorfizama prstenova $\varphi : R \to S$ i $\psi : S \to T$ je izomorfizam prstenova. Stoga je izomorfnost prstenova relacija ekvivalencije. Pri tome kažemo da je **prsten** $R$ **izomorfan prstenu** $S$ i pišemo $R \equiv S$ ako postoji izomorfizam prstenova $\varphi : R \to S$.

Očito je slika homomorfizma prstenova $\varphi : R \to S$

$$\operatorname{Im} \varphi = \varphi(R) = \{\varphi(a);\ a \in R\}$$

potprsten prstena $S$. Doista, za $c, d \in \operatorname{Im}\varphi$ postoje $a, b \in R$ takvi da je $c = \varphi(a)$ i $d = \varphi(b)$, pa imamo

$$c - d = \varphi(a) - \varphi(b) = \varphi(a - b) \in \operatorname{Im}\varphi \qquad \text{i} \qquad cd = \varphi(a)\varphi(b) = \varphi(ab) \in \operatorname{Im}\varphi.$$

Jezgra homomorfizma $\varphi$

$$\operatorname{Ker}\varphi = \{a \in R;\ \varphi(a) = 0\}$$

je potprsten od $R$, jer za $a, b \in \operatorname{Ker}\varphi$ vrijedi

$$\varphi \quad \Longrightarrow \quad \varphi(a - b) = \varphi(a) - \varphi(b) = 0 - 0 = 0 \qquad \Longrightarrow \qquad a - b \in \operatorname{Ker}\varphi$$

i

$$\varphi(ab) = \varphi(a)\varphi(b) = 0 \cdot 0 = 0 \qquad \Longrightarrow \qquad ab \in \operatorname{Ker}\varphi.$$

Taj potprsten ima još i svojstvo da za svaki $a \in \operatorname{Ker}\varphi$ i svaki $b \in R$ vrijedi $ab, ba \in \operatorname{Ker}\varphi$ :

$$\varphi(ab) = \varphi(a)\varphi(b) = 0\varphi(b) = 0, \qquad \varphi(ba) = \varphi(b)\varphi(a) = \varphi(b)0 = 0.$$

U vezi s tim imamo sljedeće definicije: aditivna podgrupa $J$ prstena $R$ zove se **lijevi ideal** u prstenu $R$ ako vrijedi

$$a \in J, \quad b \in R \qquad \Longrightarrow \qquad ba \in J,$$

a **desni ideal** u prstenu $R$ ako vrijedi

$$a \in J, \quad b \in R \qquad \Longrightarrow \qquad ab \in J.$$

Ako je $J$ i lijevi i desni ideal u prstenu $R$ onda se $J$ zove **obostrani** ili **dvostrani ideal** u $R$.

Neka je $R$ prsten i $J$ dvostrani ideal u $R$. Tada je $J$ podgrupa aditivne komutativne grupe prstena $R$, pa možemo formirati kvocijentnu grupu $R/J$. Elementi od $R/J$ su skupovi oblika

$$a + J = \{a + b;\ b \in J\}, \qquad a \in R,$$

a grupovna operacija (zbrajanje) je zadana sa

$$(a + J) + (b + J) = (a + b) + J, \qquad a + J, b + J \in R/J, \quad \text{tj.} \quad a, b \in R.$$

Zbog svojstava dvostranog ideala ima smisla definirati i operaciju množenja na $R/J$ :

$$(a + J)(b + J) = ab + J, \qquad a + J, b + J \in R/J.$$

Doista, dokažimo smislenost ovakve definicije, tj. njenu neovisnost o izboru predstavnika klasa $a + J, b + J \in R/J$. Neka su $c \in a + J$ i $d \in b + J$ bilo koji predstavnici tih dviju klasa; tj. $a + J = c + J$ i $b + J = d + J$. Tada su $a - c, b - d \in J$, dakle, i $a(b - d), (a - c)d \in J$, pa imamo

$$ab - cd = a(b - d) + (a - c)d \in J \qquad \Longrightarrow \qquad ab + J = cd + J.$$

Time je dokazana smislenost definicije množenja na aditivnoj grupi $R/J$. To množenje je asocijativno i s obje strane distributivno u odnosu na operaciju zbrajanja. Doista, ako su $a, b, c \in R$, imamo zbog svojstava množenja u $R$ :

$$[(a+J)(b+J)](c+J) = (ab+J)(c+J) = (ab)c+J = a(bc)+J = (a+J)(bc+J) = (a+J)[(b+J)(c+J)],$$

$$(a + J)[(b + J) + (c + J)] = (a + J)[(b + c) + J] = a(b + c) + J =$$
$$= (ab + ac) + J = (ab + J) + (ac + J) = (a + J)(b + J) + (a + J)(c + J),$$

$$[(a+J)+(b+J)](c+J) = [(a+b)+J](c+J) = (a+b)c+J =$$
$$= (ac+bc)+J = (ac+J)+(bc+J) = (a+J)(c+J)+(b+J)(c+J).$$

Prema tome, s tako definiranim operacijama $R/J$ je prsten i on se zove **kvocijentni prsten** prstena $R$ po (dvostranom) idealu $J$. Ukoliko je prsten $R$ unitalan i jedinica mu je 1 onda je i kvocijentni prsten $R/J$ unitalan i jedinica mu je $1+J$ :

$$(1+J)(a+J) = 1a+J = a+J, \qquad (a+J)(1+J) = a1+J = a+J.$$

Napokon, preslikavanje $\pi : R \to R/J$ koje svakom elementu $a \in R$ pridružuje njegovu klasu $a+J \in R/J$,

$$\pi(a) = a+J, \qquad a \in R,$$

je homomorfizam prstenova:

$$\pi(a+b) = (a+b)+J = (a+J)+(b+J) = \pi(a)+\pi(b), \quad \pi(ab) = ab+J = (a+J)(b+J) = \pi(a)\pi(b);$$

$\pi$ se zove **kvocijentni homomorfizam**. Ako je prsten $R$ unitalan, taj je homomorfizam unitalan:

$$\pi(1) = 1+R.$$

Nadalje, kako je

$$R/J = \{a+J;\ a \in R\} = \{\pi(a);\ a \in R\} = \operatorname{Im}\pi,$$

vidimo da je kvocijentni homomorfizam $\pi : R \to R/J$ surjektivan, tj. $\pi$ je epimorfizam.

Neka je $\varphi : R \to S$ homomorfizam prstenova. Kao što smo već konstatirali njegova slika

$$T = \operatorname{Im}\varphi = \{\varphi(a);\ a \in R\}$$

je potprsten prstena $S$, a njegova jezgra

$$J = \operatorname{Ker}\varphi = \{a \in R;\ \varphi(a) = 0\}$$

je dvostrani ideal u prstenu $R$. Prema teoremu 2.2. dobro je definirano preslikavanje $\Phi : R/J \to T$ relacijom

$$\Phi(a+J) = \varphi(a), \qquad a+J \in R/J,$$

i to je izomorfizam aditivnih grupa prstenova $R/J$ i $T$. Nadalje, to je i homomorfizam prstenova:

$$\Phi((a+J)(b+J)) = \Phi(ab+J) = \varphi(ab) = \varphi(a)\varphi(b) = \Phi(a+J)\Phi(b+J), \qquad a+J, b+J \in R/J.$$

Dakle, $\Phi$ je izomorfizam kvocijentnog prstena $R/J$ na prsten $T$. Time je dokazan

**Teorem 3.1.** *Neka je $\varphi : R \to S$ homomorfizam prstenova.*

(a) *$T = Im\varphi$ je potprsten prstena $S$.*

(b) *$J = Ker\varphi$ je dvostrani ideal u prstenu $R$.*

(c) *Preslikavanje $\Phi : R/J \to T$ definirano sa $\Phi(a+J) = \varphi(a)$, $a \in R$, je izomorfizam kvocijentnog prstena $R/J$ na prsten $T$.*

*Ako je homomorfizam $\varphi$ unitalni, $T$ je unitalni potprsten prstena $S$ i izomorfizam $\Phi : R/J \to T$ je unitalni.*

Moduli nad prstenima definiraju se analogno vektorskim prostorima nad poljima. Neka je $R$ prsten; **lijevi modul** nad prstenom $R$ ili **lijevi $R-$modul** je komutativna aditivna grupa $V$ na kojoj je definirana operacija $R \times V \to V$, $(a, m) \mapsto am$, množenja elemenata iz $V$ s elementima iz $R$ i ako ta operacija ima sljedeća svojstva:

$(a)$ distributivnost u odnosu na zbrajanje u $R$

$$(a+b)v = av + bv, \qquad \forall a, b \in R, \quad \forall v \in V;$$

$(b)$ distributivnost u odnosu na zbrajanje u $V$

$$a(v+w) = av + aw, \qquad \forall a \in R, \quad \forall v, w \in V;$$

$(c)$ kvaziasocijativnost

$$(ab)v = a(bv), \qquad \forall a, b \in R, \quad \forall v \in V.$$

**Desni modul** nad prstenom $R$ ili **desni $R-$modul** definira se analogno: sada se operacija množenja $V \times R \to V$ označava sa $(v, a) \mapsto va$ i svojstva su

$(a')$ $v(a+b) = va + vb,\ \forall v \in V,\ \forall a, b \in R;$

$(b')$ $(v+w)a = va + wa,\ \forall v, w \in V,\ \forall a \in R;$

$(c')$ $v(ab) = (va)b,\ \forall v \in V,\ \forall a, b \in R.$

Ako je prsten $R$ unitalan, **lijevi $R-$modul** $V$ je **unitalan** ako vrijedi

$(d)$ $1v = v\ \ \forall v \in V.$

Analogno, **unitalan desni $R-$modul** je onaj za koji vrijedi

$(d')$ $v1 = v\ \ \forall v \in V.$

U daljnjem ćemo se baviti isključivo s lijevim $R-$modulima; naravno, za sve tvrdnje vrijede i analogne tvrdnje za desne $R-$module.

Neka su $V$ i $W$ lijevi $R-$moduli. Preslikavanje $\psi : V \to W$ se zove **homomorfizam $R-$modula** ili **$R-$homomorfizam** vrijedi

$$\psi(v+v') = \psi(v) + \psi(v'), \qquad \psi(av) = a\psi(v), \qquad \forall v, v' \in V, \quad \forall a \in R.$$

Ako je $V$ lijevi $R-$modul, $W \subseteq V$ se zove **podmodul** ako je $W$ modul s obzirom na iste operacije, tj. $W$ je podgrupa

$$v, w \in W \qquad \Longrightarrow \qquad v - w \in W$$

i vrijedi

$$a \in R, \quad v \in W \qquad \Longrightarrow \qquad av \in W.$$

U tom slučaju na kvocijentnoj grupi $V/W = \{v + W;\ v \in V\}$ možemo definirati množenje elementima iz $R$ :

$$a(v+W) = av + W, \qquad a \in R, \quad v + W \in V/W.$$

Definicija je smislena, jer ako je $v'$ drugi predstavnik klase $v + W$, tj. $v + W = v' + W$, tada je $v - v' \in W$, dakle i $a(v - v') \in W$, pa imamo

$$av - av' = a(v - v') \in W \qquad \Longrightarrow \qquad av + W = av' + W.$$

S tako definiranom operacijom množenja kvocijentna grupa $V/W$ postaje lijevi $R-$modul, jer za sve $a, b \in R$ i sve $v+W, v'+W \in V/W$ vrijedi:

$$(a+b)(v+W) = [(a+b)v]+W = (av+bv)+W = (av+W)+(bv+W) = a(v+W)+b(v+W);$$

$$a[(v+W)+(v'+W)] = a[(v+v')+W] = [a(v+v')]+W =$$
$$= (av+av')+W = (av+W)+(av'+W) = a(v+W)+a(v'+W);$$
$$(ab)(v+W) = [(ab)v]+W = [a(bv)]+W = a(bv+W) = a[b(v+W)].$$

$R-$modul $V/W$ zovemo **kvocijentni modul** lijevog $R-$modula $V$ po podmodulu $W$. Ako je prsten $R$ unitalan i $V$ je unitalan lijevi $R-$modul, onda je očito svaki podmodul $W$ od $V$ unitalan; u tom slučaju je i kvocijentni modul $V/W$ unitalan:

$$1(v+W) = 1v+W = v+W \qquad \forall v+W \in V/W.$$

Iz teorema 2.2. neposredno slijedi

**Teorem 3.2.** *Neka je $\varphi : V \to W$ homomorfizam lijevih modula nad prstenom $R$.*

(a) $U = Ker\varphi = \{v \in V;\ \varphi(v) = 0\}$ *je $R-$podmodul od $V$.*

(b) $T = Im\varphi = \{\psi(v);\ v \in V\}$ *je $R-$podmodul od $W$.*

(c) *Preslikavanje $\Phi : V/U \to T$ je sa*

$$\Phi(v+U) = \varphi(v), \qquad v \in V,$$

*dobro definirano i to je izomorfizam kvocijentnog modula $V/U$ na modul $T$.*

Štoviše, vrijede sljedeći važni teoremi:

**Teorem 3.3.** (**Prvi teorem o izomorfizmu**) *Neka je $R$ prsten, $\varphi : V \to W$ epimorfizam lijevih $R-$modula i $U = \{v \in V;\ \varphi(v) = 0\}$ njegova jezgra. Tada je*

$$T \mapsto \varphi(T) = \{\varphi(t);\ t \in T\}$$

*bijekcija sa skupa svih podmodula od $V$ koji sadrže $U$ na skup svih podmodula od $W$. Nadalje, za svaki podmodul $T$ od $V$ koji sadrži $U$ sa*

$$v+T \mapsto \varphi(v)+\varphi(T), \qquad v \in V,$$

*je definiran izomorfizam kvocijentnog modula $V/T$ na kvocijentni modul $W/\varphi(T)$.*

**Dokaz:** Prije svega, za svaki podmodul $T$ od $V$ njegova slika $\varphi(T)$ je podmodul od $W$. Doista, ako su $w, w' \in \varphi(T)$ onda postoje $t, t' \in T$ takvi da je $w = \varphi(t)$ i $w' = \varphi(t'$, tako da imamo

$$w - w' = \varphi(t) - \varphi(t') = \varphi(t-t') \in \varphi(T),$$

a također za $a \in R$ je

$$aw = a\varphi(t) = \varphi(at) \in \varphi(T).$$

Dokažimo sada injektivnost preslikavanja $T \mapsto \varphi(T)$ sa skupa svih podmodula $T$ od $V$ koji sadrže $U$ u skup svih podmodula od $W$. Neka su $T, T'$ podmoduli od $V$ koji sadrže $U$ i pretpostavimo da je $\varphi(T) = \varphi(T')$. Za $t \in T$ je tada $\varphi(t) \in \varphi(T')$, pa postoji $t' \in T'$ takav da je $\varphi(t) = \varphi(t')$. No tada je $\varphi(t-t') = 0$, tj. $u = t-t' \in U \subseteq T'$, pa slijedi $t = t'+u \in T'$. Time je

dokazano da je $T \subseteq T'$. Sasvim analogno dokazujemo da vrijedi i obrnuta inkluzija $T' \subseteq T$, dakle jednakost $T = T'$.

Dokažimo surjektivnost. Neka je $S$ podmodul od $W$. Stavimo

$$T = \varphi^{-1}(S) = \{v \in V;\ \varphi(v) \in S\}.$$

Tada je $T$ podmodul od $V$ koji sadrži $U$ :

$$t, t' \in T \implies \varphi(t - t') = \varphi(t) - \varphi(t') \in S \implies t - t' \in T;$$

$$t \in T, \quad a \in R \implies \varphi(at) = a\varphi(t) \in S \implies at \in T;$$

$$u \in U \implies \varphi(u) = 0 \in S \implies u \in T.$$

Treba još dokazati da je $\varphi(T) = S$. Ako je $t \in T$ onda je po definiciji $\varphi(t) \in S$. Dakle, vrijedi $\varphi(T) \subseteq S$. Neka je $s \in S$. Kako je $\varphi : V \to W$ surjekcija, postoji $v \in V$ takav da je $s = \varphi(v)$. No tada po definiciji od $T$ vrijedi $v \in T$, pa zaključujemo da je $s = \varphi(v) \in \varphi(T)$. Time je dokazana i obrnuta inkluzija $S \subseteq \varphi(T)$, dakle, jednakost $S = \varphi(T)$.

Dokažimo drugu tvrdnju. Neka je $T$ podmodul od $V$ koji sadrži $U = \operatorname{Ker}\varphi$. Prije svega treba dokazati da je sa

$$\Phi(v + T) = \varphi(v) + \varphi(T), \qquad v \in V,$$

dobro definirano preslikavanje sa $V/T$ u $W/\varphi(T)$. Doista, ako su $v, v' \in V$ takvi da je $v+T = v'+T$, tada je $v - v' \in T$, pa je

$$\varphi(v) - \varphi(v') = \varphi(v - v') \in \varphi(T) \qquad \Longrightarrow \qquad \varphi(v) + \varphi(T) = \varphi(v') + \varphi(T).$$

$\Phi$ je homomorfizam modula, jer za $v, v' \in V$ i $a \in R$ imamo

$$\Phi((v + T) + (v' + T)) = \Phi((v + v') + T) = \varphi(v + v') + \varphi(T) = (\varphi(v) + \varphi(v')) + \varphi(T) =$$

$$= (\varphi(v) + \varphi(T)) + (\varphi(v') + \varphi(T)) = \Phi(v + T) + \Phi(v' + T),$$

$$\Phi(a(v + T)) = \Phi(av + T) = \varphi(av) + \varphi(T) = a\varphi(v) + \varphi(T) = a(\varphi(v) + \varphi(T)) = a\Phi(v + T).$$

Dokažimo da je homomorfizam $\Phi : V/T \to W/\varphi(T)$ injektivan. Neka su $v, v' \in V$ takvi da je $\Phi(v+T) = \Phi(v'+T)$. To znači da je $\varphi(v)+\varphi(T) = \varphi(v')+\varphi(T)$, tj. $\varphi(v-v') = \varphi(v)-\varphi(v') \in \varphi(T)$. Budući da je $S \mapsto \varphi(S)$ bijekcija sa skupa svih podmodula $S$ od $V$ koji sadrže $U$ na skup svih podmodula od $W$, odatle slijedi da je $v - v' \in T$. Dakle, vrijedi $v + T = v' + T$ i time je injektivnost od $\Phi$ dokazana.

Treba još dokazati surjektivnost od $\Phi$. Neka je $w + \varphi(T)$ proizvoljan element od $W/\varphi(T)$. Kako je $\varphi : V \to W$ surjekcija, postoji $v \in V$ takav da je $w = \varphi(v)$. No tada je $w + \varphi(T) = = \varphi(v) + \varphi(T) = \Phi(v + T)$. Time je dokazana i surjektivnost homomorfizma $\Phi : V/T \to W/\varphi(T)$.

**Teorem 3.4.** (**Drugi teorem o izomorfizmu**) *Neka je $V$ lijevi modul nad prstenom $R$ i neka su $W$ i $U$ podmoduli od $V$. Tada je njihov presjek $W \cap U$ podmodul od $V$ a i suma*

$$W + U = \{w + u;\ w \in W, u \in U\}$$

*je podmodul od $V$. Sa*

$$w + (W \cap U) \mapsto w + U, \qquad w \in W,$$

*je dobro definirano preslikavanje kvocijentnog modula $W/(W \cap U)$ u kvocijentni modul $(W + U)/U$ i to je izomorfizam $R-$modula.*

**Dokaz:** Jednostavna su posljedice definicija podmodula da su $W \cap U$ i $W + U$ podmoduli od $V$. Dokažimo da je definirano preslikavanje smisleno. Doista, ako su $w_1, w_2 \in W$ takvi da je $w_1 + (W \cap U) = w_2 + (W \cap U)$, onda je $w_1 - w_2 \in (W \cap U) \subseteq U$, pa slijedi da je $w_1 + U = w_2 + U$. Označimo to preslikavanje sa $\varphi$. Dakle, $\varphi$ je preslikavanje sa $W/(W \cap U)$ u $(W + U)/U$ zadano sa

$$\varphi(w + (W \cap U)) = w + U, \qquad w \in W.$$

To je homomorfizam modula jer za $a \in R$ i $w, w_1, w_2 \in W$ imamo

$$\varphi((w_1 + (W \cap U)) + (w_2 + (W \cap U))) = \varphi((w_1 + w_2) + (W \cap U)) = (w_1 + w_2) + U =$$

$$= (w_1 + U) + (w_2 + U) = \varphi(w_1 + (W \cap U)) + \varphi(w_2 + (W \cap U)),$$

$$\varphi(a(w + (W \cap U))) = \varphi(aw + (W \cap U)) = aw + U = a(w + U) = a\varphi(w + (W \cap U)).$$

Dokažimo da je homomorfizam $\varphi$ injektivan. Neka su $w_1, w_2 \in W$ takvi da je $\varphi(w_1 + (W \cap U)) = \varphi(w_2 + (W \cap U))$. To znači da je $w_1 + U = w_2 + U$, tj. $w_1 - w_2 \in U$. No kako su $w_1, w_2 \in W$, vrijedi i $w_1 - w_2 \in W$. Dakle, $w_1 - w_2 \in W \cap U$, pa slijedi $w_1 + (W \cap U) = w_2 + (W \cap U)$. Time je dokazana injektivnost homomorfizma $\varphi : W/(W \cap U) \to (W + U)/U$.

Napokon, dokažimo surjektivnost od $\varphi$. Proizvoljan element od $(W + U)/U$ ima oblik $v + U$, gdje je $v \in W + U$. No tada postoje $w \in W$ i $u \in U$ takvi da je $v = w + u$. Slijedi $v - w = u \in U$, dakle, $v + U = w + U = \varphi(w + (W \cap U))$. Time je dokazana i surjektivnost od $\varphi$.

## 3.2 Integralne domene i polja razlomaka

Neka je $R$ komutativni unitalni prsten. Element $a \neq 0$ prstena $R$ zove se **djelitelj nule** ako postoji $b \in R$, $b \neq 0$, takav da je $ab = 0$. Na primjer, element 2 u prstenu $\mathbb{Z}_6$ je djelitelj nule jer u tom prstenu su $2 \neq 0$ i $3 \neq 0$ ali $2 \cdot 3 = 0$. **Integralna domena** je naziv za komutativni unitalni prsten $R \neq \{0\}$ u kome nema djelitelja nule. Dakle, to je prsten u kome vrijedi $ab = 0$ ako i samo ako je ili $a = 0$ ili $b = 0$. U takvom prstenu možemo *skraćivati*: ako su $a, b, c \in R$, $a \neq 0$ i $ab = ac$, onda je $b = c$. Doista, jednakost $ab = ac$ može se zapisati kao $a(b - c) = 0$, a kako je $a \neq 0$ mora biti $b - c = 0$, odnosno, $b = c$.

Najjednostavniji primjer integralne domene je prsten $\mathbb{Z}$ cijelih brojeva. Naravno, svako polje je integralna domena. Nadalje, ako je $K$ polje, onda je prsten polinoma $K[X]$ u jednoj varijabli s koeficijentima iz $K$ integralna domena. Doista, ako su $P, Q \in K[X]$, $P \neq 0$ i $Q \neq 0$, tada su $\deg P \geq 0$ i $\deg Q \geq 0$, pa je i $\deg PQ = \deg P + \deg Q \geq 0$, dakle, $PQ \neq 0$.

Naravno, ako je $R$ unitalni potprsten integralne domene, onda je i $R$ integralna domena. Posebno, unitalan potprsten svakog polja je integralna domena. U stvari, to je karakterizacija integralnih domena: svaka integralna domena izomorfna je unitalnom potprstenu nekog polja. Glavni cilj ovog odjeljka je da uvidimo kako se na kanonski način svaka integralna domena može uroniti u polje. Prototip za konstrukciju polja koje sadrži zadanu integralnu domenu je konstrukcija polja racionalnih brojeva $\mathbb{Q}$ iz prstena cijelih brojeva $\mathbb{Z}$. Naime, razlomak $\frac{a}{b} \in \mathbb{Q}$, $a, b \in \mathbb{Z}$, $b \neq 0$, možemo shvaćati kao uređen par $(a, b)$, s tim da identificiramo razlomke $\frac{a}{b}$ i $\frac{c}{d}$ ako i samo ako je $ad = bc$.

Neka je sada $R \neq \{0\}$ integralna domena. Jedinicu prstena $R$ kao i obično označavamo sa 1. Formirajmo skup

$$\tilde{K} = R \times (R \setminus \{0\}) = \{(a, b);\ a, b \in R,\ b \neq 0\}.$$

Uvodimo sada relaciju $\sim$ na skupu $\tilde{K}$ na sljedeći način:

$$(a, b) \sim (c, d) \qquad \Longleftrightarrow \qquad ad = bc.$$

Dokažimo da je $\sim$ relacija ekvivalencije. Doista, $(a, b) \sim (a, b)$ za svaki $(a, b) \in \tilde{K}$, jer vrijedi $ab = ba$, tj. relacija $\sim$ je refleksivna. Nadalje, relacija $\sim$ je simetrična jer imamo redom

$$(a, b) \sim (c, d) \qquad \Longrightarrow \qquad ad = bc \qquad \Longrightarrow \qquad cb = da \qquad \Longrightarrow \qquad (c, d) \sim (a, b).$$

Napokon, tranzitivnost relacije $\sim$ dokazuje se korištenjem definicionog svojstva integralne domene:

$$(a, b) \sim (c, d) \quad \text{i} \quad (c, d) \sim (e, f) \qquad \Longrightarrow \qquad ad = bc \quad \text{i} \quad cf = de \qquad \Longrightarrow$$

$$\Longrightarrow \qquad d(af) = f(ad) = f(bc) = b(cf) = b(de) = d(be).$$

Budući da je $d \neq 0$, iz $d(af) = d(be)$ slijedi $af = be$, odnosno, $(a, b) \sim (e, f)$.

Označimo sa $K$ skup svih klasa ekvivalencije u skupu $\tilde{K}$ u odnosu na relaciju $\sim$ . Klasu ekvivalencije para $(a, b) \in \tilde{K}$ označavat ćemo sa $\frac{a}{b}$. Dakle,

$$K = \left\{ \frac{a}{b};\ a, b \in R,\ b \neq 0 \right\},$$

pri čemu je

$$\frac{a}{b} = \{(c, d);\ c, d \in R,\ d \neq 0,\ ad = bc\}.$$

Nadalje, za $\frac{a}{b}, \frac{c}{d} \in K$ vrijedi

$$\frac{a}{b} = \frac{c}{d} \qquad \Longleftrightarrow \qquad ad = bc.$$

Posebno, to znači da se klasa $\frac{a}{b}$ ne mijenja ako i brojnik i nazivnik pomnožimo istim elementom $c \in R$, $c \neq 0$. Doista, imamo

$$a(bc) = (ac)b \qquad \Longrightarrow \qquad \frac{a}{b} = \frac{ac}{bc}.$$

Definirat ćemo sada operacije zbrajanja i množenja u skupu $K$. Prije svega, za $\frac{a}{b}, \frac{c}{d} \in K$ stavljamo

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}.$$

Dokažimo da je definicija smislena, tj. da ne ovisi o predstavnicima dviju klasa $\frac{a}{b}$ i $\frac{c}{d}$. Dakle, treba dokazati implikaciju

$$\frac{a}{b} = \frac{a'}{b'} \quad \text{i} \quad \frac{c}{d} = \frac{c'}{d'} \qquad \Longrightarrow \qquad \frac{ad + cb}{bd} = \frac{a'd' + c'b'}{b'd'}.$$

Doista, jednakosti klasa $\frac{a}{b} = \frac{a'}{b'}$ i $\frac{c}{d} = \frac{c'}{d'}$ znače da je $ab' = a'b$ i $cd' = c'd$. Odatle nalazimo

$$(ad + cb)(b'd') = (ab')(dd') + (cd')(bb') = (a'b)(dd') + (c'd)(bb') = (a'd' + c'b')(bd),$$

a to znači jednakost klasa

$$\frac{ad + cb}{bd} = \frac{a'd' + c'b'}{b'd'}.$$

Dokažimo sada da s tako definiranom operacijom $+$ skup $K$ postaje komutativna grupa. Prije svega, operacija $+$ je komutativna:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd} = \frac{cb + ad}{db} = \frac{c}{d} + \frac{a}{b}.$$

Operacija $+$ je i asocijativna:

$$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad + cb}{bd} + \frac{e}{f} = \frac{(ad + cb)f + e(bd)}{(bd)f} =$$

$$= \frac{a(df) + (cf + ed)b}{b(df)} = \frac{a}{b} + \frac{cf + ed}{df} = \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right).$$

Ulogu neutralnog elementa za operaciju $+$ ima klasa

$$\frac{0}{1} = \{(0, b);\ b \in R,\ b \neq 0\},$$

jer je

$$\frac{a}{b} + \frac{0}{1} = \frac{a1 + 0b}{b1} = \frac{a}{b}.$$

Napokon, za svaki element $\frac{a}{b} \in K$ postoji suprotni element; to je $\frac{-a}{b}$ :

$$\frac{a}{b} + \frac{-a}{b} = \frac{ab - ab}{b^2} = \frac{0}{b^2} = \frac{0}{1}.$$

Time je dokazano da je skup $K$ s operacijom $+$ komutativna grupa.

Definirat ćemo sada operaciju množenja u skupu klasa $K$ ovako:

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

I ta je definicija smislena, tj. ne ovisi o izboru predstavnika dviju klasa iz $K$. Doista, ako je $\frac{a}{b} = \frac{a'}{b'}$ i $\frac{c}{d} = \frac{c'}{d'}$, onda je $ab' = ba'$ i $cd' = dc'$, pa imamo

$$(ac)(b'd') = (ab')(cd') = (ba')(dc') = (bd)(a'c'),$$

a to znači da je $\frac{ac}{bd} = \frac{a'c'}{b'd'}$. Asocijativnost operacije množenja u $K$ slijedi iz asocijativnosti množenja u prstenu $R$ :

$$\left(\frac{a}{b}\frac{c}{d}\right)\frac{e}{f} = \frac{ac}{bd}\frac{e}{f} = \frac{(ac)e}{(bd)f} = \frac{a(ce)}{b(df)} = \frac{a}{b}\frac{ce}{df} = \frac{a}{b}\left(\frac{c}{d}\frac{e}{f}\right).$$

Komutativnost množenja u $K$ slijedi iz komutativnosti množenja u $R$ :

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d}\frac{a}{b}.$$

Dokažimo distributivnost množenja u odnosu na zbrajanje u $K$ :

$$\frac{a}{b}\left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b}\frac{cf + ed}{df} = \frac{a(cf + ed)}{b(df)} = \frac{acf + aed}{bdf}.$$

Kako je $b \neq 0$, množenje brojnika i nazivnika posljednjeg izraza ne mijenja tu klasu, pa je to dalje jednako:

$$\frac{abcf + abed}{b^2df} = \frac{(ac)(bf) + (ae)(bd)}{(bd)(bf)} = \frac{ac}{bd} + \frac{ae}{bf} = \frac{a}{b}\frac{c}{d} + \frac{a}{b}\frac{e}{f}.$$

Komutativna polugrupa $K$ u odnosu na množenje je monoid: svojstvo neutralnog elementa u odnosu na množenje ima klasa

$$\frac{1}{1} = \{(c, c);\ c \in R,\ c \neq 0\},$$

jer očito za svaki $\frac{a}{b} \in K$ vrijedi

$$\frac{a}{b}\frac{1}{1} = \frac{a1}{b1} = \frac{a}{b}.$$

Na taj smo način dokazali da je $K$ komutativan unitalan prsten. Napokon, dokažimo da je $K$ polje, tj. da je svaki njegov element različit od nule invertibilan u odnosu na množenje. Ulogu nule u prstenu $K$ igra klasa

$$\frac{0}{1} = \{(0, c);\ c \in K,\ c \neq 0\}.$$

Neka je $\frac{a}{b} \in K$. Pretpostavka $\frac{a}{b} \neq \frac{0}{1}$ znači da je $a1 \neq 0b$, odnosno, $a \neq 0$. Tada je $\frac{b}{a} \in K$ i to je invers od $\frac{a}{b}$ u odnosu na množenje:

$$\frac{a}{b}\frac{b}{a} = \frac{ab}{ba} = \frac{1}{1} \quad \text{jer je} \quad ab = ba \neq 0.$$

Ovako konstruirano polje $K$ zove se **polje razlomaka** integralne domene $R$. Definiramo sada preslikavanje $\varphi : R \to K$ na sljedeći način:

$$\varphi(a) = \frac{a}{1}, \qquad a \in R.$$

Preslikavanje $\varphi$ je homorfizam prstenova, jer za $a, b \in R$ imamo

$$\varphi(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = \varphi(a) + \varphi(a) \qquad \text{i} \qquad \varphi(ab) = \frac{ab}{1} = \frac{a}{1}\frac{b}{1} = \varphi(a)\varphi(b).$$

Taj je homomorfizam prstenova unitalan, jer je $\varphi(1) = \dfrac{1}{1}$, a to je jedinica u $K$. Napokon, unitalni homomorfizam $\varphi$ je injektivan. Doista, za $a, b \in R$ imamo redom

$$\varphi(a) = \varphi(b) \qquad \Longrightarrow \qquad \frac{a}{1} = \frac{b}{1} \qquad \Longrightarrow \qquad a1 = b1 \qquad \Longrightarrow \qquad a = b.$$

Dakle, $\varphi$ je unitalni izomorfizam prstena $R$ s unitalnim potprstenom

$$\varphi(R) = \{\varphi(a);\ a \in R\} = \left\{\frac{a}{1};\ a \in R\right\}$$

polja $K$. Stoga $\varphi$ možemo upotrijebiti kao identifikaciju: element $a \in R$ identificiramo s klasom $\dfrac{a}{1}$ u $K$ :

$$a = \frac{a}{1}, \qquad a \in R.$$

Ako je $b \in R$, $b \neq 0$, onda u polju $K$ imamo

$$b^{-1} = \left(\frac{b}{1}\right)^{-1} = \frac{1}{b}.$$

Stoga za bilo koji element $\dfrac{a}{b}$ polja $K$ imamo uz identifikaciju $R \subseteq K$ :

$$\frac{a}{b} = \frac{a1}{1b} = \frac{a}{1}\frac{1}{b} = ab^{-1}.$$

Ako se $R$ može pomoću unitalnog monomorfizma smjestiti u bilo koje drugo polje $L$ to se smještenje jedinstveno proširuje do smještenja polja razlomaka od $R$ u polje $L$ :

**Teorem 3.5.** *Neka $R$ integralna domena i $K \supseteq R$ njeno polje razlomaka. Neka je $\psi$ unitalni monomorfizam $R$ u polje $L$. Tada postoji jedinstveni unitalni homomorfizam $\Psi : K \to L$ koji proširuje $\psi$ : $\Psi|R = \psi$. Homomorfizam $\Psi$ je također injektivan.*

**Dokaz:** Definiramo preslikavanje $\Psi : K \to L$ sa

$$\Psi\left(\frac{a}{b}\right) = \psi(a)\psi(b)^{-1}, \qquad \frac{a}{b} \in K.$$

Dokažimo da je definicija preslikavanja $\Psi$ je smislena. Prije svega, ako je $\dfrac{a}{b} \in K$, onda je $b \neq 0$, pa je zbog injektivnosti preslikavanja $\psi$ element $\psi(b)$ polja $L$ različit od nule, dakle, invertibilan; stoga ima smisla pisati $\psi(b)^{-1}$. Za smislenost definicije preslikavanja $\Psi$ treba još provjeriti neovisnost o izboru predstavnika klase $\dfrac{a}{b} \in K$. Doista, ako su $\dfrac{a}{b}, \dfrac{c}{d} \in K$ i $\dfrac{a}{b} = \dfrac{c}{d}$, onda je $ad = bc$, odakle primjenom homomorfizma $\psi$ slijedi $\psi(a)\psi(d) = \psi(b)\psi(c)$. Pomnožimo li obje strane ove jednakosti s inversima $\psi(b)^{-1}$ i $\psi(d)^{-1}$ dobivamo traženu neovisnost o izboru predstavnika klase u $K$ :

$$\psi(a)\psi(b)^{-1} = \psi(c)\psi(d)^{-1}.$$

Preslikavanje $\Psi : K \to L$ je homomorfizam:

$$\Psi\left(\frac{a}{b}+\frac{c}{d}\right)=\Psi\left(\frac{ad+cb}{bd}\right)=\psi(ad+cb)\psi(bd)^{-1}=[\psi(a)\psi(d)+\psi(c)\psi(b)][\psi(b)\psi(d)]^{-1}=$$

$$=\psi(a)\psi(d)\psi(b)^{-1}\psi(d)^{-1}+\psi(c)\psi(b)\psi(b)^{-1}\psi(d)^{-1}=\psi(a)\psi(b)^{-1}+\psi(c)\psi(d)^{-1}=\Psi\left(\frac{a}{b}\right)+\Psi\left(\frac{c}{d}\right);$$

nadalje,

$$\Psi\left(\frac{a}{b}\frac{c}{d}\right)=\Psi\left(\frac{ac}{bd}\right)=\psi(ac)\psi(bd)^{-1}=\psi(a)\psi(c)[\psi(b)\psi(d)]^{-1}=$$

$$=\left[\psi(a)\psi(b)^{-1}\right]\left[\psi(c)\psi(d)^{-1}\right]=\Psi\left(\frac{a}{b}\right)\Psi\left(\frac{c}{d}\right).$$

Homomorfizam $\Psi$ proširuje $\psi$, jer je $\psi(1)=\psi(1)^{-1}$ jedinica u polju $L$, pa za $a\in R$ imamo

$$\Psi(a)=\Psi\left(\frac{a}{1}\right)=\psi(a)\psi(1)^{-1}=\psi(a).$$

Posebno, $\Psi$ je kao i $\psi$ unitalan homomorfizam. Napokon, homomorfizam $\Psi$ je injektivan. Doista, ako je

$$\frac{a}{b}\in K \quad \text{takav da je} \quad \Psi\left(\frac{a}{b}\right)=0,$$

onda je $\psi(a)\psi(b)^{-1}=0$, a odatle množenjem sa $\psi(b)$ slijedi $\psi(a)=0$. No kako je po pretpostavci homomorfizam $\psi$ injektivan, slijedi $a=0$, pa imamo

$$\frac{a}{b}=\frac{0}{b}=\frac{0}{1}=0.$$

Treba još dokazati jedinstvenost proširenja monomorfizma $\psi$. Pretpostavimo da je $\Omega: K\to L$ homomorfizam polja takav da je $\Omega|R=\psi$, donosno, $\Omega(a)=\psi(a)\ \ \forall a\in R$. Tada za proizvoljne $a,b\in R$, $b\neq 0$, imamo

$$\psi(b)\Omega\left(\frac{a}{b}\right)=\Omega(b)\Omega\left(\frac{a}{b}\right)=\Omega\left(b\frac{a}{b}\right)=\Omega(a)=\psi(a),$$

a odatle množenjem sa $\psi(b)^{-1}$ slijedi

$$\Omega\left(\frac{a}{b}\right)=\psi(a)\psi(b)^{-1}=\Psi\left(\frac{a}{b}\right).$$

Ako je $K$ bilo koje polje, prsten polinoma $K[X]$ je integralna domena. Njeno polje razlomaka obično se označava sa $K(X)$ i zove **polje racionalnih funkcija** u jednoj varijabli s koeficijentima iz polja $K$. Elementi su razlomci oblika

$$\frac{P}{Q},\qquad P,Q\in K[X],\quad Q\neq 0.$$

Nadalje, za $P,Q,R,S\in K[X]$, $Q\neq 0$, $S\neq 0$, vrijedi

$$\frac{P}{Q}=\frac{R}{S}\qquad \text{ako i samo ako je}\qquad PS=RQ.$$

Racionalna funkcija $\dfrac{P}{Q}$ definira funkciju na skupu $K\setminus N$, gdje je $N=\{\lambda\in K;\ Q(\lambda)=0\}$ skup nultočaka polinoma $Q$ u polju $K$ :

$$\frac{P}{Q}(\lambda)=\frac{P(\lambda)}{Q(\lambda)},\qquad \lambda\in K,\quad Q(\lambda)\neq 0.$$

Najveće područje definicije dobivamo ako skratimo razlomak $\dfrac{P}{Q}$ koliko god možemo, odnosno, podijelimo brojnik i nazivnik s njihovom najvećom zajedničkom mjerom, tako da dobijemo razlomak u kome su brojnik i nazivnik relativno prosti. U tom slučaju brojnik i nazivnik nemaju zajedničkih nultočaka.

## 3.3 Prosti i maksimalni ideali

U ovom odjeljku $R$ će označavati komutativan unitalan prsten različit od $\{0\}$. Definirat ćemo pojmove *prost ideal* i *maksimalan ideal* i istražiti veze između ta dva pojma.

Ideal $I$ u prstenu $R$ zove se **prost** ako je $I \neq R$ i ako iz $ab \in I$ slijedi da je ili $a \in I$ ili $b \in I$.

**Propozicija 3.1.** *Ideal $I$ u prstenu $R$ je prost ako i samo ako je kvocijentni prsten $R/I$ integralna domena.*

**Dokaz:** Pretpostavimo da je $I$ ideal različit od $R$ koji nije prost. Tada postoje $a, b \in R \setminus I$ takvi da je $ab \in I$. Tada su elementi $a + I$ i $b + I$ kvocijentnog prstena $R/I$ različiti od nule, a njihov produkt $ab + I$ je nula u prstenu $R/I$ jer je $ab \in I$. Dakle, $R/I$ nije integralna domena.

Pretpostavimo sada da je $I \neq R$ i da $R/I$ nije integralna domena. Tada postoje elementi $a+I$ i $b+I$ kvocijentnog prstena različiti od nule, dakle, $a \notin I$ i $b \notin I$, takvi da je njihov produkt $ab+I$ nula u prstenu $R/I$, dakle, $ab \in I$. To pokazuje da ideal $I$ nije prost.

Ideal $I \neq R$ se zove **maksimalan** ako u $R$ ne postoji ideal $J$ takav da je $I \subsetneq J \subsetneq R$. Primijetimo da za ideal $I$ u $R$ vrijedi $I \neq R$ ako i samo ako $1 \notin I$. Doista, ako je $1 \in I$, onda za svaki $a \in R$ vrijedi $a = a1 \in I$, dakle je $I = R$.

**Propozicija 3.2.** *Neka je $I \neq R$ ideal. Tada postoji maksimalan ideal u $R$ koji sadrži $I$.*

Da bismo ovu propoziciju dokazali, potrebna nam je tzv. *Zornova lema* iz teorije skupova, koju ćemo sada izreći. U tu svrhu trebamo definirati još neke pojmove. **Parcijalno uređen skup** je neprazan skup $\mathcal{S}$ na kome je zadana relacija uređaja, tj. relacija $\leq$ sa sljedeća dva svojstva:

(*a*) *Antisimetričnost*: Ako su $x, y \in \mathcal{S}$, onda vrijedi $x \leq y$ i $y \leq x$ ako i samo ako je $x = y$.

(*b*) *Tranzitivnost*: Ako su $x, y, z \in \mathcal{S}$ takvi da je $x \leq y$ i $y \leq z$, onda je $x \leq z$.

Podskup $\mathcal{T}$ parcijalno uređenog skupa $\mathcal{S}$ zove se **lanac** ako za bilo koje $x, y \in \mathcal{T}$ vrijedi ili $x \leq y$ ili $y \leq x$. Za podskup $\mathcal{T}$ parcijalno uređenog skupa $\mathcal{S}$ kažemo da je **odozgo omeđen** (u $\mathcal{S}$) ako postoji $x \in \mathcal{S}$ takav da je $y \leq x \ \forall y \in \mathcal{T}$. Napokon, za element $x$ parcijalno uređenog skupa $\mathcal{S}$ kažemo da je **maksimalan** (u $\mathcal{S}$) ako ne postoji $y \in \mathcal{S}$ takav da je $x \leq y$ i $x \neq y$.

**Teorem 3.6.** (**Zornova lema**) *Neka je $\mathcal{S}$ parcijalno uređen skup u kome je svaki lanac odozgo omeđen. Tada u $\mathcal{S}$ postoji barem jedan maksimalan element.*

**Dokaz propozicije 3.2.** Neka je $\mathcal{S}$ skup svih ideala $J \neq R$ koji sadrže ideal $I$. To je neprazan skup jer je $I \in \mathcal{S}$. U skup $\mathcal{S}$ uvodimo relaciju uređaja pomoću inkluzije. Naravno, maksimalni ideal koji sadrži $I$ je upravo maksimalni element parcijalno uređenog skupa $\mathcal{S}$. Da bismo dokazali da takav postoji, prema Zornovoj lemi dovoljno je provjeriti da je zadovoljen uvjet Zornove leme, tj. da je svaki lanac u $\mathcal{S}$ odozgo omeđen. Neka je, dakle, $\mathcal{T}$ lanac u $\mathcal{S}$. To znači da je $\mathcal{T}$ skup ideala $J \neq R$ koji sadrže $I$ takav da za $J, K \in \mathcal{T}$ vrijedi ili $J \subseteq K$ ili $K \subseteq J$. Stavimo tada

$$L = \bigcup_{J \in \mathcal{T}} J.$$

Dokažimo da je $L$ ideal u $R$. Doista, ako su $a, b \in L$, onda postoje $J, K \in \mathcal{T}$ takvi da je $a \in J$ i $b \in K$. Kako je $\mathcal{T}$ lanac, vrijedi ili $J \subseteq K$ ili $K \subseteq J$. Pretpostavimo npr. da je $K \subseteq J$. Tada su $a, b \in J$, a kako je $J$ ideal, to je i $a - b \in J$, dakle i $a - b \in L$. Time je dokazano da je $L$ aditivna podgrupa od $R$. Nadalje, ako je $a \in R$ i $b \in L$, tada je $b \in J$ za neki $J \in \mathcal{T}$, pa je i $ab \in J$, dakle i $ab \in L$. Time je dokazano da je $L$ ideal u $R$. Kako je $J \neq R \ \forall J \in \mathcal{T}$, to je $1 \notin J \ \forall J \in \mathcal{T}$. No tada slijedi $1 \notin L$, dakle, $L \neq R$. Jasno je da $L$ sadrži ideal $I$. Prema tome je $L \in \mathcal{S}$. Napokon, očito vrijedi $J \subseteq L \ \forall J \in \mathcal{T}$ i time je dokazano da je lanac $\mathcal{T}$ odozgo omeđen. Kako je $\mathcal{T}$ bio proizvoljan lanac u $\mathcal{S}$ zadovoljen je uvjet Zornove leme.

**Propozicija 3.3.** *$R$ je polje ako i samo ako je $\{0\}$ jedini ideal u $R$ različit od $R$.*

**Dokaz:** Neka je $R$ polje i neka je $I \neq \{0\}$ ideal u $R$. Izaberimo $a \in I$, $a \neq 0$. Tada je $a$ invertibilan, pa slijedi $1 = a^{-1}a \in I$, a odatle je $I = R$.

Obratno, pretpostavimo da su $\{0\}$ i $R$ jedini ideali u $R$. Neka je $a \in R$, $a \neq 0$. Neka je

$$I = Ra = \{ba;\ b \in R\}.$$

Tada je $I$ ideal u $R$. Doista, ako su $x, y \in I$, onda je $x = ba$ i $y = ca$ za neke $b, c \in R$, pa slijedi $x - y = ba - ca = (b - c)a \in I$, što pokazuje da je $I$ aditivna podgrupa od $R$. Nadalje, za $x \in I$ i $y \in R$ je $x = ba$ za neki $b \in R$, pa je $yx = (yb)a \in I$. Ideal $I$ je različit od $\{0\}$, jer je $0 \neq a = 1a \in I$. Po pretpostavci je tada $I = R$. No to znači da je $1 \in I$, dakle, postoji $b \in R$ takav da je $ba = 1$. Time je dokazano da je element $a$ invertibilan u $R$, a kako je $a$ bio proizvoljan element iz $R \setminus \{0\}$, zaključujemo da je $R$ polje.

**Propozicija 3.4.** *Ideal $I$ u $R$ je maksimalan ako i samo ako je kvocijentni prsten $R/I$ polje.*

**Dokaz:** Prstene $R$ i $R/I$ možemo promatrati kao module nad prstenom $R$. Tada su ideali u $R$ upravo podmoduli $R-$modula $R$, a također ideali u prstenu $R/I$ su podmoduli $R-$modula $R/I$. Kvocijentno preslikavanje $\pi : R \to R/I$, definirano sa $\pi(a) = a + I$, $a \in R$, je homomorfizam $R-$modula. Doista, za $a, b \in R$ je

$$\pi(a + b) = (a + b) + I = (a + I) + (b + I) = \pi(a) + \pi(b).$$

Također,

$$a\pi(b) = a(b + I) = ab + I = \pi(ab).$$

Prema prvom teoremu o izomorfizmu (teorem 3.3.) $J \mapsto \pi(J)$ je bijekcija sa skupa svih podmodula $J$ od $R$ koji sadrže $I$ na skup svih podmodula od $R/I$. Drugim riječima, $J \mapsto \pi(J)$ je bijekcija sa skupa svih ideala u $R$ koji sadrže $I$ na skup svih ideala u prstenu $R/I$. Prema propoziciji 3.3. prsten $R/I$ je polje ako i samo ako je $R/I$ jedini ideal različit od nule. No to znači da je $R$ jedini ideal u $R$ koji sadrži $I$ i koji je različit od $I$, odnosno, to znači da je ideal $I$ u prstenu $R$ maksimalan.

**Korolar 3.1.** *Svaki maksimalan ideal u $R$ je prost.*

**Dokaz:** Ako je $I$ maksimalan ideal u $R$ prema propoziciji 3.4. kvocijentni prsten $R/I$ je polje. No polje je i integralna domena, pa iz propozicije 3.1. slijedi da je ideal $I$ prost.

Obrat ne vrijedi. U prstenu $R$ ne mora svaki prost ideal biti maksimalan. Da to uvidimo, razmotrimo sljedeći primjer. Neka je $R = \mathbb{Z}[X]$ prsten polinoma jedne varijable s cjelobrojnim koeficijentima. Promatrajmo ideal

$$I = X\mathbb{Z}[X] = \{XQ;\ Q \in \mathbb{Z}[X]\} = \{P \in \mathbb{Z}[X];\ P(0) = 0\}.$$

Ideal $I$ je prost. Doista, ako su $A, B \in \mathbb{Z}[X]$ takvi da je $AB \in I$, tada je $0 = (AB)(0) = A(0)B(0)$, dakle, ili je $A(0) = 0$ ili je $B(0) = 0$. No to znači da je ili $A \in I$ ili $B \in I$. Međutim, ideal $I$ nije maksimalan u prstenu $\mathbb{Z}[X]$. Doista, neka je

$$J = \{P \in \mathbb{Z}[X];\ 2|P(0)\}.$$

Tada je $J$ ideal u $\mathbb{Z}[X]$, i očito je $I \subsetneq J \subsetneq \mathbb{Z}[X]$.

U jednoj klasi prstenova svaki je prost ideal različit od $\{0\}$ maksimalan. To su integralne domene koje su ujedno tzv. *prsteni glavnih ideala*. U prstenu $R$ **glavni ideal** je svaki ideal oblika

$$Ra = \{ba;\ b \in R\}$$

za neki $a \in R$. Za $R$ kažemo da je **prsten glavnih ideala** ako je svaki ideal u $R$ glavni ideal. Integralna domena koja je prsten glavnih ideala zove se domena glavnih ideala.

**Propozicija 3.5.** *Neka je $R$ domena glavnih ideala. Tada je svaki prost ideal $I \neq \{0\}$ u $R$ maksimalan ideal u $R$.*

**Dokaz:** Neka je $I \neq \{0\}$ prost ideal u $R$. Kako je $R$ prsten glavnih ideala, postoji $a \in I$ takav da je $I = Ra$. Budući da je $I \neq \{0\}$, to je $a \neq 0$. Nadalje, $I \neq R$, pa element $a$ nije invertibilan u $R$ : inače bi bilo $1 = a^{-1}a \in I$, dakle, $I = R$. Neka je sada $J$ ideal u $R$ koji sadrži $I$. Tada je $J = Rb$ za neki $b \in J$. Imamo

$$I \subseteq J \quad \Longrightarrow \quad Ra \subseteq Rb \quad \Longrightarrow \quad a \in Rb \quad \Longrightarrow \quad a = cb \quad \text{za neki} \quad c \in R.$$

Kako je $I$ prost ideal i $a \in I$, nužno je ili $b \in I$ ili $c \in I$. Ako je $b \in I$, onda je $J = Rb \subseteq I$, dakle, $J = I$. Pretpostavimo da je $J \neq I$. Tada je $c \in I$, dakle, $c = da$ za neki $d \in R$. No tada je $a = cb = dab = abd$. Budući da je $R$ integralna domena, u jednakostima je dozvoljeno "*kraćenje*" elementima različitim od nule, pa slijedi $1 = bd \in J$, dakle, $J = R$.

Ova propozicija pokazuje da prsten $\mathbb{Z}[X]$ iz prethodnog primjera, koji očigledno jest integralna domena, nije prsten glavnih ideala. U stvari, lako se vidi da promatrani ideal

$$J = \{P \in \mathbb{Z}[X];\ 2|P(0)\}$$

nije glavni ideal.

**Propozicija 3.6.** *Prsteni $\mathbb{Z}$ i $K[X]$, gdje je $K$ polje, su domene glavnih ideala.*

**Dokaz:** Prema lemi 2.2. čak je svaka podgrupa aditivne grupe $\mathbb{Z}$ oblika $m\mathbb{Z}$ za neki $m \in \mathbb{Z}$. Prema tome, svaki je ideal u $\mathbb{Z}$ glavni ideal.

Ako je $I \neq \{0\}$ ideal u $K[X]$. Neka je $P$ među svim polinomima u $I$ različitim od 0 najmanjeg stupnja. Dakle,

$$Q \in I, \quad Q \neq 0 \quad \Longrightarrow \quad \deg P \leq \deg Q.$$

Tada je naravno $K[X]P \subseteq I$. Neka je $Q \in I$. Prema propoziciji 1.12. postoje $A, B \in K[X]$ takvi da je $Q = AP + B$ i $\deg B < \deg P$. Tada je $B = Q - AP \in I$, pa prema izboru polinoma $P$ slijedi $B = 0$. Dakle, $Q = AP \in K[X]P$. Time je dokazana i obrnuta inkluzija $I \subseteq K[X]P$, odnosno, imamo jednakost $I = K[X]P$.

## 3.4 Faktorijalni prsteni

Vidjeli smo da se svaki cijeli broj $m \in \mathbb{Z}$ različit od 0 i $\pm 1$ može faktorizirati u $\pm$ produkt prostih brojeva i taj je zapis jedinstven do na poredak. Slično vrijedi i u prstenu polinoma $K[X]$ s koeficijentima iz polja $K$ : svaki neinvertibilan polinom različit od 0 može napisati kao produkt ireducibilnih polinoma i ako se ograničimo na normirane polinome (što postižemo izlučivanjem faktora $\alpha \in K \setminus \{0\}$) faktorizacija je ponovo jedinstvena do na poredak. U ovom ćemo odjeljku detaljnije istražiti svojstvo takve jedinstvene faktorizacije. Budući da su pri faktorizaciji djelitelji nule velika smetnja, ograničit ćemo se na promatranje integralnih domena.

Prije svega, na jednom ćemo primjeru vidjeti da jedinstvena faktorizacija nije istinita u svakoj integralnoj domeni. Promatrat ćemo sljedeći potprsten polja kompleksnih brojeva:

$$R = \{a + bi\sqrt{5};\ a, b \in \mathbb{Z}\}.$$

$R$ je najmanji unitalni potprsten od $\mathbb{C}$ koji sadrži broj $i\sqrt{5}$. Za $\alpha \in R$ označimo sa $N(\alpha)$ kvadrat njegove apsolutne vrijednosti. Dakle,

$$N\left(a + bi\sqrt{5}\right) = a^2 + 5b^2.$$

Naravno, za svaki $\alpha \in R$ različit od nule je $N(\alpha)$ prirodan broj. Nadalje, iz svojstava apsolutne vrijednosti kompleksnih brojeva slijedi da je

$$N(\alpha\beta) = N(\alpha)N(\beta), \qquad \forall \alpha, \beta \in R. \tag{3.1}$$

Odredimo sada grupu $R^*$ svih invertibilnih elemenata u prstenu $R$. Ako je $\alpha \in R$, onda je $\alpha\alpha^{-1} = 1$, pa slijedi $N(\alpha)N(\alpha^{-1}) = N(1) = 1$. To pokazuje da je $N(\alpha) = 1$ za svaki $\alpha \in R^*$. Pišemo li $\alpha = a + bi\sqrt{5}$ slijedi da mora biti $a^2 + 5b^2 = 1$, a to je moguće samo ako je $b = 0$ i $a = \pm 1$. Na taj način dokazali smo da je $R^* = \{1, -1\}$.

Produktna formula (3.1) pokazuje da ukoliko pokušavamo neki element prstena $R$ rastavljati u produkt, taj pokušaj faktorizacije će nakon konačno mnogo koraka završiti. Dakle, moguća je faktorizacija u produkt nekakvih "*elementarnih*" elemenata, koje bismo mogli zvati ireducibilnima − to su oni koji nisu invertibilni i koji se ne mogu pisati kao umnožak dvaju neinvertibilnih. Uočimo sada jednakost u prstenu $R$ :

$$6 = \left(1 + i\sqrt{5}\right)\left(1 - \sqrt{5}\right) = 2 \cdot 3. \tag{3.2}$$

Imamo

$$N\left(1 + i\sqrt{5}\right) = N\left(1 - i\sqrt{5}\right) = 6, \qquad N(2) = 4, \qquad N(3) = 9.$$

Budući da je $N\left(a + bi\sqrt{5}\right) = a^2 + 5b^2$, vidimo da je $N(\alpha) \neq 2$ i $N(\alpha) \neq 3$ za svaki $\alpha \in R$. To nam pokazuje da elementi $1 + i\sqrt{5}$, $1 - i\sqrt{5}$, 2 i 3 prstena $R$ nemaju netrivijalne faktorizacije, odnosno, da su u gornjem smislu ireducibilni. Taj primjer pokazuje da iako u prstenu $R$ možemo govoriti o faktorizaciji ta faktorizacija nije jedinstvena.

U prstenima $\mathbb{Z}$ i $K[X]$ pojmovi prostog elementa i ireducibilnog elementa se podudaraju, ali općenito nije tako. Prijeđimo na formalne defincije u proizvoljnoj integralnoj domeni $R$. Ako su $a, b \in R$ i $a \neq 0$, kažemo da $a$ **dijeli** $b$ ako postoji $c \in R$ takav da je $b = ac$. Kažemo još da je $a$ **djelitelj**, **divizor** ili **faktor** od $b$. Tu činjenicu bilježimo kao i kod brojeva i polinoma s uspravnom crtom: $a|b$. Element $r \in R$ se zove **ireducibilan** ako je $r$ neinvertibilan element različit od 0 koji

se ne može napisati kao produkt dvaju neinvertibilnih elemenata. Neinvertibilni elementi različiti od 0 koji nisu ireducibilni zovu se **reducibilni**. Za neinvertibilan element $p \in R$ različit od 0 kažemo da je **prost** ako ima sljedeće svojstvo:

$$a, b \in R, \quad p|(ab) \qquad \Longrightarrow \qquad p|a \quad \text{ili} \quad p|b.$$

**Propozicija 3.7.** *Svaki je prost element ireducibilan.*

**Dokaz:** Pretpostavimo suprotno, tj. da postoji prost element $p$ koji je reducibilan. Tada ga možemo zapisati u obliku $p = ab$, gdje su $a, b \in R$ neinvertibilni. No tada očito $p|p$, dakle $p|(ab)$, pa slijedi da ili $p|a$ ili $p|b$. Uzmimo jedno od toga, npr. $p|a$. Tada je $a = pc$ za neki $c \in R$, pa slijedi $p = ab = pcb$, a odatle je $cb = 1$ suprotno pretpostavci da je $b$ neinvertibilan. Ova kontradikcija dokazuje tvrdnju.

Obratno, ireducibilan element ne mora biti prost. Npr. u prethodnom primjeru element $1+i\sqrt{5}$ je ireducibilan. On dijeli $6 = 2 \cdot 3$, ali očito ne dijeli ni 2 ni 3, dakle, $1 + i\sqrt{5}$ nije prost.

Integralna domena $R$ zove se **faktorijalan prsten** (ili **domena jedinstvene faktorizacije**, engl. terminologija je *unique factorization domain*) ako ima sljedeća dva svojstva:

(1) svaki neinvertibilan element različit od 0 je ili ireducibilan ili je produkt konačno mnogo ireducibilnih elemenata;

(2) faktorizacija iz (1) jedinstvena je do na poredak i do na množenje pojedinih faktora invertibilnim elementima.

Uočava se da je svojstvo (2) (jedinstvenost faktorizacije) iskazano u određenoj mjeri nespretnije nego što je to bio slučaj u prstenima $\mathbb{Z}$ i $K[X]$. Tamo smo stvarno imali jedinstvenost do na poredak. Razlog je u tome što se mogli ograničiti u slučaju prstena $\mathbb{Z}$ na prirodne brojeve, a u slučaju prstena $K[X]$ na normirane polinome. U općim integralnim prstenima takav izbor predstavnika nije tako jednostavan. Ipak, moguće je postići određeniji iskaz jedinstvenosti.

Postupamo na sljedeći način. Neka je $R$ integralna domena i $R^*$ njena multiplikativna grupa invertibilnih elemenata. Grupa $R^*$ djeluje na $R$ pomoću množenja. To djelovanje definira na $R$ relaciju ekvivalencije koja se zove *asociranost*. Konkretno, kažemo da su elementi $a$ i $b$ iz $R$ **asocirani** ako postoji $\alpha \in R^*$ takav da je $a = \alpha b$. Naravno, $\{0\}$ je jedna od klasa ekvivalencije u odnosu na tu relaciju, odnosno, jedna klasa asociranosti. Također, čitava grupa $R^*$ je jedna klasa asociranosti. Ono što nas zanima u problemima faktorizacije je ostatak prstena $R$, odnosno skup $R \setminus (R^* \cup \{0\})$ svih neinvertibilnih elemenata različitih od nule. Taj je skup disjunktna unija klasa asociranosti. Ako iz svake takve klase izaberemo po jednog predstavnika dobivamo skup koji ćemo označiti sa $R'$ i koji može igrati sličnu ulogu kao i $\mathbb{N} \setminus \{1\}$ u slučaju $\mathbb{Z}$, odnosno, kao skup normiranih nekonstantnih polinoma u slučaju prstena $K[X]$. Nadalje, neka je $R'_i$ skup svih ireducibilnih elemenata u $R'$. Svaki ireducibilan element tada je asociran jedinstvenom elementu iz $R'_i$. Svojstva faktorijalnog prstena mogu se sada određenije iskazati:

(1) za svaki neinvertibilan element $a \neq 0$ postoje $\alpha \in R^*$, $n \in \mathbb{N}$ i $p_1, \ldots, p_n \in R'_i$ takvi da je

$$a = \alpha p_1 \cdots p_n.$$

(2) ako su $\alpha, \beta \in R^*$, $n, m \in \mathbb{N}$ i $p_1, \ldots, p_n, q_1, \ldots, q_m \in R'_i$ takvi da je

$$\alpha p_1 \cdots p_n = \beta q_1 \cdots q_m$$

Tada je $\alpha = \beta$ i $n = m$ i postoji permutacija $\sigma \in S_m$ takva da je

$$q_j = p_{\sigma(j)} \qquad \text{za} \quad j = 1, \ldots, m.$$

Sljedeća propozicija pokazuje važnost razlikovanja pojmova *prost* i *ireducibilan*:

**Propozicija 3.8.** *Neka je $R$ integralna domena sa svojstvom* (1). *Tada $R$ ima i svojstvo* (2) *ako i samo ako je svaki ireducibilan element u $R$ prost.*

**Dokaz:** Pretpostavimo da (2) vrijedi i neka je $p$ ireducibilan element koji dijeli umnožak $ab$. Možemo pretpostaviti da je $ab \neq 0$. Neka su $q \in R_i'$ i $\varepsilon \in R^*$ takvi da je $p = \varepsilon q$. Tada i $q$ dijeli umnožak $ab$. Dakle, $ab = qc$ za neki $c$. Neka su

$$a = \alpha p_1 \cdots p_n, \qquad b = \beta q_1 \cdots q_m, \qquad c = \gamma r_1 \cdots r_k$$

faktorizacije u skladu sa (1), odnosno, $\alpha, \beta, \gamma \in R^*$ i $p_1, \ldots, p_n, q_1, \ldots, q_m, r_1, \ldots, r_k$. Slijedi

$$\alpha\beta p_1 \cdots p_n q_1 \cdots q_m = \gamma q r_1 \cdots r_k.$$

Prema (2) jedan od faktora $p_1, \ldots, p_n, q_1, \ldots, q_m$ s lijeve strane jednak je $q$. Dakle, ili je $q = p_i$ za neki $i$ i tada $q|a$, ili je $q = q_j$ za neki $j$ i tada $q|b$. Kako je $q = \varepsilon^{-1}p$, slijedi da ili $p|a$ ili $p|b$. Time je dokazano da je element $p$ prost.

Pretpostavimo sada da je svaki ireducibilan element od $R$ prost. Sada se sasvim analogno dokazima teorema 1.1. i 1.6. dokazuje da vrijedi (2). Provedimo taj dokaz detaljno. Pretpostavimo, dakle, da je

$$\alpha p_1 \cdots p_n = \beta q_1 \cdots q_m, \qquad \alpha, \beta \in R^*, \quad n, m \in \mathbb{N}, \quad p_1, \ldots, p_n, q_1, \ldots, q_m \in R_i'. \tag{3.3}$$

Možemo pretpostaviti da je $m \leq n$. Dokaz provodimo indukcijom u odnosu na $m$.

Baza indukcije: $m = 1$. Pretpostavljamo da je $\beta q_1 = \alpha p_1 \cdots p_n$, $\alpha, \beta \in R^*$, $q_1, p_1, \ldots, p_n \in R_i'$. Zbog ireducibilnosti od $q_1$ slijedi $n = 1$ i $q_1 = \beta^{-1}\alpha p_1$. Dakle, $q_1$ i $p_1$ su asocirani. No kako su $p_1, q_1 \in R_i'$, a $R_i'$ je formiran od po točno jednog predstavnika svake klase asociranosti u skupu $R \setminus (R^* \cup \{0\})$, zaključujemo da je $q_1 = p_1$. Tada je $\beta^{-1}\alpha = 1$, tj. $\alpha = \beta$. Time je proveden dokaz baze indukcije.

Korak indukcije: $m \geq 2$ i pretpostavljamo da je tvrdnja dokazana za manje od $m$ faktora. Iz (3.3) slijedi da $q_m$ dijeli umnožak $p_1 \cdots p_n$. $q_m$ je ireducibilan, pa je po pretpostavci prost. Stoga $q_m$ dijeli jedan od faktora, npr. $p_k$. No kako je i $p_k$ ireducibilan, slijedi da su $q_m$ i $p_k$ asocirani, a budući da su oba iz skupa $R_i'$, u kome se iz svake klase asociranosti nalazi točno jedan element, zaključujemo da je $q_m = p_k$. No tada dvije strane jednakosti (3.3) možemo skratiti sa $p_k$, pa dobivamo:

$$\alpha p_1 \cdots p_{k-1} p_{k+1} \cdots p_n = \beta q_1 \cdots q_{m-1}.$$

Po pretpostavci indukcije slijedi da je $m - 1 = n - 1$, dakle, $m = n$, da je $\alpha = \beta$ i da postoji bijekcija

$$\sigma : \{1, \ldots, m-1\} \to \{1, \ldots, k-1, k+1, \ldots, m\}$$

takva da je

$$q_j = p_{\sigma(j)} \qquad \text{za} \quad j = 1, \ldots, m-1.$$

Stavimo li još $\sigma(m) = k$, dobivamo da je $\sigma \in S_m$ i da vrijedi

$$q_j = p_{\sigma(j)} \qquad \text{za} \quad j = 1, \ldots, m.$$

Time je i korak indukcije proveden.

**Propozicija 3.9.** *Neka je $R$ integralna domena i $p \in R$, $p \neq 0$. Tada je element $p$ prost ako i samo ako je glavni ideal $Rp$ prost.*

**Dokaz:** Pretpostavimo da je element $p$ prost. Tada je $Rp \neq R$, jer $p$ nije invertibilan. Pretpostavimo da su $a, b \in R$ i $ab \in Rp$. Tada je $ab = rp$ za neki $r \in R$, pa slijedi da $p|ab$. No tada $p|a$ ili $p|b$. U prvom slučaju je $a \in Rp$, u drugom je $b \in Rp$. Dakle, ideal $Rp$ je prost.

Pretpostavimo sada da je ideal $Rp$ prost i da je $p \neq 0$. Budući da je $Rp \neq R$, element $p$ nije invertibilan. Pretpostavimo da $p|ab$. Tada je $ab = cp$ za neki $p$, dakle, $ab \in Rp$. Budući da je ideal $Rp$ prost, slijedi da je ili $a \in Rp$ ili $b \in Rp$. U prvom slučaju $p|a$ a u drugom $p|b$. Dakle, element $p$ je prost.

**Teorem 3.7.** *Neka je $R$ domena glavnih ideala. Tada je $R$ faktorijalan prsten.*

**Dokaz:** Neka je $a_1 \in R \setminus (R^* \cup \{0\})$. Ako $a_1$ nije ireducibilan, tada je $a_1 = a_2 b_2$, pri čemu $a_2$ i $b_2$ nisu invertibilan. Ako $a_2$ i $b_2$ nisu oba ireducibilni, možemo pretpostaviti da $a_2$ nije ireducibilan. Tada je $a_2 = a_3 b_3$, pri čemu $a_3$ i $b_3$ nisu invertibilni. Nastavimo na taj način dok god možemo. Trebamo dokazati da se taj proces ne može nastavljati u nedogled, nego ćemo nakon konačno koraka doći do faktorizacije elementa $a_1$ u produkt ireducibilnih elemenata. Pretpostavimo suprotno. Jednakost $a_1 = a_2 b_2$, pri čemu $b_2$ nije invertibilan, znači da je $a_1 \in Ra_2$, ali $a_2 \notin Ra_1$, odnosno, da je $Ra_1 \subsetneq Ra_2$. Sada iz $a_2 = a_3 b_3$ slijedi $Ra_2 \subsetneq Ra_3$. Dakle, dobivamo beskonačan striktno rastući niz glavnih ideala

$$Ra_1 \subsetneq Ra_2 \subsetneq Ra_3 \subsetneq \cdots\cdots \subsetneq Ra_n \subsetneq Ra_{n+1} \subsetneq \cdots\cdots$$

Stavimo

$$I = \bigcup_{n=1}^{\infty} Ra_i.$$

Tada je $I$ ideal u $R$. Budući da je $R$ prsten glavnih ideala, vrijedi $I = Ra$ za neki $a \in R$. Tada je $a \in I$, dakle, $a \in Ra_k$ za neki $k \in \mathbb{N}$. No to znači da je i $Ra_k \subseteq Ra$ i $Ra \subseteq Ra_k$, dakle, $Ra_k = Ra$. No odatle slijedi da je $Ra_m = Ra \ \ \forall m \geq k$ suprotno pretpostavci. Ova kontradikcija pokazuje da je nemoguće nastavljati opisani proces u nedogled, nego nakon konačno mnogo koraka dolazimo do prikaza elementa $a_1$ kao produkta ireducibilnih elemenata. Time je dokazano da prsten $r$ ima svojstvo (1).

Prema propoziciji 3.8. teorem će biti dokazan, ako pokažemo da je svaki ireducibilan element u $R$ prost. Neka je $p$ ireducibilan element od $R$. Tada $p$ nije invertibilan, pa je $Rp \neq R$. Pretpostavimo da je $I \supsetneq Rp$ ideal. Budući da je $R$ prsten glavnih ideala, vrijedi $I = Rc$ za neki $c \in R$. Tada je $p = rc$ za neki $r \in R$. Kako je $I \neq Rp$, $r$ ne može biti invertibilan. Sada ireducibilnost elementa $p$ povlači da je $c$ invertibilan. No tada je $I = R$. Na taj način dokazali smo da je ideal $Rp$ maksimalan. Prema korolaru 3.1. ideal $Rp$ je prost, a prema propoziciji 3.9. element $p$ je prost.

Time je teorem u potpunosti dokazan.

## 3.5 Gaussova lema

Vidjeli smo da je svaka domena glavnih ideala faktorijalan prsten. Posebno, za svako polje $K$ prsten polinoma $K[X]$ je faktorijalan prsten. Cilj je ovog odjeljka da dokažemo znatno više, naime, da je za svaki faktorijalan prsten $R$ prsten polinoma $R[X]$ s koeficijentima iz $R$ također faktorijalan prsten. Glavni prototip je $\mathbb{Z}[X]$; to jest faktorijalan prsten iako nije prsten glavnih ideala kao što smo vidjeli. Drugi primjer, vrlo važan u algebarskoj geometriji je prsten polinoma $K[X_1, X_2, \ldots, X_n]$ u više varijabli. Naime, na taj će slučaj biti induktivno primjenjiv najavljeni rezultat zbog izomorfizma $K[X_1, \ldots, X_n] \simeq K[X_1, \ldots, X_{n-1}][X_n]$.

Da bismo dokazali da je $R[X]$ faktorijalan prsten za svaki faktorijalan prsten $R$, ključna je tzv. *Gaussova lema*, a ta će lema imati i druge važne posljedice. Ta lema uspoređuje pojam ireducibilnosti u prstenima $R[X]$ i $K[X]$, gdje je $R$ faktorijalan prsten, a $K$ je polje razlomaka prstena $R$.

Prijeđimo na potrebne definicije. Neka je $R$ faktorijalan prsten shvaćen kao potprsten njegovog polja razlomaka $K$. Za $a, b \in R$ koji nisu oba jednaki 0 definira se **najveća zajednička mjera** od $a$ i $b$ kao bilo koji element $c \in R$ koji dijeli i $a$ i $b$ i za koji vrijedi:

$$d \in R, \quad d|a \quad \text{i} \quad d|b \qquad \Longrightarrow \qquad d|c.$$

Ako su i $a \neq 0$ i $b \neq 0$ i ako su

$$a = \alpha p_1^{i_1} \cdots p_n^{i_n} \qquad \text{i} \qquad b = \beta p_1^{j_1} \cdots p_n^{j_n}$$

njihove faktorizacije, pri čemu su $\alpha$ i $\beta$ invertibilni i $p_1, \ldots, p_n$ su ireducibilni elementi od $R$, i $i_1, \ldots, i_n, j_1, \ldots, j_n \in \mathbb{Z}_+$, onda se lako vidi da je umnožak $p_1^{k_1} \cdots p_n^{k_n}$, gdje je $k_\ell = \min\{i_\ell, j_\ell\}$, $1 \leq \ell \leq n$, jedna najveća zajednička mjera elemenata $a$ i $b$. Nadalje, ako je $c$ bilo koja najveća zajednička mjera elemenata $a$ i $b$ onda je $\{\gamma c;\ \gamma \in R^*\}$ skup svih najvećih zajedničkih mjera od $a$ i $b$.

Definicija najveće zajedničke mjere neposredno se generalizira na slučaj više elemenata iz $R$. Ako su $a_1, a_2, \ldots, a_n \in R$, od kojih nisu svi jednaki 0, njihova **najveća zajednička mjera** je element $c \in R$ sa sljedeća dva svojstva:

$$c|a_1, \quad c|a_2, \quad \ldots \quad c|a_n$$

$$d \in R, \quad d|a_1, \quad d|a_2, \quad \ldots \quad d|a_n \qquad \Longrightarrow \qquad d|c.$$

Najveća zajednička mjera postoji i jedinstvena je do na množenje s invertibilnim elementom iz $R$. Drugim riječima, skup svih najvećih zajedničkih mjera elemenata $a_1, a_2, \ldots, a_n$ je jedna klasa asociranosti u $R \setminus \{0\}$.

Radi određenijeg označavanja možemo postupiti slično kao u prethodnom odjeljku. Izaberemo skup $R'$ koji se sastoji od po točno jednog predstavnika svake klase asociranosti u $R \setminus \{0\}$, s tim da je $1 \in R'$; dakle, $R^* \cap R' = \{1\}$. Nadalje, možemo pretpostavljati da je $R'$ multiplikativni monoid, tj. da iz $a, b \in R'$ slijedi $ab \in R'$. To možemo postići tako da najprije izaberemo skup $\mathcal{P}$ predstavnika svih ireducibilnih klasa asociranosti u $R$, a zatim definiramo $R'$ kao najmanji multiplikativni monoid u $R$ koji sadrži $\mathcal{P}$. Dakle, $R' = \{1\} \cup \mathcal{P} \cup \mathcal{Q}$, gdje je $\mathcal{Q}$ skup svih produkata elemenata iz $\mathcal{P}$. Tada ćemo za $a_1, a_2, \ldots, a_n \in R$, od kojih nisu svi jednaki 0, jedinstvenu u $R'$ najveću zajedničku mjeru tih elemenata označavati sa $GCD(a_1, a_2, \ldots, a_n)$.

Neka je sada $P \in R[X] \setminus \{0\}$. Tada definiramo **sadržaj polinoma** $P$ kao najveću zajedničku mjeru koeficijenata polinoma $P$. Sadržaj polinoma $P$ označavat ćemo sa $c(P)$. Dakle,

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \in R[X] \setminus \{0\} \qquad \Longrightarrow \qquad c(P) = GCD(a_0, a_1, a_2, \ldots, a_n).$$

Polinom $P$ zove se **primitivan** ako je $c(P) = 1$, tj. ako ne postoji neinvertibilan element iz $R$ koji dijeli sve koeficijente polinoma $P$.

**Propozicija 3.10.** *Uz uvedene oznake neka su $S \in R[X]$ i $P, Q \in K[X]$ takvi da je $S = PQ$. Tada postoji $\lambda \in K \setminus \{0\}$ takav da su $\lambda P \in R[X]$ i $\lambda^{-1}Q \in R[X]$. Posebno, ako je $S$ ireducibilan u $R[X]$, onda je $S$ ireducibilan i u $K[X]$.*

**Dokaz:** Koeficijenti polinoma $P$ i $Q$ su kvocijenti elemenata iz $R$. Ako je $a$ najmanji zajednički nazivnik svih koeficijenata od $P$ tada je $P^* = aP \in R[X]$. Slično, ako je $b$ najmanji zajednički nazivnik razlomaka koji predstavljaju koeficijente polinoma $Q$, onda je $Q^* = bQ \in R[X]$. Dakle, $abS = P^*Q^*$, gdje su $P^*, Q^* \in R[X]$ i $c = ab \in R$.

Neka je sada $p$ bilo koji ireducibilni djelitelj od $c$, odnosno, bilo koji prosti faktor od $c$. Dokazat ćemo da tada ili $p$ dijeli sve koeficijente od $P^*$ ili dijeli sve koeficijente od $Q^*$. Doista, neka je

$$P^* = b_0 + b_1X + \cdots + b_qX^q \qquad \text{i} \qquad Q^* = c_0 + c_1X + \cdots + c_sX^s.$$

Budući da je $p$ prosti djelitelj od $c = ab$ i budući da je $abS = P^*Q^*$, zaključujemo da $p$ dijeli sve koeficijente od $P^*Q^*$. Pretpostavimo da $p$ ne dijeli sve $b_i$ i da $p$ ne dijeli sve $c_j$. Neka su $u$ i $v$ najmanji indeksi takvi da $p$ ne dijeli $b_u$ i da $p$ ne dijeli $c_v$. Koeficijent od $X^{u+v}$ u polinomu $P^*Q^*$ je

$$b_0c_{u+v} + b_1c_{u+v-1} + \cdots + b_uc_v + \cdots + b_{u+v-1}c_1 + b_{u+v}c_0.$$

Zbog izbora indeksa $u$ i $v$ element $p$ dijeli svaki sumand osim $b_uc_v$. No odatle slijedi da $p$ ne dijeli gornju sumu. Ova kontradikcija pokazuje da je pretpostavka bila pogrešna, odnosno, dokazano je da $p$ dijeli sve koeficijente od $P^*$ ili $p$ dijeli sve koeficijente od $Q^*$.

Dakle, za svaki prosti faktor $p$ od $c = ab$ možemo s njim podijeliti $c$ i sve koeficijente jednog od polinoma $P^*$ i $Q^*$. Korak po korak na taj način dolazimo do izraza oblika $S = P_0Q_0$, gdje je $P_0 \in R[X]$ dobiven iz $P^*$ dijeljenjem svih koeficijenata od $P^*$ s nekim njihovim zajedničkim djeliteljem iz $R$, a također, $Q_0 \in R[X]$ je dobiven iz $Q^*$ dijeljenjem svih koeficijenata od $Q^*$ s nekim njihovim zajedničkim djeliteljem. Budući da je $P^*$ dobiven iz $P$ množenjem s nekim elementom iz $R$, a $P_0$ je dobiven iz $P^*$ dijeljenjem s nekim elementom iz $R$, zaključujemo da je $P_0 = \lambda P$ za neki $\lambda \in K$. No tada imamo

$$PQ = S = P_0Q_0 = \lambda PQ_0 \qquad \Longrightarrow \qquad Q = \lambda Q_0 \qquad \Longrightarrow \qquad Q_0 = \lambda^{-1}Q.$$

Mala modifikacija gornjeg dokaza daje nam tzv. **Gaussovu lemu**:

**Teorem 3.8.** *Uz uvedene oznake neka su $P$ i $Q$ nekonstantni polinomi u $R[X]$. Tada vrijedi $c(PQ) = c(P)c(Q)$. Posebno, ako su polinomi $P$ i $Q$ primitivni, tada je i njihov umnožak $PQ$ primitivan polinom.*

**Dokaz:** Po definiciji sadržaja je $P = c(P)P^*$ i $Q = c(Q)Q^*$, gdje su $P^*$ i $Q^*$ primitivni polinomi. Tada imamo $PQ = c(P)c(Q)P^*Q^*$. Slijedi da $c(P)c(Q)$ dijeli svaki koeficijent od $PQ$, pa slijedi da $c(P)c(Q)$ dijeli $c(PQ)$. Neka je sada $p \in \mathcal{P}$ bilo koji prosti faktor od $c(PQ)$. Tada $p$ dijeli $c(P)c(Q)P^*Q^* = PQ$, a dokaz propozicije 3.10. pokazuje da $p$ dijeli sve koeficijente od $P$ ili $p$ dijeli sve koeficijente od $Q$. No to znači da $p$ dijeli $c(P)$ ili $p$ dijeli $c(Q)$. U oba slučaja $p$ dijeli umnožak $c(P)c(Q)$. Odatle korak po korak slijedi da $c(PQ)$ dijeli $c(P)c(Q)$. Dakle, $c(PQ)$ i $c(P)c(Q)$ su asocirani, a kako se $R'$ sastoji od točno jednog elementa svake klase asociranosti, slijedi $c(PQ) = c(P)c(Q)$.

**Korolar 3.2.** *Neka je $P \in R[X]$ nekonstantni polinom i $P = aP^*$, gdje je $a \in R$ i polinom $P^*$ je primitivan. Tada je $a$ asociran sa $c(P)$.*

**Dokaz:** Budući da $a$ dijeli svaki koeficijent od $P$ slijedi da $a$ dijeli $c(P)$. S druge strane, ako je $p$ bilo koji prosti faktor od $c(P)$, tada $p$ dijeli svaki koeficijent od $P = aP^*$, pa slijedi da $p$ dijeli $a$ ili $p$ dijeli svaki koeficijent od $P^*$. No kako je polinom $P^*$ primitivan, njegovi koeficijenti nemaju zajedničkih prostih faktora. Prema tome $p$ dijeli $a$. Podijelimo li s $p$ i nastavimo na isti način kao i u prethodnom dokazu, zaključujemo da $c(P)$ dijeli $a$. Time je dokazano da su $a$ i $c(P)$ asocirani.

**Korolar 3.3.** *Ako je $P \in R[X]$ primitivan polinom i ako $P$ dijeli polinom $Q \in R[X]$ u prstenu $K[X]$, onda $P$ dijeli $Q$ u prstenu $R[X]$.*

**Dokaz:** Pretpostavimo da je $Q = PS$ za neki $S \in K[X]$. Možemo pisati $S = \alpha S^*$, gdje je $\alpha \in K$ i $S^*$ je primitivan polinom u $R[X]$. Slijedi $Q = \alpha PS^*$. S druge strane je $Q = c(Q)Q^*$, gdje je $Q^*$ primitivan, pa imamo $c(Q)Q^* = \alpha PS^*$. Ako je $a \in R$ takav da je $b = \alpha a \in R$, slijedi $ac(Q)Q^* = bPS^*$. Polinomi $Q^*$ i $PS^*$ su primitivni, pa zaključjemo da su $ac(Q)$ i $b$ asocirani, tj. $ac(Q) = bd$ za neki invertibilan element $d \in R$. Dobivamo $bdQ = ac(Q)Q^* = bPS^*$, pa slijedi $dQ = PS^*$. Dakle, $Q = d^{-1}PS^*$, a kako je $d^{-1}S^* \in R[X]$, vidimo da $P$ dijeli $Q$ u $R[X]$.

Iz propozicije 3.10. slijedi precizna usporedba ireducibilnih elemenata u $R[X]$ i $K[X]$ :

**Propozicija 3.11.** *Ako je $P$ nekonstantni polinom u $R[X]$, onda je $P$ ireducibilan u $R[X]$ ako i samo ako je primitivan i ireducibilan u $K[X]$.*

**Dokaz:** Pretpostavimo da je $P$ ireducibilan element prstena $R[X]$. Prema propoziciji 3.10. tada je $P$ ireducibilan u prstenu $K[X]$. Kad $P$ ne bi bio primitivan, imali bismo $P = c(P)P^*$, gdje je $P^*$ primitivan i $c(P) \in R$ je neinvertibilan. No to je u suprotnosti s ireducibilnošću od $P$ u prstenu $R[X]$. Prema tome, $P$ je primitivan.

Pretpostavimo sada da je $P$ primitivan i ireducibilan u prstenu $K[X]$. Nadalje, pretpostavimo da suprotno tvrdnji $P$ nije ireducibilan u $R[X]$. Tada postoje neinvertibilni elementi $Q, Q' \in R[X]$ takvi da je $P = QQ'$. Budući da je $P$ primitivan, niti $Q$ niti $Q'$ ne mogu biti konstantni polinomi, odnosno, ne može biti $Q \in R$ niti $Q' \in R$. Dakle, $\deg Q \geq 1$ i $\deg Q' \geq 1$. No to je nemoguće, jer je $R \subseteq K$ i $P$ je po pretpostavci ireducibilan u $K[X]$.

Gaussova lema ima za posljedicu najavljeni rezultat:

**Teorem 3.9.** *Ako je $R$ faktorijalan prsten, tada je i $R[X]$ faktorijalan prsten.*

**Dokaz:** Pretpostavimo da je $P \in R[X]$, $P \neq 0$. Tada je $P = c(P)P^*$, gdje je polinom $P^*$ primitivan. No tada su prema teoremu 3.8. svi djelitelji od $P^*$ u $R[X]$ primitivni. Posebno, oni među njima koji su stupnja 0 su invertibilni elementi od $R$. Dakle, u svakoj netrivijalnoj faktorizaciji $P^* = QQ'$ polinomi $Q$ i $Q'$ su primitivni i stupnja manjeg od $\deg P^* = \deg P$. Zaključujemo da je proces faktorizacije u primitivne faktore moguće ponoviti samo konačno mnogo puta, dakle, po propoziciji 3.11. dolazimo do rastava $P^*$ u produkt ireducibilnih polinoma u $R[X]$. Sada još rastavimo $c(P)$ u produkt ireducibilnih elemenata prstena $R$, pa vidimo da je zadovoljen uvjet (1) iz definicije faktorijalnog prstena.

Prema propoziciji 3.8. treba još dokazati da je svaki polinom $P \in R[X]$ koji je ireducibilan u prstenu $R[X]$ ujedno prost u tom prstenu. Neka je, dakle, $P \in R[X]$ ireducibilan element prstena $R[X]$. Razmotrit ćemo sada dvije mogućnosti: $\deg P \geq 1$ i $\deg P = 0$.

Neka je najprije $\deg P \geq 1$. Tada je po propoziciji 3.11. polinom $P$ primitivan i ireducibilan u $K[X]$. Pretpostavimo da $P$ dijeli umnožak $AB$, gdje su $A, B \in R[X]$. Kako je $K[X]$ faktorijalan prsten, slijedi da je $P$ prost u $K[X]$, dakle, $P$ dijeli $A$ u $K[X]$ ili $P$ dijeli $B$ u $K[X]$. Prema korolaru 3.3. $P$ dijeli $A$ u $R[X]$ ili $P$ dijeli $B$ u $R[X]$. Dakle, $P$ je prost element prstena $R[X]$.

Pretpostavimo sada da je $\deg P = 0$, tj. $P \in R$. Tada je $P$ ireducibilan element prstena $R$, a

kako je prsten $R$ faktorijalan, $P$ je prost element prstena $R$. Treba dokazati da odatle slijedi da je $P$ prost u prstenu $R[X]$. Pretpostavimo da $P$ dijeli umnožak $AB$, gdje su $A, B \in R[X]$, dakle, $AB = PQ$, za neki $Q \in R[X]$. Tada imamo

$$A = c(A)A^*, \quad B = c(B)B^*, \quad Q = c(Q)Q^*, \qquad \text{gdje su} \quad A^*, B^*, Q^* \quad \text{primitivni.}$$

Slijedi $c(A)c(B)A^*B^* = Pc(Q)Q^*$. Polinom $Q^*$ je primitivan, a po teoremu 3.8. i umnožak $A^*B^*$ je primitivan polinom. Slijedi da su $c(A)c(B) = Pc(Q)$ asocirani u $R$, tj. postoji invertibilan element $d$ prstena $R$ takav da je $c(A)c(B) = Pc(Q)d$. Dakle, $P$ dijeli umnožak $c(A)c(B)$ u prstenu $R$, a kako je $P$ prost u prstenu $R$, zaključujemo da $P$ dijeli $c(A)$ ili $P$ dijeli $c(B)$. Ako $P$ dijeli $c(A)$ u prstenu $R$, onda $P$ dijeli $A = c(A)A^*$ u $R[X]$, a ako $P$ dijeli $c(B)$ u prstenu $R$, onda $P$ dijeli $B = c(B)B^*$ u $R[X]$.

Time je teorem u potpunosti dokazan.

Sljedeći tzv. **Eisensteinov kriterij ireducibilnosti** često se koristi da bi se dokazalo da je neki polinom ireducibilan.

**Teorem 3.10.** *Neka je $P \in R[X]$ nekonstantni polinom:*

$$P = c_0 + c_1X + \cdots + c_nX^n, \qquad c_0, c_1, \ldots, c_n \in R, \quad c_n \neq 0, \quad n \geq 1.$$

*Pretpostavimo da postoji prosti element $p$ prstena $R$ sa sljedećim svojstvima:*

(*a*) *$p$ dijeli $c_0, c_1, \ldots, c_{n-1}$;*

(*b*) *$p$ ne dijeli $c_n$.*

(*c*) *$p^2$ ne dijeli $c_0$.*

*Tada je polinom $P$ ireducibilan u prstenu $K[X]$.*

**Dokaz:** Podijelimo li $P$ s njegovim sadržajem $c(P)$ dolazimo do primitivnog polinoma s istim svojstvima, budući da zbog (*b*) $p$ ne dijeli $c(P)$. Dakle, u dokazu možemo pretpostavljati da je polinom $P$ primitivan. Sada je prema propoziciji 3.11. dovoljno dokazati da je polinom $P$ ireducibilan u $R[X]$. Dakle, pretpostavimo da je $P = AB$, gdje su

$$A = a_0 + a_1X + \cdots + a_rX^r, \quad B = b_0 + b_1X + \cdots + b_sX^s, \quad a_0, a_1, \ldots, a_r, b_0, b_1, \ldots, b_s \in R, \quad a_rb_s \neq 0.$$

Ako je $r = 0$, onda $A = a_0$ dijeli sve koeficijente od $P$, dakle, $a_0$ dijeli $c(P) = 1$, pa slijedi da je $a_0$ invertibilni element od $R$, dakle, i od $R[X]$. Stoga možemo pretpostaviti da je $r \geq 1$ i analogno $s \geq 1$. Po pretpostavci $p$ dijeli $c_0 = a_0b_0$, ali $p^2$ ne dijeli $c_0$. Dakle, $p$ ne dijeli i $a_0$ i $b_0$ nego samo jednog od njih. Možemo pretpostaviti da $p$ dijeli $a_0$ i ne dijeli $b_0$. Nadalje, $c_n = a_rb_s$, a po pretpostavci (*b*) $p$ ne dijeli $c_n$. Prema tome, $p$ ne dijeli niti $a_r$ niti $b_s$. Neka je $i$ najmanji indeks iz $\{0, 1, \ldots, r\}$ takav da $p$ ne dijeli $a_i$. Tada je $1 \leq i \leq r < n$, jer je $r + s = n$ i $s \geq 1$. Imamo

$$c_i = a_0b_i + a_1b_{i-1} + \cdots + a_{i-1}b_1 + a_ib_0.$$

Prema izboru indeksa $i$ znamo da $p$ dijeli $a_0, \ldots, a_{i-1}$, a kako $p$ dijeli $c_i$, iz gornje jednakosti slijedi da $p$ dijeli umnožak $a_ib_0$. No kako $p$ ne dijeli $a_i$, zaključujemo da $p$ dijeli $b_0$. To je u suprotnosti s prijašnjim zaključkom da $p$ ne dijeli $b_0$. Ova kontradikcija pokazuje da ne postoji takva faktorizacija $P = AB$, što znači da je $P$ ireducibilan u prstenu $R[X]$.

# Poglavlje 4

# Osnovni pojmovi teorije proširenja polja

## 4.1 Proširenja polja

Ako je $K$ polje, tada znamo da je prsten polinoma $K[X]$ faktorijalan; štoviše, to je domena glavnih ideala. Prema tome, svaki se nekonstantan polinom $P$ može u biti na jedinstven način faktorizirati u produkt ireducibilnih polinoma. Svaka nultočka $\alpha$ od $P$ je nultočka nekog od tih ireducibilnih faktora, pa je taj ireducibilni faktor oblika $\beta(X-\alpha)$, $\beta \neq 0$. Međutim, može se naravno dogoditi da $P$ uopće nema nultočaka u polju $K$. Npr. polinom $X^2+1$ nema realnih nultočaka, ali ako promatramo šire polje kompleksnih brojeva, onda taj polinom ima dvije nultočke, $i$ i $-i$.

Ako su $K$ i $L$ polja i $K \subseteq L$, tada kažemo da je $L$ **proširenje polja** $K$. U tom slučaju $L$ možemo promatrati i kao vektorski prostor nad poljem $K$. Ukoliko je taj vektorski prostor konačnodimenzionalan, kažemo da je $L$ **konačno proširenje** polja $K$, a prirodan broj $\dim_K L$ zovemo **stupanj proširenja** i označavamo $[L : K]$. Ukoliko proširenje $L$ polja $K$ nije konačno, pišemo $[L : K] = \infty$.

Ako je $P$ nekonstantni polinom iz $K[X]$, uvijek možemo pronaći proširenje $L$ polja $K$ u kome $P$ ima nultočku. Da to dokažemo, uočimo najprije jednostavnu činjenicu:

**Lema 4.1.** *Neka su $K$ i $L$ polja i neka je $\varphi : K \to L$ netrivijalni homomorfizam prstenova, tj. preslikavanje $\neq 0$ takvo da je $\varphi(\alpha+\beta) = \varphi(\alpha)+\varphi(\beta)$ i $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$ za sve $\alpha, \beta \in K$. Tada je $\varphi(1_K) = 1_L$ i $\varphi$ je monomorfizam.*

**Dokaz:** Tvrdnja slijedi iz činjenice da je prema tvrdnji $(b)$ teorema 3.1. $\operatorname{Ker}\varphi$ ideal u $K$, a prema propoziciji 3.3. $\{0\}$ i $K$ su jedini ideali u $K$. Budući da je $\varphi \neq 0$, to je $\operatorname{Ker}\varphi \neq K$, pa slijedi $\operatorname{Ker}\varphi = \{0\}$, što znači da je $\varphi$ monomorfizam.

**Teorem 4.1.** *Neka je $K$ polje i $P \in K[X]$ nekonstantni polinom. Tada postoji proširenje $L$ polja $K$ i element $\alpha \in L$ takav da je $P(\alpha) = 0$.*

**Dokaz:** Budući da se $P$ može faktorizirati u produkt ireducibilnih polinoma, bez smanjenja općenitosti možemo pretpostaviti da je polinom $P$ ireducibilan. Budući da je $K[X]$ faktorijalan prsten, prema propoziciji 3.8. $P$ je prost element prstena $K[X]$. Iz propozicije 3.9. zaključujemo da je $\mathcal{J} = K[X]P$ prost ideal, a kako je $K[X]$ domena glavnih ideala, prema propoziciji 3.5. $\mathcal{J}$ je maksimalan ideal u prstenu $K[X]$. Sada iz propozicije 3.4. slijedi da je kvocijentni prsten $L = K[X]/\mathcal{J}$ polje. Definiramo preslikavanje $\varphi : K \to L$ kao restrikciju kvocijentnog homomorfizma $K[X] \to K[X]/\mathcal{J}$, tj. $\varphi(\lambda) = \lambda + \mathcal{J}$, $\lambda \in K$. Tada je $\varphi$ homomorfizam prstenova koji jedinicu $1 \in K$ prslikava u jedinicu $1+\mathcal{J}$ polja $L$. Prema tome je $\varphi \neq 0$, pa je po lemi 4.1. $\varphi$ monomorfizam. Pomoću monomorfizma $\varphi$ možemo polje $K$ identificirati s potpoljem od $L$ : element $\lambda \in K$ identificira se s klasom $\lambda + \mathcal{J} \in L$. Neka je sada $\alpha = X + \mathcal{J} \in L$. Ako je

$P = \alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n$, onda imamo

$$P(\alpha) = (\alpha_0 + \mathcal{J}) + \alpha_1(X + \mathcal{J}) + \cdots + \alpha_n(X + \mathcal{J})^n = (\alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n) + \mathcal{J} = P + \mathcal{J}.$$

Međutim, $P \in K[X]P = \mathcal{J}$, dakle, $P + \mathcal{J}$ je nula u polju $L = K[X]/\mathcal{J}$. Time je dokazano da je $P(\alpha) = 0$.

**Korolar 4.1.** *Polinomi $P, Q \in K[X]$ su relativno prosti ako i samo ako oni ni u jednom proširenju polja $K$ nemaju zajedničku nultočku.*

**Dokaz:** Pretpostavimo da su polinomi $P$ i $Q$ relativno prosti. Tada im je najveća zajednička mjera 1, pa postoje $A, B \in K[X]$ takvi da je $AP + BQ = 1$. Kad bi za neko proširenje $L$ od $K$ i za neki $\alpha \in L$ bilo $P(\alpha) = Q(\alpha) = 0$, slijedilo bi $0 = 1$. Ova kontradikcija pokazuje da $P$ i $Q$ nemaju zajedničku nultočku ni u jednom proširenju $L$ polja $K$.

Pretpostavimo sada da $P$ i $Q$ nisu relativno prosti. Tada je njihova najveća zajednička mjera $M$ nekonstantni polinom. Prema teoremu 4.1. postoje proširenje $L$ polja $K$ i element $\alpha \in L$ takvi da je $M(\alpha) = 0$. Budući da $M$ dijeli i $P$ i $Q$, slijedi da je $P(\alpha) = Q(\alpha) = 0$.

**Korolar 4.2.** *Neka su $P$ i $Q$ međusobno različiti normirani ireducibilni polinomi u $K[X]$. Tada $P$ i $Q$ nemaju zajedničku nultočku ni u jednom proširenju polja $K$.*

**Dokaz:** Tvrdnja je neposredna posljedica korolara 4.1. budući da su različiti normirani ireducibilni polinomi relativno prosti.

Neka je $L$ proširenje polja $K$. Za $\alpha \in L$ ćemo sa $K[\alpha]$ označavati najmanji potprsten od $L$ koji sadrži $K$ i $\alpha$. Svaki potprsten od $L$ koji sadrži $K$ i $\alpha$ mora sadržavati i sve potencije $\alpha^n$, $n \geq 0$, dakle i sve $K-$linearne kombinacije tih potencija. No $K-$linearna kombinacija potencija od $\alpha$ je u stvari element od $L$ oblika $P(\alpha)$ za neki $P \in K[X]$. Dakle,

$$K[\alpha] = \{P(\alpha);\ P \in K[X]\}.$$

Primijetimo još da je preslikavanje $P \mapsto P(\alpha)$ epimorfizam prstena $K[X]$ na prsten $K[\alpha]$.

Uz iste pretpostavke sa $K(\alpha)$ označavamo najmanje potpolje od $L$ koje sadrži $K$ i $\alpha$. Naravno, $K[\alpha] \subseteq K(\alpha)$. Prsten $K[\alpha]$ je integralna domena sadržana u polju $L$. Identično preslikavanje $\beta \mapsto \beta$, $\beta \in K[\alpha]$, možemo shvatiti kao unitalni monomorfizam prstena $K[\alpha]$ u polje $L$. Stoga po teoremu 3.5. postoji njegovo jedinstveno proširenje sa polja razlomaka od $K[\alpha]$ u polje $L$. Budući da je $K(\alpha)$ najmanje potpolje od $L$ koje sadrži $K[\alpha]$, to proširenje je izomorfizam polja razlomaka prstena $K[\alpha]$ na polje $K(\alpha)$. To znači da je

$$K(\alpha) = \{P(\alpha)Q(\alpha)^{-1};\ P, Q \in K[X],\ Q(\alpha) \neq 0\}.$$

U stvari, uskoro ćemo vidjeti da postoji mnogo jednostavniji opis polja $K(\alpha)$.

Neka je $L$ proširenje polja $K$. Za element $\alpha \in L$ kažemo da je **algebarski nad** $K$ ako postoji nekonstantni polinom $P \in K[X]$ takav da je $P(\alpha) = 0$. Ako $\alpha$ nije algebarski nad $K$ kažemo da je **transcendentan nad** $K$. Ako je svaki element $\alpha \in L$ algebarski nad $K$, kažemo da je $L$ **algebarsko proširenje polja** $K$.

Neka je $\alpha \in L$ algebarski nad $K$. Stavimo

$$\mathcal{J} = \{P \in K[X];\ P(\alpha) = 0\}.$$

Očito je $\mathcal{J}$ ideal u prstenu $K[X]$. Kako je $K[X]$ domena glavnih ideala, postoji jedinstven normiran polinom $\mu_\alpha \in K[X]$ takav da je

$$\mathcal{J} = \{P \in K[X];\ P(\alpha) = 0\} = K[X]\mu_\alpha = \{Q\mu_\alpha;\ Q \in K[X]\}.$$

Polinom $\mu_\alpha$ zove se **minimalni polinom** elementa $\alpha \in L$ algebarskog nad $K$. Taj polinom ima sljedeća svojstva:

(1) Ako je $P \in K[X]$, onda vrijedi $P(\alpha) = 0$ ako i samo ako je polinom $P$ djeljiv s polinomom $\mu_\alpha$.

(2) Polinom $\mu_\alpha$ ima najmanji stupanj među svim nekonstantnim polinomima iz $K[X]$ kojima je $\alpha$ nultočka.

(3) Polinom $\mu_\alpha$ je ireducibilan u prstenu $K[X]$.

(4) $\mu_\alpha$ je jedini normiran ireducibilan polinom u $K[X]$ kome je $\alpha$ nultočka.

Doista, svojstvo (1) izlazi neposredno iz definicije, a svojstvo (2) je direktna posljedica svojstva (1). Dokažimo svojstvo (3). Pretpostavimo da je $\mu_\alpha = PQ$, gdje su $P, Q \in K[X]$ nekonstantni polinomi. Tada je $P(\alpha)Q(\alpha) = \mu_\alpha(\alpha) = 0$, dakle je $P(\alpha) = 0$ ili $Q(\alpha) = 0$. Međutim, kako su i $P$ i $Q$ po pretpostavci nekonstantni, dakle, $\deg P \geq 1$ i $\deg Q \geq 1$, vrijedi $\deg P < \deg \mu_\alpha$ i $\deg Q < \deg \mu_\alpha$. Stoga su $P(\alpha) = 0$ i $Q(\alpha) = 0$ u suprotnosti sa svojstvom (2). Ova kontradikcija pokazuje da je nemoguća faktorizacija polinoma $\mu_\alpha$ u produkt dvaju nakonstantnih polinoma, dakle, polinom $\mu_\alpha$ je ireducibilan. Odatle slijedi i svojstvo (4).

Razmotrimo promatranu problematiku na još jedan način. Za element $\alpha$ proširenja $L$ polja $K$ definiramo preslikavanje $\Phi_\alpha : K[X] \to L$ ovako:

$$\Phi_\alpha(P) = P(\alpha), \qquad P \in K[X].$$

Znamo da vrijedi $(P+Q)(\alpha) = P(\alpha)+Q(\alpha)$ i $(PQ)(\alpha) = P(\alpha)Q(\alpha)$ za sve $P, Q \in K[X]$; nadalje, ako je $P$ konstanta 1, onda je, naravno, $P(\alpha) = 1$. To znači da je $\Phi_\alpha$ unitalni homomorfizam prstena $K[X]$ u polje $L$. Očito je prije promatrani ideal $\mathcal{J} = \{P \in K[X];\ P(\alpha) = 0\}$ upravo jezgra homomorfizma $\Phi_\alpha$. Dakle, element $\alpha \in L$ je algebarski nad $K$ ako i samo ako homomorfizam $\Phi_\alpha$ nije injektivan. S druge strane, element $\alpha$ je transcendentan nad $K$ ako i samo ako je $\Phi_\alpha$ monomorfizam.

**Teorem 4.2.** *Neka je $L$ proširenje polja $K$ i neka je element $\alpha \in L$ algebarski nad $K$. Neka je $\mu_\alpha$ minimalni polinom od $\alpha$ nad $K$ i $m = \deg \mu_\alpha$. Tada je*

$$K(\alpha) = K[\alpha] = \{P(\alpha);\ P \in K[X],\ \deg P \leq m-1\}.$$

*Preciznije, $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$ je baza vektorskog prostora $K(\alpha)$ nad poljem $K$. Posebno,*

$$[K(\alpha) : K] = m = \deg \mu_\alpha.$$

**Dokaz:** Stavimo

$$K_{m-1}[\alpha] = \{P(\alpha);\ P \in K[X],\ \deg P \leq m-1\}.$$

Očito je $K_{m-1}[\alpha] \subseteq K[\alpha]$. Dokažimo da vrijedi i obrnuta inkluzija, dakle, jednakost. Neka je $Q \in K[X]$. Tada po propoziciji 1.12. postoje $R, P \in K[X]$ takvi da je

$$Q = R\mu_\alpha + P \qquad \text{i} \qquad \deg P < \deg \mu_\alpha.$$

No to znači da je $\deg P \leq m-1$ i imamo

$$Q(\alpha) = R(\alpha)\mu_\alpha(\alpha) + P(\alpha) = P(\alpha),$$

jer je $\mu_\alpha(\alpha) = 0$. Dakle, za svaki $Q \in K[X]$ postoji $P \in K[X]$ takav da je $Q(\alpha) = P(\alpha)$ i $\deg P \leq m-1$. Time je dokazana obrnuta inkluzija, odnosno jednakost $K[\alpha] = K_{m-1}[\alpha]$.

Vrijedi $K[\alpha] \subseteq K(\alpha)$, a da bismo dokazali da se radi o jednakosti, dovoljno je dokazati da je prsten $K[\alpha]$ polje, tj. da sadrži invers svakog svog elementa različitog od nule. Doista, neka je $\beta \in K[\alpha]$, $\beta \neq 0$. Prema dokazanom postoji $P \in K[X]$ takav da je $\beta = P(\alpha)$ i $\deg P \leq m-1$. Budući da je polinom $\mu_\alpha$ ireducibilan i $\deg P < \deg \mu_\alpha$, polinomi $\mu_\alpha$ i $P$ su relativno prosti. No tada po korolaru 1.8. postoje polinomi $A, B \in K[X]$ takvi da je $AP + B\mu_\alpha = 1$. Kako je $\mu_\alpha(\alpha) = 0$, slijedi $A(\alpha)P(\alpha) = 1$. Prema tome, $\beta^{-1} = A(\alpha) \in K[\alpha]$. Time je dokazano da je $K[\alpha]$ potpolje od $L$, tj. vrijedi $K[\alpha] = K(\alpha)$.

Napokon, ako je $P \in K[X]$ stupnja $\leq m-1$, onda je $P(\alpha)$ $K-$linearna kombinacija elemenata $1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$. To znači da skup $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$ razapinje vektorski prostor $K(\alpha)$ nad poljem $K$. Taj je skup linearno nezavisan. Doista, ako pretpostavimo da su $a_0, a_1, \ldots, a_{m-1} \in K$ takvi da je

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{m-1}\alpha^{m-1} = 0,$$

onda je $P = a_0 + a_1X + a_2X^2 + \cdots + a_{m-1}X^{m-1}$ polinom stupnja $\leq m-1$ i vrijedi $P(\alpha) = 0$. Sada iz svojstva (2) minimalnog polinoma slijedi da je $P$ konstantan polinom, a kako je $P(\alpha) = 0$, nužno je ta konstanta nula, tj. $P = 0$. No to znači da su svi koeficijenti $a_0, a_1, \ldots, a_{m-1}$ jednaki nuli. Time je dokazana linearna nezavisnost elemenata $1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$ nad poljem $K$. Dakle, $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$ je baza vektorskog prostora $K(\alpha)$ nad poljem $K$.

U slučaju transcendentnog elementa proširenja situacija je bitno drugačija:

**Teorem 4.3.** *Neka je $L$ proširenje polja $K$ i neka je element $\alpha \in L$ transcendentan nad $K$. Tada se monomorfizam $\Phi_\alpha : K[X] \to L$ jedinstveno proširuje do monomorfizma polja $K(X)$ racionalnih fukcija, tj. polja razlomaka integralne domene $K[X]$, u polje $L$ i to je izomorfizam polja $K(X)$ na potpolje $K(\alpha)$ polja $L$.*

**Dokaz:** Iz teorema 3.5. neposredno slijedi da se monomorfizam $\Phi_\alpha$ jedinstveno proširuje do monomorfizma $\Psi_\alpha : K(X) \to L$. Budući da je polje $K(X)$ generirano prstenom $K[X]$, slijedi da je slika tog monomorfizma najmanje potpolje od $L$ koje sadrži $K[\alpha]$, odnosno, slika od $\Psi_\alpha$ je upravo potpolje $K(\alpha)$.

Vratimo se na opću teoriju proširenja polja. Dokazat ćemo sada pomoćnu tvrdnju koja će imati za posljedicu multiplikativnu formulu za uzastopna proširenja polja.

**Lema 4.2.** *Neka su $K \subseteq L \subseteq M$ polja, dakle, $L$ je proširenje polja $K$ i $M$ je proširenje polja $L$. Neka je $\{\alpha_i;\ i \in I\}$ baza vektorskog prostora $L$ nad poljem $K$ i neka je $\{\beta_j;\ j \in J\}$ baza vektorskog prostora $M$ nad poljem $L$. Tada je skup produkata $\{\alpha_i\beta_j;\ i \in I,\ j \in J\}$ baza vektorskog prostora $M$ nad poljem $K$.*

**Dokaz:** Svaki $\gamma \in M$ je linearna kombinacija elemenata $\beta_j$ s koeficijentima iz $L$.

$$\gamma = \sum_{j \in J} \delta_j\beta_j, \qquad \delta_j \in L, \quad \text{skup} \quad J_0 = \{j \in J;\ \delta_j \neq 0\} \quad \text{je konačan.}$$

Svaki od tih koeficijenata $\delta_j$ je linearna kombinacija elemenata $\alpha_i$ s koeficijentima iz $K$ :

$$\delta_j = \sum_{i \in I} \varepsilon_{ij}\alpha_i, \qquad j \in J_0, \quad \varepsilon_{ij} \in K, \quad \text{skupovi} \quad I_j = \{i \in I;\ \varepsilon_{ij} \neq 0\} \quad \text{su konačni.}$$

Slijedi

$$\gamma = \sum_{j \in J} \sum_{i \in I} \varepsilon_{ij}\alpha_i\beta_j.$$

Time je dokazano da je vektorski prostor $M$ nad poljem $K$ razapet skupom produkata $\{\alpha_i\beta_j;\ i \in I,\ j \in J\}$. Treba još dokazati da su ti produkti linearno nezavisni nad poljem $K$. U tu svrhu pretpostavimo da su $\lambda_{ij} \in K$ takvi da je skup $\{(i,j) \in I \times J;\ \lambda_{ij} \neq 0\}$ konačan i da je

$$\sum_{(i,j)\in I\times J} \lambda_{ij}\alpha_i\beta_j = 0.$$

Stavimo tada

$$\delta_j = \sum_{i\in I} \lambda_{ij}\alpha_i, \qquad j \in J.$$

Tada su $\delta_j \in L$ i vrijedi

$$\sum_{j\in J} \delta_j\beta_j = 0.$$

Kako su elementi $\beta_j$, $j \in J$, linearno nezavisni nad poljem $L$, slijedi da je $\delta_j = 0\ \ \forall j \in J$. Dakle,

$$\sum_{i\in I} \lambda_{ij}\alpha_i = 0 \qquad \forall j \in J.$$

Međutim, koeficijenti $\lambda_{ij}$ su iz $K$ i elementi $\alpha_i$, $i \in I$, su linearno nezavisni nad $K$, pa slijedi $\lambda_{ij} = 0\ \ \forall i \in I$ i $\forall j \in J$. Time je dokazano da su produkti $\alpha_i\beta_j$, $i \in I$, $j \in J$, linearno nezavisni nad poljem $K$.

**Teorem 4.4.** *Neka su $K \subseteq L \subseteq M$ polja. Tada je*

$$[M : K] = [M : L] \cdot [L : K].$$

*Pri tome je operacija množenja proširena sa skupa prirodnih brojeva $\mathbb{N}$ na skup $\mathbb{N} \cup \{\infty\}$ ovako:*

$$\infty \cdot n = n \cdot \infty = \infty \cdot \infty = \infty, \qquad n \in \mathbb{N}.$$

*Drugim riječima, proširenje $M$ polja $K$ je konačno ako i samo ako su proširenja $M$ od $L$ i $L$ od $K$ konačna i tada je stupanj $[M : K]$ umnožak stupnjeva $[M : L]$ i $[L : K]$.*

**Dokaz:** Uz oznake iz leme 4.2., ako za svaki beskonačan skup $S$ stavimo $|S| = \infty$, onda je $[L : K] = |I|$ i $[M : L] = |J|$, a po toj lemi je $[M : K] = |I \times J| = |I| \cdot |J| = [L : K] \cdot [M : L]$.

Ako je $L$ proširenje polja $K$ i $S$ bilo koji podskup od $L$, onda ćemo sa $K(S)$ označiti najmanje potpolje od $L$ koje sadrži $K$ i $S$. Dakle, $K(S)$ je presjek svih potpolja od $L$ koja sadrže $K \cup S$. Ako je $S$ konačan skup, $S = \{\alpha_1, \ldots, \alpha_n\}$, $\alpha_1, \ldots, \alpha_n \in L$, onda ćemo pisati $K(S) = K(\alpha_1, \ldots, \alpha_n)$. Očito je $K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$. Za polje $L$ kažemo da je **konačno generirano proširenje polja** $K$, ako postoji $n \in \mathbb{N}$ i elementi $\alpha_1, \ldots, \alpha_n \in L$ takvi da je $L = K(\alpha_1, \ldots, \alpha_n)$.

**Teorem 4.5.** *Proširenje $L$ polja $K$ je konačno ako i samo ako je to proširenje algebarsko i konačno generirano.*

**Dokaz:** Pretpostavimo najprije da je proširenje $L$ polja $K$ konačno. Neka je $\alpha \in L$. Kako je $L$ konačnodimenzionalan vektorski prostor nad poljem $K$, beskonačan niz $1, \alpha, \alpha^2, \alpha^3, \ldots$ ne može biti linearno nezavisan nad poljem $K$. Stoga postoji prirodan broj $m$ i $a_0, a_1, a_2, \ldots, a_m \in K$ koji nisu svi jednaki nuli i takvi da je

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_m\alpha^m = 0.$$

No tada za polinom $P = a_0 + a_1X + a_2X^2 + \cdots + a_mX^m \in K[X]$ vrijedi $P \neq 0$ i $P(\alpha) = 0$. Dakle, svaki element $\alpha \in L$ je algebarski nad $K$ i time je dokazano da je $L$ algebarsko proširenje polja $K$.

Neka je sada $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ baza vektorskog prostora $L$ nad poljem $K$. Tada je očito

$$K(\alpha_1, \alpha_2, \ldots, \alpha_n) \subseteq L.$$

S druge strane,

$$L = \{a_1\alpha_1 + a_2\beta_2 + \cdots + a_n\alpha_n;\ a_1, a_2, \ldots, a_n \in K\} \subseteq K(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Iz dvije inkluzije slijedi jednakost

$$L = K(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Time je dokazana jedna implikacija iz tvrdnje teorema.

Pretpostavimo sada da je proširenje $L$ polja $K$ algebarsko i konačno generirano, tj. da postoje $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$ takvi da je $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Stavimo $K_0 = K$, $K_j = K(\alpha_1, \alpha_2, \ldots, \alpha_j)$ za $j = 1, 2, \ldots, n$. Tada je

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_{n-1} \subseteq K_n = L,$$

pa iz teorema 4.4. indukcijom po $n$ izvodimo

$$[L : K] = [K_n : K_{n-1}] \cdot [K_{n-1} : K_{n-2}] \cdots [K_2 : K_1] \cdot [K_1 : K_0]. \tag{4.1}$$

Za svaki $j$ je $K_j = K_{j-1}(\alpha_j)$, a kako je $\alpha_j$ algebarski nad $K$, on je algebarski i nad $K_{j-1}$. Stoga iz teorema 4.2. slijedi

$$[K_j : K_{j-1}] < \infty \qquad \text{za svaki} \quad j = 1, 2, \ldots, n,$$

a odatle i iz (4.1) slijedi $[L : K] < \infty$. Time je teorem u potpunosti dokazan.

**Teorem 4.6.** *Neka je $L$ proširenje polja $K$. Tada je skup $M$ svih elemenata $\alpha \in L$ algebarskih nad $K$ polje.*

**Dokaz:** Neka su $x, y \in M$, tj. $x$ i $y$ su algebarski nad $K$. Tada je $K \subseteq K(x) \subseteq K(x, y)$, pa je

$$[K(x, y) : K] = [K(x, y) : K(x)] \cdot [K(x) : K].$$

Kako je element $x$ algebarski nad $K$, to je $[K(x) : K] < \infty$. Nadalje, element $y$ je algebarski nad $K$ dakle i nad $K(x)$, pa slijedi i $[K(x, y) : K(x)] < \infty$. Zaključujemo da je $[K(x, y) : K] < \infty$, odnosno, $K(x, y)$ je konačno proširenje polja $K$. Prema teoremu 4.5. $K(x, y)$ je algebarsko proširenje od $K$, odnosno, svi elementi polja $K(x, y)$ su algebarski nad $K$. Posebno, $x \pm y$ i $xy$ su algebarski nad $K$, a također i $x^{-1}$ ako je $x \neq 0$. Dakle,

$$x, y \in M \qquad x + y, x - y, xy \in M \quad \text{i} \quad x^{-1} \in M \quad \text{ako je} \quad x \neq 0.$$

Time je dokazano da je $M$ potpolje od $L$; naravno, $K \subseteq M$.

Polje $M$ iz teorema 4.6. zove se **algebarsko zatvorenje polja $K$ u proširenju $L$.**

Dokazat ćemo sada da je proširenje polja $K$ nultočkom ireducibilnog polinoma $P \in K[X]$, čija je egzistencija dokazana u teoremu 4.1., u biti jedinstveno:

**Teorem 4.7.** *Neka je $P \in K[X]$ ireducibilan polinom i neka su $L$ i $L'$ proširenja polja $K$ i $\alpha \in L$ i $\beta \in L'$ takvi da je $P(\alpha) = P(\beta) = 0$, $L = K(\alpha)$, $L' = K(\beta)$. Tada postoji jedinstven homomorfizam polja $\varphi : L \to L'$ takav da je $\varphi(\alpha) = \beta$ i $\varphi(a) = a \ \forall a \in K$. Nadalje, $\varphi$ je izomorfizam polja $L$ na polje $L'$.*

**Dokaz:** Prije svega, neka su $\varphi, \psi : L \to L'$ homomorfizmi polja takvi da je $\varphi(a) = \psi(a) = a$ $\forall a \in K$ i $\varphi(\alpha) = \psi(\alpha) = \beta$. Stavimo $M = \{\gamma \in L;\ \varphi(\gamma) = \psi(\gamma)\}$. Tada je $M$ potpolje od $L$ koje sadrži $K \cup \{\alpha\}$, a kako je po pretpostavci $L = K(\alpha)$, slijedi $M = L$. Dakle, $\varphi = \psi$ i time je dokazana jedinstvenost. Nadalje, ako takav homomorfizam $\varphi$ postoji on je surjektivan jer je $L' = K(\beta)$, a također i injektivan, jer svaki homomorfizam polja je injektivan prema lemi 4.1.

Ostaje da dokažemo egzistenciju homomorfizma $\varphi$. Pri tome možemo pretpostaviti da je polinom $P$ normiran. Nadalje, prema dokazu teorema 4.1. možemo pretpostaviti da je $L = K[X]/\mathcal{J}$, gdje je $\mathcal{J} = K[X]P$, i $\alpha = X + \mathcal{J}$. Definiramo sada $\Phi : K[X] \to L'$ ovako:

$$\Phi(Q) = Q(\beta), \qquad Q \in K[X].$$

Tada je $\Phi$ unitalni homomorfizam prstenova. Njegova je jezgra

$$\operatorname{Ker}\Phi = \{Q \in K[X];\ Q(\beta) = 0\}.$$

Kako je $P(\beta) = 0$ i $P$ je normiran ireducibilni polinom u $K[X]$ zaključujemo da je $P$ minimalni polinom od $\beta$ nad $K$. No tada znamo da je $Q(\beta) = 0$ ako i samo ako je polinom $Q \in K[X]$ djeljiv s polinomom $P$. Dakle,

$$\operatorname{Ker}\Phi = \{Q \in K[X];\ P|Q\} = K[X]P = \mathcal{J}.$$

Stoga možemo definirati homomorfizam $\varphi : K[X]/\mathcal{J} \to L'$ sa

$$\varphi(Q + \mathcal{J}) = \Phi(Q), \qquad Q \in K[X].$$

Dakle, $\varphi$ je homomorfizam polja $L = K[X]/\mathcal{J}$ u polje $L'$ i vrijedi $\varphi(Q + \mathcal{J}) = Q(\beta)$, $Q \in K[X]$. Polje $K$ identificirano je s potpoljem od $L$ na način da je $a \in K$ identificiran s $a + \mathcal{J} \in L$, gdje se $a$ shvaća kao konstantni polinom iz $K[X]$. Dakle, $\varphi(a) = \varphi(a + \mathcal{J}) = a$ za svaki $a \in K$. Nadalje, $\varphi(\alpha) = \varphi(X + \mathcal{J}) = \beta$. Time je dokazana egzistencija homomorfizma $\varphi$.

## 4.2 Polja razlaganja

Neka je $K$ polje i $P \in K[X]$ nekonstantni polinom. Kažemo da se polinom $P$ **razlaže nad proširenjem** $L$ polja $K$ ako postoje $a \in K$ i $\alpha_1, \ldots, \alpha_n \in L$ takvi da je

$$P = a(X - \alpha_1) \cdots (X - \alpha_n).$$

Ako je k tome $L = K(\alpha_1, \ldots, \alpha_n)$, kažemo da je proširenje $L$ **polje razlaganja za polinom** $P$ **nad poljem** $K$.

**Teorem 4.8.** (*Egzistencija polja razlaganja*) *Neka je $K$ polje i $P \in K[X]$ nekonstantni polinom. Tada postoji polje razlaganja za $P$ nad $K$.*

**Dokaz:** Dokazat ćemo najprije da postoji proširenje $M$ polja $K$ nad kojim se polinom $P$ razlaže. U tom dokazu možemo pretpostavljati da je polinom $P$ normiran. Taj ćemo dokaz provesti metodom matematičke indukcije u odnosu na stupanj deg $P$ polinoma $P$.

Baza indukcije: Ako je deg $P = 1$, onda je tvrdnja trivijalna, jer je $P = X - a$ za $a \in K$, pa za $M$ možemo uzeti samo polje $K$.

Korak indukcije: Neka je deg $P = n \geq 2$ i pretpostavimo da je egzistencija proširenja nad kojim se polinom razlaže dokazana za normirane polinome stupnja manjeg od $n$. Prema teoremu 4.1. postoje proširenje $K_1$ polja $K$ i $\alpha_1 \in K_1$ takvi da je $P(\alpha_1) = 0$. Tada je $P = (X - \alpha_1)Q$, gdje je $Q \in K_1[X]$ normiran polinom i deg $Q = n - 1$. Po pretpostavci indukcije postoji proširenje $M$ polja $K_1$ nad kojim se polinom $Q$ razlaže, tj. postoje $\alpha_2, \ldots, \alpha_n \in M$ takvi da je $Q = (X - \alpha_2) \cdots (X - \alpha_n)$. No tada je $P = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)$ i $\alpha_1, \alpha_2, \ldots, \alpha_n \in M$. Time je korak indukcije proveden.

Ako je $M$ proširenje od $K$ i $\alpha_1, \ldots, \alpha_n \in M$ su takvi da je $P = a(X - \alpha_1) \cdots (X - \alpha_n)$, gdje je $a \in K$, onda je potpolje $L = K(\alpha_1, \ldots, \alpha_n)$ polje razlaganja polinoma $P$ nad poljem $K$.

**Teorem 4.9.** (*Jedinstvenost polja razlaganja*) *Neka je $P \in K[X]$ nekonstantni polinom i neka su $L$ i $L'$ proširenja polja $K$ koja su polja razlaganja polinoma $P$ nad poljem $K$. Tada postoji izomorfizam polja $\varphi : L \to L'$ takav da je $\varphi(a) = a \ \forall a \in K$.*

Ideja dokaza ovog teorema prilično je jednostavna, ali kad ga pokušamo provesti nailazimo na tehničke poteškoće. Ideja je da se dokaz provodi indukcijom koristeći jedinstvenost iz teorema 4.7. za proširenja s jednom nultočkom prostog faktora od $P$, i to ponavljamo dok god ne iscrpimo sve nultočke. Teškoća je što nakon prvog koraka koeficijenti dvaju polinoma koji se dobiju kao kvocijenti polinoma $P$ više nisu u istom polju nego samo znamo da su u međusobno izomorfnim poljima. Stoga se već drugi korak primjene teorema 4.7. ne može direktno provesti. Ono što nam treba je malo reformulirana verzija teorema 4.7. − to će biti naš teorem 4.10. No tada ćemo moći dokazati i generalniji oblik teorema 4.9. − to će biti naš teorem 4.11.

Neka su $K$ i $K'$ i neka je $\sigma : K \to K'$ izomorfizam polja. Tada naravno primjenom izomorfizma $\sigma$ na koeficijente polinoma $P \in K[X]$ dolazimo do izomorfizma prstenova $K[X] \to K'[X]$, koji ćemo označiti sa $P \mapsto P^\sigma$ :

$$P = a_0 + a_1 X + \cdots + a_n X^n \in K[X] \quad \Longrightarrow \quad P^\sigma = \sigma(a_0) + \sigma(a_1)X + \cdots + \sigma(a_n)X^n \in K'[X].$$

**Teorem 4.10.** *Neka je $\sigma : K \to K'$ izomorfizam polja. Pretpostavimo da je $P$ normiran ireducibilni polinom u $K[X]$ i neka su $L = K(\alpha)$ i $L' = K'(\beta)$ proširenja od $K$ i $K'$ takva da je $P(\alpha) = 0$ i $P^\sigma(\beta) = 0$. Tada postoji jedinstven homomorfizam polja $\varphi : L \to L'$ takav da je $\varphi|K = \sigma$ i $\varphi(\alpha) = \beta$. Nadalje, $\varphi$ je izomorfizam polja $L$ na polje $L'$.*

**Dokaz** u potpunosti slijedi dokaz teorema 4.7. Za egzistenciju polazimo od epimorfizma prstenova $K[X]$ na $L'$ definiranog sa $Q \mapsto Q^\sigma(\beta)$. Ponovo se nalazi da je jezgra $\mathcal{J} = K[X]P$ i prijelazom na kvocijent $K[X]/\mathcal{J} \simeq L$ dolazimo do traženog izomorfizma $L \to L'$.

**Teorem 4.11.** *Neka je $\sigma : K \to K'$ izomorfizam polja i neka je $P \in K[X]$ nekonstatni polinom. Nadalje, neka je $L$ polje razlaganja za polinom $P$ nad poljem $K$ i $L'$ polje razlaganja za polinom $P^\sigma$ nad poljem $K'$. Tada postoji izomorfizam polja $\varphi : L \to L'$ takav da je $\varphi|K = \sigma$ i da je $\alpha \in L$ nultočka od $P$ ako i samo ako je $\varphi(\alpha)$ nultočka od $P^\sigma$.*

**Dokaz:** Dokaz provodimo metodom matematičke indukcije u odnosu na deg $P \geq 1$.

Baza indukcije: Slučaj deg $P$ je trivijalan jer tada je $L = K$ i $L' = K'$ pa tvrdnja vrijedi za $\varphi = \sigma$.

Korak indukcije: Pretpostavimo da je $n \geq 2$ i da je tvrdnja dokazana za nekonstantne polinome stupnja manjeg od $n$. Neka je deg $P = n$. Neka je $Q$ normiran prosti faktor od $P$. Naravno, tada je $Q^\sigma$ normiran prosti faktor od $P^\sigma$. Polinom $Q$ ima nultočku $\alpha_1 \in L$ a polinom $Q^\sigma$ ima nultočku $\beta_1 \in L'$. Prema teoremu 4.10. postoji izomorfizam $\sigma_1 : K(\alpha_1) \to K'(\beta_1)$ takav da je $\sigma_1|K = \sigma$ i $\sigma_1(\alpha_1) = \beta_1$. Tada je $P = (X - \alpha_1)R$ za neki polinom $R \in K(\alpha_1)[X]$. Primijenimo li $\sigma_1$ na sve koeficijente u toj jednakosti, dobivamo jednakost $P^\sigma = (X - \beta_1)R^{\sigma_1}$ u prstenu $K'(\beta_1)[X]$. Tada je $L$ polje razlaganja za polinom $R$ nad poljem $K(\alpha_1)$ i $L'$ je polje razlaganja za polinom $R^{\sigma_1}$ nad poljem $K'(\beta_1)$. Po pretpostavci indukcije $\sigma_1$ se može proširiti do traženog izomorfizma $\varphi : L \to L'$, a kako je $\sigma_1|K = \sigma$, to je i $\varphi|K = \sigma$.

## 4.3 Konačna polja

U ovom ćemo odjeljku iskoristiti rezultate o poljima razlaganja kako bismo klasificirali sva konačna polja. Od takvih do sada znamo za polja $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$, gdje je $p \in \mathbb{N}$ prost broj.

Neka je $K$ bilo koje polje. Jedinicu u polju $K$ označimo sa $1_K$, a nulu sa $0_K$. Promatramo sada preslikavanje $\varphi : \mathbb{Z} \to K$ definirano na sljedeći način:

$$\varphi(0) = 0_K, \qquad \varphi(1) = 1_K, \qquad \varphi(n) = \underbrace{1_K + \cdots + 1_K}_{n} \quad \text{ako je} \quad n \in \mathbb{N},\ n \geq 2,$$

$$\varphi(n) = -\varphi(-n) \quad \text{ako je} \quad n \in \mathbb{Z}, \quad n < 0.$$

Lako se vidi da je $\varphi$ homomorfizam prstena $\mathbb{Z}$ u polje $K$. Njegova jezgra je ideal u prstenu $\mathbb{Z}$. Ako je ta jezgra $\{0\}$, tj. ako je $\varphi$ monomorfizam, tada $\mathbb{Z}$ možemo identificirati sa potprstenom $\varphi(\mathbb{Z})$ tako na 1 identificiramo sa $1_K$. U tom slučaju se i polje razlomaka $\mathbb{Q}$ integralne domene $\mathbb{Z}$ identificira s potpoljem od $K$. U tom slučaju kažemo da je $K$ **polje karakteristike** 0, a $\mathbb{Q}$ je najmanje potpolje od $K$ i zove se **prosto potpolje** polja $K$.

Ako je jezgra homomorfizma $\varphi$ različita od $\{0\}$, tj. ako $\varphi$ nije monomorfizam, što je nužno u slučaju da je polje $K$ konačno, onda znamo da je jezgra oblika

$$\operatorname{Ker}\varphi = p\mathbb{Z} = \{m \in \mathbb{Z};\ p|m\} = \{kp;\ k \in \mathbb{Z}\}$$

za neki $p \in \mathbb{N}$. Naravno, mora biti $n \geq 2$ jer je $\varphi(1) = 1_K \neq 0_K$, dakle, $\varphi \neq 0$. Prema teoremu 3.1. tada je sa

$$\Phi(m + p\mathbb{Z}) = \varphi(m), \qquad m \in \mathbb{Z},$$

definiran izomorfizam kvocijentnog prstena $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ na sliku $K_p = \varphi(\mathbb{Z})$ homomorfizma $\varphi$. Kako je prsten $\mathbb{Z}_p$ izomorfan potprstenu polja, slijedi da je $\mathbb{Z}_p$ integralna domena, a tada znamo da je nužno $p$ prost broj. No za prost broj $p$ je $\mathbb{Z}_p$ ne samo integralna domena, nego polje. Ono je izomorfno s najmanjim potpoljem $K_p$ polja $K$, pa se s njim može identificirati. U tom slučaju kažemo da je $K$ **polje karakteristike** $p$, a $K_p = \mathbb{Z}_p$ je najmanje potpolje od $K$ i zove se **prosto potpolje** polja $K$.

Ako je $K$ konačno polje, njegova je karakteristika neki prost broj $p$. Tada $K$ sadrži kao prosto potpolje polje $\mathbb{Z}_p$ sa $p$ elemenata. Naravno, $K$ je konačno proširenje polja $\mathbb{Z}_p$. Označimo sa $n = [K : \mathbb{Z}_p]$ stupanj tog proširenja. To znači da je $K$ $n-$dimenzionalni vektorski prostor nad konačnim poljem $\mathbb{Z}_p$ sa $p$ elemenata. Izaberemi li neku bazu $\{e_1, \ldots, e_n\}$ od $K$ nad $\mathbb{Z}_p$, onda je

$$K = \{a_1e_1 + \cdots + a_ne_n;\ a_1, \ldots, a_n \in \mathbb{Z}_p\}.$$

Odatle se vidi da polje $K$ ima $p^n$ elemenata. Zaključujemo da je za svako konačno polje $K$ broj elemenata $|K|$ jednak $p^n$ za neki prost broj $p$ (to je upravo karakteristika polja $K$) i neki prirodan broj $n$.

**Teorem 4.12.** *Za svaki prost broj $p$ i svaki prirodan broj $n$ postoji do na izomorfizam jedinstveno polje sa $p^n$ elemenata. To je polje razlaganja za polinom $X^{p^n} - X \in \mathbb{Z}_p[X]$ nad njegovim prostim potpoljem $\mathbb{Z}_p$.*

Ako je $q = p^n$, uobičajeno je da se polje iz teorema 4.12. označava sa $\mathbb{F}_q$. Teorem tvrdi da polje $\mathbb{F}_q$ postoji i da je jedinstveno do na izomorfizam. Ta se polja katkada zovu **Galoisova polja** po francuskom matematičaru Évariste Galois (1811.−1832.)

Prije dokaza teorema 4.12. treba nam određena priprema. Prije svega, za bilo koji polinom $P \in K[X]$ nad nekim poljem $K$ definiramo njegovu **derivaciju** $P' \in K[X]$, na način da preslikavanje $P \mapsto P'$, koje se zove **deriviranje polinoma**, bude $K-$linearno i da $X^n \mapsto nX^{n-1}$. Dakle, ako je

$$P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n = \sum_{k=0}^{n} a_kX^k \in K[X],$$

onda je

$$P' = a_1 + 2a_2X + \cdots + na_nX^{n-1} = \sum_{k=1}^{n} ka_kX^{k-1} = \sum_{k=0}^{n-1}(k+1)a_{k+1}X^k.$$

**Propozicija 4.1.** *Ako su $P, Q, R \in K[X]$ i $P = QR$, onda je $P' = Q'R + QR'$.*

**Dokaz:** Budući da je deriviranje $P \mapsto P'$ $K-$linearno, dovoljno je jednakost dokazati u slučaju $Q = X^n$, $R = X^m$ i $P = QR = X^{n+m}$. No tada je

$$P' = (n+m)X^{n+m-1} = nX^{n-1}X^m + mX^nX^{m-1} = Q'R + QR'.$$

**Korolar 4.3.** *Ako je $n \in \mathbb{N}$, $a \in K$ i $P = (X-a)^n$, onda je $P' = n(X-a)^{n-1}$.*

**Dokaz:** Tvrdnja slijedi neposredno iz propozicije 4.1. indukcijom u odnosu na $n$, jer je $(X-a)' = 1$.

**Korolar 4.4.** *Neka je $a \in K$. Ako je polinom $P \in K[X]$ djeljiv s polinomom $(X-a)^2$, onda je $P(a) = P'(a) = 0$.*

**Dokaz:** Možemo pisati $P = (X-a)^2Q$, za neki $Q \in K[X]$. Očito je $P(a) = 0$. Deriviramo li tu jednakost, zbog propozicije 4.1. i korolara 4.3. nalazimo

$$P' = 2(X-a)Q + (X-a)^2Q' \qquad \Longrightarrow \qquad P'(a) = 0.$$

**Teorem 4.13.** *Neka je $p$ prost broj i $K$ polje karakteristike $p$. Tada je preslikavanje $\varphi : K \to K$, definirano sa $\varphi(x) = x^p$, $x \in K$, monomorfizam polja $K$ u samoga sebe. Ako je $K$ konačno polje, $\varphi$ je* **automorfizam** *od $K$, odnosno, izomorfizama polja $K$ na samoga sebe.*

**Dokaz:** Očito je

$$\varphi(xy) = (xy)^p = x^py^p = \varphi(x)\varphi(y).$$

Nadalje, primijetimo da je binomni koeficijent $\binom{p}{j}$ za $1 \leq j \leq p-1$ djeljiv sa $p$. To znači da u polju $K$ množenje sa $\binom{p}{j}$ daje nulu. Prema tome,

$$\varphi(x+y) = (x+y)^p = \sum_{j=0}^{p} \binom{p}{j} x^jy^{p-1} = x^p + y^p = \varphi(x) + \varphi(y).$$

Time je dokazano da je $\varphi$ homomorfizam $K$ u $K$, dakle, monomorfizam jer se radi o polju. No ukoliko je polje $K$ konačno, svaka injekcija $K$ u $K$ je i surjekcija. Dakle, u tom je slučaju $\varphi$ automorfizam od $K$.

Preslikavanje $x \mapsto x^p$ iz teorema 4.13. obično se zove **Frobeniusovo preslikavanje**.

**Dokaz jedinstvenosti u teoremu 4.12.** Neka je $K$ konačno polje karakteristike $p$ i neka je $K_p \simeq \mathbb{Z}_p$ njegovo prosto potpolje. Znamo da je tada broj elemenata polja $K$ jednak $q = p^n$ za neki

$n \in \mathbb{N}$. Multiplikativna grupa $K^* = K \setminus \{0\}$ je reda $q-1$, pa svaki element $x \in K^*$ zadovoljava $x^{q-1} = 1$. Odatle slijedi da je $x^q = x \ \forall x \in K$. Formiramo li polinom $P = X^q - X \in K_p[X]$, vidimo da je svaki element polja $K$ nultočka tog polinoma. Dakle, ako je $K = \{a_1, a_2, \ldots, a_q\}$, imamo

$$P = X^q - X = (X - a_1)(X - a_2) \cdots (X - a_q).$$

Prema tome, $K$ je polje razlaganja za polinom $P = X^q - X$ nad poljem $K_p$. Sada iz teorema 4.11. slijedi jedinstvenost polja $K$ do na izomorfizam.

**Dokaz egzistencije u teoremu 4.12.** Neka je zadan $q = p^n$. Definiramo $K$ kao polje razlaganja polinoma $P = X^q - X$ nad prostim poljem $\mathbb{Z}_p$. Naravno, budući da je $K$ proširenje polja $\mathbb{Z}_p$, ono ima karakteristiku $p$. Po definiciji polja razlaganja slijedi da za neke $a_1, a_2, \ldots, a_q \in K$ vrijedi

$$P = X^q - X = (X - a_1)(X - a_2) \cdots (X - a_q), \qquad K = \mathbb{Z}_p(a_1, a_2, \ldots, a_q).$$

Promatrajmo sada preslikavanje $\psi : K \to K$ definirano sa $\varphi(x) = x^q$, $x \in K$. Budući da je $q = p^n$, to je preslikavanje kompozicija $n$ Frobeniusovih preslikavanja, dakle, $\psi$ je monomorfizam polja $K$ u samoga sebe. No tada je

$$L = \{x \in K;\ \psi(x) = x\}$$

potpolje od $K$. Element $x \in K$ se nalazi u potpolju $L$ ako i samo ako je $x^q = x$, odnosno, ako i samo ako je $x$ nultočka polinoma $P = X^q - X$. Slijedi da je $L = \{a_1, a_2, \ldots, a_q\}$. No kako je $K = \mathbb{Z}_p(a_1, a_2, \ldots, a_q)$, slijedi da je $L = K$. Dokaz egzistencije će biti potpun ako pokažemo da su su svi elementi $a_j$ međusobno različiti, tj. ako polje $K$ stvarno ima $q$ elemenata. Pretpostavimo da nije tako. To znači da polinom $P$ koji je stupnja $q$ ima u svom polju razlaganja manje od $q$ nultočaka. To onda povlači da je za neki $a \in K$ polinom $P = X^q - X$ djeljiva sa $(X - a)^2$. Prema korolaru 4.4. tada je $a$ nultočka derivacije $P'$. Međutim, $P' = qX^{q-1} - 1$, a kako je polje $K$ karakteristike $p$, množenje sa $p$, dakle, i sa $q = p^n$, daje nulu. To znači da je $P' = -1$, a to je konstantni polinom $\neq 0$, pa on uopće nema nultočaka. Ova kontradikcija pokazuje da su sve nultočke polinoma $P = X^q - X$ jednostruke, tj. da ih stvarno ima ukupno $q$.

**Korolar 4.5.** *Neka su $q, r \in \mathbb{N}$, $2 \leq q \leq r$. Polje $\mathbb{F}_q$ izomorfno je potpolju polja $\mathbb{F}_r$ ako i samo ako je $r = q^n$ za neki prirodan broj $n$.*

**Dokaz:** Ako je polje $\mathbb{F}_q$ izomorfno potpolju polja $\mathbb{F}_r$, onda je $\mathbb{F}_r$ vektorski prostor nad poljem $\mathbb{F}_q$. Ako je njegova dimenzija jednaka $n$, onda je $r = q^n$.

Pretpostavimo sada da je $r = q^n$ za neki $n \in \mathbb{N}$. Tada je $\mathbb{F}_r$ polje razlaganja polinoma $X^{q^n} - X$ nad prostim potpoljem $\mathbb{Z}_p$. Promatrajmo sada polinom $P = X^q - X$ i neka je $L$ skup svih njegovih nultočaka u polju $K$ :

$$L = \{x \in K;\ x^q = x\}$$

Budući da je $x \mapsto x^q$ kompozicija Frobeniusovih preslikavanja, to je $L$ potpolje od $K$.

Stavimo

$$k = q - 1 \qquad \text{i} \qquad \ell = \frac{q^n - 1}{q - 1} = q^{n-1} + q^{n-2} + \cdots + q + 1.$$

Tada je $k\ell = q^n - 1$, pa imamo

$$X^{q^n - 1} - 1 = X^{k\ell} - 1 = \left(X^k\right)^\ell - 1 = (X^k - 1)(X^{(\ell-1)k} + X^{(\ell-2)k} + \cdots + X^k + 1).$$

Pomnožimo li tu jednakost sa $X$ vidimo da je polinom $X^{q^n} - X$ djeljiv s polinomom $X^{k+1} - X = X^q - X$. Budući da se polinom $X^{q^n} - X$ razlaže nad poljem $\mathbb{F}_r$ i ima sve nultočke jednostruke, isto vrijedi i za polinom $X^q - X$. To znači da polinom $X^q - X$ ima u polju $K$ točno $q$ nultočaka. To pokazuje da potpolje $L$ polja $K$ ima $q$ elemenata. Stoga je po teoremu 4.12. polje $\mathbb{F}_q$ izomorfno potpolju $L$ polja $\mathbb{F}_r$.

## 4.4 Geometrijske konstrukcije pomoću ravnala i šestara

Konstrukcija pomoću ravnala je konstrukcija pravca kroz zadane dvije točke u ravnini. Konstrukcija pomoću šestara je konstrukcija kružnice u ravnini sa središtem u nekoj zadanoj točki i s radijusom jednakim udaljenosti između neke dvije zadane točke. Definiciju možemo formalizirati na sljedeći način. Neka je $S$ neki skup točaka u ravnini $M$ i $|S| \geq 2$. Kažemo da je neka točka $P$ ravnine $M$ **neposredno konstruktibilna** iz skupa $S$, ako je ona sjecište dvaju različitih pravaca od kojih svaki prolazi dvjema točkama iz $S$, ili je $P$ jedno od sjecišta pravca koji prolazi dvjema točkama iz $S$ i kružnice čije je središte neka točka iz $S$ a radijus je udaljenost nekih dviju točaka iz $S$, ili je $P$ jedno od sjecišta dviju različitih kružnica čija su središta točke iz $S$ a radijusi su udaljenosti nekih točaka iz $S$. Za točku $P$ ravnine $M$ kažemo da je **konstruktibilna** iz skupa $S$, ako postoje točke $P_1, \ldots, P_n$ takve da je $P_n = P$ i da je za svaki $j \in \{1, \ldots, n\}$ točka $P_j$ neposredno konstruktibilna iz skupa $S \cup \{P_i;\ 1 \leq i < j\}$.

Poznata su tri problema koji su od antičkog doba bili slavni i ostali neriješeni sve do XIX. stoljeća:

(1) **Duplikacija kocke.** Može li se duplicirati kocka, tj. može li se konstruirati stranica kocke čiji će volumen biti dva puta veći nego volumen zadane kocke?

(2) **Trisekcija kuta.** Mogu li se konstruirati dva pravca koji će podijeliti zadani kut u ravnini u tri jednaka dijela?

(3) **Kvadratura kruga.** Može li se konstruirati kvadrat koji će imati površinu jednaku površini zadanog kruga?

Prvi korak u rješavanju problema geometrijske konstruktibilnosti jest da se problem algebraizira. Ako su nam zadane neke dvije točke u ravnini, možemo izabrati Kartezijev koordinatni sustav u ravnini u odnosu na koji te dvije točke imaju koordinate $(0,0)$ i $(1,0)$. Sve točke ravnine tada su zadane s po dvije Kartezijeve koordinate, a time su određene i sve udaljenosti. S druge strane, svaku udaljenost možemo nanijeti kao točku na pozitivnom ili negativnom dijelu $x-$osi i $x-$koordinata je upravo $\pm$udaljenost od točke $(0,0)$. Postavlja se pitanje koje su sve točke $x-$osi konstruktibilne iz točaka $(0,0)$ i $(1,0)$.

Neka je $\mathcal{C}$ skup svih konstruktibilnih $x-$koordinata. Očito skup $\mathcal{C}$ sadrži 0 i 1. Nadalje, ako su $x, y \in \mathcal{C}$, onda su i $x + y \in \mathcal{C}$ i $x - y \in \mathcal{C}$; da to uvidimo čak i ne trebamo ravnalo, nego samo šestar. Neka su $a, b, c \in \mathcal{C}$ brojevi veći od nule. Konstruirajmo sada bilo koji šiljasti kut u ravnini $-$ tj. dvije zrake $p$ i $q$ koje imaju isti vrh $P$ i kut među njima je šiljast. Neka je $A$ točka na zraci $p$ čija je udaljenost od $P$ jednaka $a$. Neka je $B$ točka na zraci $q$ čija je udaljenost od $P$ jednaka $b$. Napokon, neka je $C$ točka na zraci $p$ čija je udaljenost od točke $P$ jednaka $a + c$; dakle, udaljenost od $C$ do $A$ je jednaka je $c$. Sada konstruiramo pravac kroz točku $C$ koji je paralelan s pravcem kroz točke $A$ i $B$. Neka je $D$ sjecište tog pravca sa zrakom $q$ i $d$ udaljenost između točaka $B$ i $D$. Dakle, $d \in \mathcal{C}$. Međutim, iz poučka o sličnosti trokutova slijedi da je

$$\frac{a}{b} = \frac{c}{d} \qquad \Longrightarrow \qquad d = \frac{bc}{a}.$$

Uzmemo li $a = 1$, vidimo da je $bc \in \mathcal{C}$. Ako umjesto toga uzmemo $c = 1$, vidimo da je kvocijent $b/a \in \mathcal{C}$. Budući da je $-\mathcal{C} = \mathcal{C}$, vidimo da je $\mathcal{C}$ potpolje polja $\mathbb{R}$ realnih brojeva. Naravno, ono sadrži polje $\mathbb{Q}$ racionalnih brojeva. Nadalje, konstrukcija pomoću pravokutnog trokuta pokazuje da vrijedi

$$a \in \mathcal{C}, \quad a > 0 \qquad \Longrightarrow \qquad \sqrt{a} \in \mathcal{C}.$$

Naime, ako je jedna od kateta pravokutnog trokuta duljine $c$ i ako su $a$ i $b$ duljine dvaju dijelova hipotenuze dobivenih spuštanjem okomice iz suprotnog vrha, onda je $c^2 = ab$, dakle, $c = \sqrt{ab}$. Ako

izaberemo $b = 1$, vidimo da vrijedi gornja implikacija. Time je dokazana prva tvrdnja u sljedećem teoremu:

**Teorem 4.14.** *Skup $\mathcal{C}$ $x-$koordinata koje su konstruktibilne iz $x = 1$ i $x = 0$ je potpolje polja $\mathbb{R}$ realnih brojeva takvo da je $\sqrt{a} \in \mathcal{C}$ $\forall a \in \mathcal{C} \cap \mathbb{R}_+$. Obratno, elementi od $\mathcal{C}$ su točno oni realni brojevi koji leže u nekom od potpolja $K_n$ polja $\mathbb{R}$ oblika*

$$K_0 = \mathbb{Q}, \quad K_1 = \mathbb{Q}(\sqrt{a_0}), \quad K_2 = K_1(\sqrt{a_1}), \quad \ldots\ldots, \quad K_n = K_{n-1}(\sqrt{a_{n-1}}),$$

*pri čemu je $a_j \in K_j \cap \mathbb{R}_+$ za svaki $j = 0, 1, \ldots, n-1$.*

**Dokaz druge tvrdnje:** Pretpostavimo da imamo polje $K = K_n$ opisanog tipa. Mogućnosti za dobivanje nove konstruktibilne točke polazeći od $K$ dolaze od tri situacije: presjecište dvaju pravaca od koji svaki prolazi nekim točkama s koordinatama iz $K$; presjecište pravca i kruž nice od kojih su oboje određeni pomoću podataka iz $K$; presjecište dviju kružnica, od kojih su obje određene pomoću podataka iz $K$.

U slučaju prsjecišta dvaju pravaca, svaki od njih ima jednadžbu oblika $ax + by = c$ za neke $a, b, c \in K$. Presjecište je tada točka $(x, y) \in K \times K$. Dakle, u tom slučaju uopće ne treba povećavati polje $K$.

U slučaju presjecišta pravca i kružnice, pravac ima jednadžbu $ax + by = c$ za neke $a, b, c \in K$, a kružnica jednadžbu oblika $(x - h)^2 + (y - k)^2 = r^2$, $h, k, r \in K$. Uvrstimo jednadžbu pravca u jednadžbu kružnice, jednu od varijabli $x$ ili $y$ možemo eliminirati, a za drugu dobivamo kvadratnu jednadžbu koja ima realne nultočke, jer se po pretpostavci pravac i kružnica sijeku. To znači da je diskriminanta te kvadratne jednadžbe $\geq 0$. Slijedi da su $x, y \in K(\sqrt{\ell})$ za neli $\ell \in K \cap \mathbb{R}_+$.

U slučaju presjecišta dviju kružnica, možemo uzeti da su njihove jednadžbe

$$x^2 + y^2 = r^2 \qquad \text{i} \qquad (x - h)^2 + (y - k)^2 = s^2, \qquad r, h, k, s \in K.$$

Oduzimanjem dobivamo

$$2hx + 2ky = h^2 + k^2 - s^2 + r^2.$$

No to je jednadžba pravca, pa sa kružnicom $x^2 + y^2 = r^2$ opet dolazimo na prethodni slučaj.

Zaključak je da svaka nova neposredna konstrukcija ravnalom i šestarom vodi od polja $K$ na polje oblika $K(\sqrt{\ell})$ za neki $\ell \in K \cap \mathbb{R}_+$. Time je teorem dokazan.

Da bismo primijenili teorem da dokažemo nemogućnost konstrukcija u tri navedena antička problema, primijetimo da je stupanj proširenja $[K_j : K_{j-1}]$ za polja iz teorema 4.14. ili 1 ili 2. Prema tome, svaki element od $\mathcal{C}$ leži u nekom konačnom proširenju pod $\mathbb{Q}$ stupnja $2^k$ za neki $k \in \mathbb{N}$.

Problem duplikacije kocke svodi se na pitanje konstruktibilnosti broja $\sqrt[3]{2}$. Kad bi broj $\sqrt[3]{2}$ bio sadržan u nekom $K_n$ iz teorema 4.14. onda bi bilo $\mathbb{Q}(\sqrt[3]{2}) \subseteq K_n$. Ako je $[K_n : \mathbb{Q}] = 2^k$, onda imamo

$$2^k = [K_n : \mathbb{Q}] = [K_n : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3[K_n : \mathbb{Q}(\sqrt[3]{2})].$$

To bi značilo da je broj $2^k$ djeljiv s 3 i došli smo do kontradikcije.

Za problem trisekcije kuta, ona jest moguća za neke kutove, npr. za ispruženi ili pravi kut, ali nije moguća npr. za kut od $60^\text{o}$. Trisekcija tog kuta znači konstrukciju kuta od $20^\text{o}$, a to se svodi na konstrukciju broja $\cos 20^\text{o}$. Tada je $\sin 20^\text{o} = \sqrt{1 - \cos^2 20^\text{o}}$. Izvest ćemo jednu jednadžbu koju zadovoljava broj $x = \cos 20^\text{o}$, polazeći od Moivreove formule

$$(\cos 20^\text{o} + i \sin 20^\text{o})^3 = \cos 60^\text{o} + i \sin 60^\text{o} = \frac{1}{2} + i\frac{\sqrt{3}}{2}.$$

Izjednačimo realne dijelove lijeve i desne strane i uvrstimo $\cos 20^o = x$, dakle, $\sin^2 20^o = 1 - x^2$. Dolazimo do

$$x^3 - 3x(1 - x^2) = \frac{1}{2} \qquad \Longrightarrow \qquad 8x^3 - 6x - 1 = 0.$$

Pokazuje se da je polinom $8X^3 - 6X - 1$ ireducibilan nad $\mathbb{Q}$. To znači da je to minimalni polinom nad $\mathbb{Q}$ za svaku svoju nultočku, pa slijedi da je $[\mathbb{Q}(x) : \mathbb{Q}] = 3$. Stoga iz pretpostavke konstruktibilnosti broja $x$ dolazimo do iste kontradikcije kao i kod duplikacije kocke.

Napokon, problem kvadrature kruga svodi se na pitanje konstruktibilnosti broja $\sqrt{\pi}$. Međutim, dokazano je da broj $\pi$ uopće nije algebarski nego transcendentan, pa slijedi da je i $\sqrt{\pi}$ transcendentan, dakle, sigurno nije konstruktibilan.

Četvrti važan problem, koji se dugo proučavao je pitanje za koje je prirodne brojeve $n$ konstruktibilan tzv. *regularan poligon* sa $n$ stranica ili *regularan $n-$gon*. To je poligon sa $n$ stranica jednake duljine koji ima opisanu kružnicu i ona je radijusa 1. Ta je konstrukcija jednostavna ako je $n = 2^k$ ili $n = 3 \cdot 2^k$ za neki $k$. Nadalje, Euklid je pronašao konstrukciju za $n = 5$. Međutim, konstrukcija je nemoguća npr. za $n = 9$. Doista, u slučaju konstruktibilnosti za $n = 9$, središnji kut bilo koje stranice ima mjeru $40^o$, a tada bi i $20^o$ bilo konstruktibilno, što nije istina.

Zanimljivo i neočekivano rješenje ovog problema dao je Gauss i to ćemo sada opisati. Prije svega **Fermatov broj** je svaki prirodan broj oblika $2^{2^n}+1$. Ako je Fematov broj ujedno prost broj, zovemo ga **Fermatov prost broj**. Fermatovi brojevi za $n = 0, 1, 2, 3, 4$ su $3, 5, 17, 257, 65537$ i svi su oni prosti. Do danas nije poznat nijedan veći Fermatov prost broj, iako se za mnoge Fermatove brojeve zna da nisu prosti. Npr. za $n = 5$ je

$$2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417.$$

**Teorem 4.15.** (**Gauss**) *Regularan $n-$gon je konstruktibilan ako i samo ako je produkt različitih Fermatovih prostih brojeva i neke potencije broja* 2.

U stvari, u objavi tog rezultata 1801. godine Gauss je ustvrdio nužnost i dovoljnost gornjeg uvjeta, ali napisao je samo dokaz dovoljnosti. Dokaz nužnosti pojavio se prvi put u članku matematičara Pierre−Laurent Wantzela 1837. godine.

## 4.5 Algebarski zatvarač

Proširenje $L$ polja $K$ zove se **algebarski zatvarač polja** $K$ ili **algebarsko zatvorenje polja** $K$ ako je to proširenje algebarsko nad $K$ i ako je polje $L$ algebarski zatvoreno. Npr. $\mathbb{C}$ je algebarski zatvarač polja $\mathbb{R}$.

Uočimo prije svega jednu jednostavnu ali vrlo korisnu činjenicu o algebarskim proširenjima:

**Teorem 4.16.** *Neka je $L$ proširenje polja $K$ i $M$ proširenje polja $L$. Tada je $M$ algebarsko proširenje polja $K$ ako i samo ako je $M$ algebarsko proširenje polja $L$ i $L$ je algebarsko proširenje polja $K$.*

**Dokaz:** Pretpostavimo da je $M$ algebarsko proširenje polja $K$. Budući da je $L \subseteq M$, očito je svaki element polja $L$ algebarski nad $K$. Dakle, polje $L$ je algebarsko proširenje polja $K$. Nadalje, ako je $\alpha \in M$, onda je element $\alpha$ algebarski nad $K$, što znači da postoji netrivijalni polinom $P \in K[X]$ takav da je $P(\alpha) = 0$. No kako je $K \subseteq L$, vrijedi $K[X] \subseteq L[X]$, dakle je $P \in L[X]$. Zaključujemo da je element $\alpha$ algebarski nad $L$. Kako je element $\alpha \in M$ bio proizvoljan, slijedi da je $M$ algebarsko proširenje polja $L$.

Pretpostavimo sada da je $L$ algebarsko proširenje polja $K$ i da je $M$ algebarsko proširenje polja $L$. Neka je $\alpha \in M$. Tada postoji netrivijalni polinom $P \in L[X]$ takav da je $P(\alpha) = 0$. Neka su $\beta_0, \ldots, \beta_n \in L$ koeficijenti polinoma $P$ i neka je $N = K(\beta_0, \ldots, \beta_n)$. Prema teoremu 4.5. $N$ je konačno proširenje polja $K$. Nadalje, vrijedi $P \in N[X]$, dakle, element $\alpha$ je algebarski nad $N$. Prema teoremu 4.2. $N(\alpha)$ je konačno proširenje polja $N$. Sada iz teorema 4.4. slijedi da je $N(\alpha)$ konačno proširenje polja $K$. Ponovnom primjenom teorema 4.5. zaključujemo da je $N(\alpha)$ algebarsko proširenje polja $K$, dakle, element $\alpha$ je algebarski nad $K$. Kako je $\alpha \in M$ bio proizvoljan, zaključujemo da je $M$ algebarsko proširenje polja $K$.

**Teorem 4.17.** *Polje $K$ je algebarski zatvoreno ako i samo ako ne postoji algebarsko proširenje $L$ polja $K$ koje je netrivijalno, tj. različito od $K$.*

**Dokaz:** Neka je $L$ algebarsko proširenje algebarski zatvorenog polja $K$ i neka je $\alpha \in L$. Tada je element $\alpha$ algebarski nad $K$, tj. postoji netrivijalan polinom $P \in K[X]$ takav da je $P(\alpha) = 0$. Neka je $n = \deg P$. Budući da je polje $K$ algebarski zatvoreno, polinom $P$ se razlaže nad $K$, tj. postoje $b, a_1, \ldots, a_n \in K$ takvi da je $P = b(X - a_1) \cdots (X - a_n)$. Kako je $b \neq 0$, iz $P(\alpha) = 0$ slijedi $\alpha \in \{a_1, \ldots, a_n\}$, dakle, $\alpha \in K$. Kako je $\alpha$ bio proizvoljan element polja $L$, slijedi $L = K$.

Pretpostavimo sada da ne postoji algebarsko proširenje $L \neq K$ polja $K$. Neka je $P \in K[X]$ nekonstantni polinom. Tada prema teoremu 4.1. postoje proširenje $L$ polja $K$ i element $\alpha \in L$ takvi da je $P(\alpha) = 0$. Tada je element $\alpha$ algebarski nad $K$, pa slijedi da je $K(\alpha)$ konačno, dakle i algebarsko, proširenje od $K$. Po pretpostavci je tada $K(\alpha) = K$, dakle, $\alpha \in K$. Time je dokazano da svaki nekonstantni polinom $P \in K[X]$ ima nultočku u polju $K$, odnosno, polje $K$ je algebarski zatvoreno.

Sljedeći teorem, čiji je dokaz u jednom dijelu sličan prethodnom, daje nam važan kriterij algebarske zatvorenosti algebarskog proširenja nekog polja.

**Teorem 4.18.** *Neka je $L$ algebarsko proširenje polja $K$. Ako se svaki nekonstantni polinom iz $K[X]$ razlaže nad $L$, polje $L$ je algebarski zatvoreno.*

**Dokaz:** Neka je $M$ algebarsko proširenje polja $L$ i neka je $\alpha \in M$. Prema teoremu 4.16. polje $M$ je algebarsko proširenje polja $K$, dakle, postoji netrivijalan $P \in K[X]$ takav da je $P(\alpha) = 0$. Po pretpostavci se polinom $P$ razlaže nad $L$, dakle, ako je $n = \deg P$, postoje $0 \neq a \in K$ i $\alpha_1, \ldots, \alpha_n \in L$ takvi da je $P = a(X - \alpha_1) \cdots (X - \alpha_n)$. Slijedi $0 = P(\alpha) = a(\alpha - \alpha_1) \cdots (\alpha - \alpha_n)$.

Kako je $a \neq 0$, vidimo da je $\alpha = \alpha_j$ za neki $j \in \{1, \ldots, n\}$, dakle, $\alpha \in L$. Kako je $\alpha$ bio proizvoljan element polja $M$, zaključujemo da je $M = L$. Sada iz teorema 4.17. slijedi da je polje $L$ algebarski zatvoreno.

Neka je sada $p$ prost broj i promatrajmo polje $\mathbb{F}_p = \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. Tada je skup $\mathbb{F}_p[X]$ prebrojivo beskonačan, tj. bijektivan sa $\mathbb{N}$. To znači da njegove elemente možemo numerirati prirodnim brojevima:

$$\mathbb{F}_p[X] = \{P_n;\ n \in \mathbb{N}\} = \{P_1, P_2, P_3, \ldots\}.$$

Stavimo $K_0 = \mathbb{F}_p$ i konstruirajmo induktivno polja $K_n$, $n \in \mathbb{N}$. Za $n \geq 1$ definiramo $K_n$ kao polje razlaganja za polinom $P_n$ nad poljem $K_{n-1}$. Tada je

$$K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_{n-1} \subseteq K_n \subseteq \cdots\cdots$$

rastući niz polja; naravno, možda ne striktno rastući jer se može dogoditi da se neki $P_n$ razlaže nad poljem $K_{n-1}$, a u tom je slučaju $K_n = K_{n-1}$. Neka je $\mathbb{K}_p$ unija svih tih polja $K_n$, $n \geq 0$. Ako su $x, y \in K$, onda postoji $n \in \mathbb{N}$ takav da su $x, y \in K_n$. No tada su $x \pm y, xy \in K_n \subseteq \mathbb{K}_p$. Dakle, $\mathbb{K}_p$ je unitalan prsten. Nadalje, ako je $x \in \mathbb{K}_p$ i $x \neq 0$, tada je $x \in K_n$ za neki $n$, pa postoji $y \in K_n \subseteq \mathbb{K}_p$ takav da je $xy = 1$. Dakle, $\mathbb{K}_p$ je polje.

Neka je $x \in \mathbb{K}_p$. Izaberimo $n \in \mathbb{N}$ tako da je $x \in K_n$. Polje $K_n$ je algebarsko proširenje polja $K_{n-1}$, a odatle indukcijom po $n$ pomoću teorema 4.16. zaključujemo da je $K_n$ algebarsko proširenje polja $K_0 = \mathbb{F}_p[X]$. Dakle, element $x$ je algebarski nad $\mathbb{F}_p$. Kako je $x$ bio proizvoljan element polja $\mathbb{K}_p$, zaključujemo da je polje $\mathbb{K}_p$ algebarsko proširenje polja $\mathbb{F}_p$.

Neka je sada $P \in \mathbb{F}_p[X]$. Tada je $P = P_n$ za neki $n \in \mathbb{N}$. Po konstrukciji polinom $P$ se razlaže nad poljem $K_n$, a kako je $K_n \subseteq \mathbb{K}_p$, polinom $P$ se razlaže nad poljem $\mathbb{K}_p$. Sada teorem 4.18. povlači da je polje $\mathbb{K}_p$ algebarski zatvoreno. Na taj način konstruirali smo algebarski zatvarač $\mathbb{K}_p$ konačnog polja $\mathbb{F}_p$. Polje $\mathbb{K}_p$ možemo shvaćati kao algebarski zatvarač svakog polja $\mathbb{F}_{p^n}$, $n \in \mathbb{N}$, zbog sljedećeg teorema:

**Teorem 4.19.** *Neka je $M$ algebarski zatvoreno polje i neka je $L$ algebarsko proširenje nekog polja $K$. Tada se svaki monomorfizam $\varphi : K \to M$ proširuje do monomorfizma $\psi : L \to M$.*

**Dokaz:** U ovom ćemo se dokazu poslužiti Zornovom lemom. Neka je $\mathcal{S}$ skup svih uređenih parova $(N, \psi)$, gdje je $N \subseteq L$ polje koje sadrži $K$, a $\psi$ je monomorfizam polja $N$ u polje $M$ takav da je $\psi|K = \varphi$. U skup $\mathcal{S}$ uvodimo relaciju $\leq$ na sljedeći način: za $(N, \psi), (N', \psi') \in \mathcal{S}$ pišemo $(N, \psi) \leq (N', \psi')$ ako i samo ako je $N \subseteq N'$ i $\psi'|N = \psi$. Lako se vidi da je $\leq$ relacija uređaja, dakle, $\mathcal{S}$ postaje parcijalno uređen skup. Vrijedi $\mathcal{S} \neq \emptyset$, jer je $(K, \varphi) \in \mathcal{S}$.

Dokažimo da $\mathcal{S}$ zadovoljava uvjet Zornove leme. Neka je $\mathcal{T}$ neprazan lanac u $\mathcal{S}$. Neka je $R$ unija svih polja $N$ takvih da je $(N, \psi) \in \mathcal{T}$ za neki $\psi$. Dokažimo da je $N$ potpolje polja $L$. Neka su $x, y \in R$. Kako je $\mathcal{T}$ lanac, postoji $(N, \psi) \in \mathcal{T}$ takav da su $x, y \in N$. Tada su $x \pm y, xy \in N \subseteq R$. Nadalje, ako je $x \neq 0$, on je invertibilan u $N$, dakle i u $R$. Time je dokazano da je $R$ potpolje od $L$. Naravno, vrijedi $K \subseteq R$, jer je $K \subseteq N$ za svaki $(N, \psi) \in \mathcal{T}$. Definirajmo sada preslikavanje $\chi : R \to M$ na sljedeći način: ako je $x \in R$, po definiciji $R$ možemo izabrati $(N, \psi) \in \mathcal{T}$ tako da je $x \in N$; tada stavimo $\chi(x) = \psi(x)$. Ta definicija ne ovisi o izboru para $(N, \psi) \in \mathcal{T}$ takvog da je $x \in N$. Doista, neka je i $(N', \psi') \in \mathcal{T}$ takav da je $x \in N'$. Kako je $\mathcal{T}$ lanac, vrijedi $(N, \psi) \leq (N', \psi')$ ili $(N', \psi') \leq (N, \psi)$. Uzmimo npr. da je $(N, \psi) \leq (N', \psi')$; druga mogućnost tretira se na isti način. Tada je $N \subseteq N'$ i $\psi'|N = \psi$. No tada je $\psi(x) = \psi'(x)$, a to je i trebalo dokazati. Neka su sada $x, y \in R$. Kako je $\mathcal{T}$ lanac, postoji $(N, \psi) \in \mathcal{T}$ takav da su $x, y \in N$. Tada su $x+y, xy, 1 \in N$, pa slijedi

$$\chi(x + y) = \psi(x + y) = \psi(x) + \psi(y) = \chi(x) + \chi(y);$$
$$\chi(xy) = \psi(xy) = \psi(x)\psi(y) = \chi(x)\chi(y); \qquad \chi(1) = \psi(1) = 1.$$

Dakle, $\chi : R \to M$ je unitalni homomorfizam polja, tj. monomorfizam po lemi 4.1. Iz definicije $\chi$ slijedi i $\chi|K = \varphi$. Dakle, $(R, \chi) \in \mathcal{S}$ i iz konstrukcije slijedi da je $(R, \chi)$ gornja međa lanca $\mathcal{T}$. Time smo dokazali da je svaki lanac u $\mathcal{S}$ odozgo omeđen, odnosno, ispunjen je uvjet Zornove leme.

Sada iz Zornove leme (teorem 3.6.) slijedi da u skupu $\mathcal{S}$ postoji barem jedan maksimalni element $(N, \psi)$. Dokazat ćemo sada da je $N = L$ i time će teorem biti dokazan. Neka je $x \in L$ i neka je $P \in N[X]$ minimalni polinom od $x$ nad $N$. Tada je polinom $P$ ireducibilan u prstenu $N[X]$. Budući da je $\psi$ izomorfizam polja $N$ na potpolje $\psi(N)$ polja $M$, slijedi da je polinom $P^\psi$ ireducibilan u prstenu $\psi(N)[X]$. Kako je polje $M$ algebarski zatvoreno, postoji $\alpha \in M$ takav da je $P^\psi(\alpha) = 0$. Sada iz teorema 4.10. slijedi da postoji (čak jedinstven) izomorfizam $\chi$ polja $N(x)$ na polje $\psi(N)(\alpha)$ takav da je $\chi|N = \psi$ i $\chi(x) = \alpha$. Tada vrijedi $\chi|K = \psi|K = \varphi$, dakle, je $(N(x), \chi) \in \mathcal{S}$. Slijedi $(N, \psi) \leq (N(x), \chi)$, a kako je $(N, \psi)$ maksimalni element od $\mathcal{S}$, zaključujemo da je $(N(x), \chi) = (N, \psi)$. Dakle, $N(x) = N$, odnosno, $x \in N$. Kako je $x$ bio proizvoljan element polja $L$, slijedi $N = L$.

Na taj način vidimo da svako konačno polje ima algebarski zatvarač. U stvari, to vrijedi ne samo za konačno nego i za svako polje. Štoviše, algebarski zatvarač je do na izomorfizam jedinstven:

**Teorem 4.20.** (**Steinitz**) *Svako polje $K$ ima algebarski zatvarač. Nadalje, ako su $L$ i $L'$ algebarski zatvarači od $K$, postoji izomorfizam polja $\psi : L' \to L$ takav da je $\psi|K = id_K$, tj. $\psi(x) = x \ \forall x \in K$.*

**Dokaz jedinstvenosti algebarskog zatvarača:** Neka su $L$ i $L'$ algebarski zatvarači polja $K$. Po teoremu 4.19. postoji monomorfizam $\psi : L \to L'$ takav da je $\psi|K = id_K$. Tada je $\psi(L)$ potpolje od $L'$ koje sadrži polje $K$ i koje je algebarski zatvoreno jer je $\psi$ izomorfizam polja $L$ na polje $\psi(L)$. Nadalje, $L'$ je algebarsko proširenje polja $K$, dakle, $L'$ je algebarsko proširenje polja $\psi(L)$. Prema teoremu 4.17. slijedi da je $\psi(L) = L'$. Prema tome, $\psi$ je izomorfizam polja $L$ na polje $L'$ takav da je $\psi|K = id_K$.

Egzistencija se dokazuje potpuno analogno konstrukciji algebarskog zatvarača konačnog polja, jedino što se sada umjesto obične indukcije koristi tzv. **transfinitna indukcija**. Mogućnost korištenja transfinitne indukcije izlazi iz tzv **Zermelovog aksioma dobrog uređenja** koji je ekvivalentan Zermelovom aksiomu izbora, dakle i Zornovoj lemi. Taj aksiom glasi:

*Na svakom skupu postoji relacija uređaja u odnosu na koju je taj skup dobro uređen.*

Pri tome kažemo da je parcijalno uređen skup $\mathcal{S}$ **dobro uređen** ako su ispunjena sljedeća dva uvjeta:

(*a*) $\mathcal{S}$ je lanac, tj. ako su $x, y \in \mathcal{S}$, onda je $x \leq y$ ili $y \leq x$.

(*b*) Svaki neprazan podskup $\mathcal{T} \subseteq \mathcal{S}$ ima najmanji element, tj. postoji $x \in \mathcal{T}$ takav da je $x \leq y$ $\forall y \in \mathcal{T}$.

Primijetimo da za svaki dobro uređen skup $\mathcal{S}$ vrijedi tzv. **princip transfinitne indukcije**:

*Neka je $\mathcal{T}$ neprazan podskup od $\mathcal{S}$ koji ima sljedeće svojstvo*:

$$x \in \mathcal{S}, \quad \{y \in \mathcal{S};\ y < x\} \subseteq \mathcal{T} \qquad \Longrightarrow \qquad x \in \mathcal{T}.$$

*Tada je $\mathcal{T} = \mathcal{S}$.*

Pri tome oznaka $y < x$ znači $y \leq x$ i $y \neq x$. Doista, pretpostavimo suprotno da je $\mathcal{T} \neq \mathcal{S}$. Tada je $\mathcal{S} \setminus \mathcal{T}$ neprazan podskup od $\mathcal{S}$ pa on ima najmanji element $x$. Sada $\{y \in \mathcal{S};\ y < x\} \cap (\mathcal{S} \setminus \mathcal{T}) = \emptyset$ znači da je $\{y \in \mathcal{S};\ y < x\} \subseteq \mathcal{T}$. Iz prepostavljenog svojstva skupa $\mathcal{T}$ slijedi da je $x \in \mathcal{T}$, što je, naravno, u kontradikciji s pretpostavkom $x \in \mathcal{S} \setminus \mathcal{T}$.

Neka je $\mathcal{S}$ dobro uređen skup. Neka je $x \in \mathcal{S}$ element koji nije najveći. Tada je skup $\{y \in \mathcal{S};\ x < y\}$ neprazan; njegov najmanji element zove se **sljedbenik** elementa $x$ i označava $x^+$. Ukoliko je $y \in \mathcal{S}$ takav da je $y^+ = x$, onda se $y$ zove **prethodnik** od $x$ i tada pišemo $y = x^-$. Najmanji element skupa $\mathcal{S}$ očito nema prethodnika, ali moguće je da postoje i drugi elementi skupa $\mathcal{S}$ koji nemaju svog prethodnika.

**Skica dokaza egzistencije algebarskog zatvarača:** Pomoću Zermelovog aksioma dobrog uređenja možemo pretpostaviti da je na skupu $K[X]$ definirana relacija uređaja u odnosu na koju je $K[X]$ dobro uređen. Neka je $P_0$ najmanji element od $K[X]$. Stavimo $K_{P_0} = K$, a pomoću transfinitne indukcije ćemo za svaki $P \in K[X]$ definirati algebarsko proširenje $K_P$ polja $K$ i to tako da je $K_P \subseteq K_Q$ ako su $P, Q \in K[X]$ i $P \leq Q$ :

(1) ako $P$ ima prethodnika $P^- \in K[X]$ i ako pretpostavimo da je proširenje $K_{P^-}$ već definirano, onda definiramo $K_P$ kao polje razlaganja polinoma $P$ nad poljem $K_{P^-}$;

(2) ako $P \neq P_0$ nema svog prethodnika u $K[X]$ i ako pretpostavimo da su proširenja $K_Q$ definirana $\forall Q < P$, i da za $Q \leq R < P$ vrijedi $K_Q \subseteq K_R$, onda se $K_P$ definira kao polje razlaganja polinoma $P$ nad poljem $\cup_{Q<P} K_Q$.

Tada se slično dokazu za konačno polje, samo korištenjem transfinitne umjesto obične matematičke indukcije, dokazuje da je unija

$$\bigcup_{P \in K[X]} K_P$$

algebarski zatvarač polja $K$.

# Poglavlje 5

# Galoisova teorija

## 5.1 Galoisova grupa proširenja

Ako su $K$ i $L$ polja, prema lemi 4.1. svaki netrivijalni homomorfizam prstenova $\varphi : K \to L$ je unitalni monomorfizam. U daljnjem će važnu će ulogu imati sljedeći netrivijalni teorem:

**Teorem 5.1.** (**Dedekindova lema**) *Neka su $K$ i $L$ polja i neka su $\varphi_1, \varphi_2, \ldots, \varphi_n : K \to L$ međusobno različiti monomorfizmi polja. Tada su $\varphi_1, \varphi_2, \ldots, \varphi_n$ linearno nezavisni nad poljem $L$.*

**Dokaz:** Pretpostavimo suprotno, tj. da postoje $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$, koji nisu svi jednaki nuli, takvi da je $\alpha_1\varphi_1 + \alpha_2\varphi_2 + \cdots + \alpha_n\varphi_n = 0$, tj. da vrijedi

$$\alpha_1\varphi_1(x) + \alpha_2\varphi_2(x) + \cdots + \alpha_n\varphi_n(x) = 0 \qquad \forall x \in K.$$

Pretpostavimo sada da smo izbor koeficijenata $\alpha_i$ napravili tako je broj indeksa $i \in \{1, 2, \ldots, n\}$, za koje je $\alpha_i \neq 0$, najmanji mogući. Označimo taj broj sa $r$. Naravno, $r \geq 2$. Promijenimo li sada na odgovarajući način numeraciju, možemo pretpostavljati da su $\alpha_{r+1} = \cdots = \alpha_n = 0$ i da je

$$\alpha_1\varphi_1(x) + \alpha_2\varphi_2(x) + \cdots + \alpha_r\varphi_r(x) = 0 \qquad \forall x \in K, \qquad \alpha_1 \neq 0,\ \alpha_2 \neq 0,\ \ldots,\ \alpha_r \neq 0. \tag{5.1}$$

Kako su $\varphi_1, \ldots, \varphi_n$ po pretpostavci međusobno različiti, posebno je $\varphi_1 \neq \varphi_r$. Prema tome, postoji $y \in K$ takav da je $\varphi_1(y) \neq \varphi_r(y)$. Jednakost (5.1) vrijedi za svaki $x \in K$, pa vrijedi i ako u nju umjesto $x$ uvrstimo $yx$ :

$$\alpha_1\varphi_1(yx) + \alpha_2\varphi_2(yx) + \cdots + \alpha_r\varphi_r(yx) = 0 \qquad \forall x \in K.$$

Uvažimo li činjenicu da su svi $\varphi_i$ homomorfizmi, iz gornje jednakosti dobivamo:

$$\alpha_1\varphi_1(y)\varphi_1(x) + \alpha_2\varphi_2(y)\varphi_2(x) + \cdots + \alpha_r\varphi_r(y)\varphi_r(x) = 0 \qquad \forall x \in K. \tag{5.2}$$

Pomožimo sada jednakost (5.1) sa $\varphi_r(y)$ i od tako dobivene jednakosti oduzmemo jednakost (5.2). Tada uz oznaku $\beta_j = \alpha_j[\varphi_r(y) - \varphi_j(y)]$ dobivamo

$$\beta_1\varphi_1(x) + \beta_2\varphi_2(x) + \cdots + \beta_{r-1}\varphi_{r-1}(x) = 0 \qquad \forall x \in K.$$

Imamo $\beta_1 = \alpha_1[\varphi_r(y) - \varphi_1(y)] \neq 0$, jer je $\alpha_1 \neq 0$ a $y \in K$ je bio izabran tako da bude $\varphi_1(y) \neq \varphi_r(y)$. Na taj način došli smo do kontradikcije sa svojstvom broja $r$. Ova kontradikcija pokazuje da je pretpostavka o linearnoj zavisnosti $\varphi_1, \varphi_2, \ldots, \varphi_n$ nad $L$ pogrešna. Time je teorem dokazan.

Neka je $K$ polje. **Automorfizam polja** $K$ je izomorfizam polja $K$ na samog sebe, dakle, bijekcija $\sigma : K \to K$ takva da je $\sigma(\alpha+\beta) = \sigma(\alpha)+\sigma(\beta)$ i $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$ $\forall \alpha, \beta \in K$. Skup svih automorfizama polja $K$ označavat ćemo sa $Aut(K)$.

Među primjerima grupa u odjeljku 1.2. naveli smo i tzv. grupu permutacija proizvoljnog nepraznog skupa $T$. To je skup $\left(T^T\right)^*$ svih bijekcija $f : T \to T$, a operacija u toj grupi je kompozicija. Kompozicija dvaju automorfizama polja $K$ ponovo je automorfizam:

$$\sigma, \tau \in Aut(K) \qquad \Longrightarrow \qquad \sigma \circ \tau \in Aut(K).$$

Nadalje, ako je $\sigma : K \to K$ automorfizam, onda je i inverzno preslikavanje $\sigma^{-1} : K \to K$ automorfizam:

$$\sigma \in Aut(K) \qquad \Longrightarrow \qquad \sigma^{-1} \in Aut(K).$$

Zaključujemo da je $Aut(K)$ podgrupa grupe permutacija $\left(K^K\right)^*$ skupa $K$. Prema tome, skup $Aut(K)$ svih automorfizama polja $K$ je grupa s obzirom na kompoziciju.

Neka su $L$ i $M$ proširenja polja $K$. Homomorfizam $\varphi : L \to M$, za koji vrijedi $\varphi(\alpha) = \alpha$, $\forall \alpha \in K$, tj. čija je restrikcija $\tau \,|\, K$ identiteta na $K$, zove se $K-$**homomorfizam**. To točno znači da je $\varphi$ linearan operator ako $L$ i $M$ promatramo kao vektorske prostore nad poljem $K$ :

$$\varphi(\alpha_1\lambda_1 + \alpha_2\lambda_2) = \varphi(\alpha_1)\varphi(\lambda_1) + \varphi(\alpha_2)\varphi(\lambda_2) = \alpha_1\varphi(\lambda_1) + \alpha_2\varphi(\lambda_2), \qquad \alpha_1, \alpha_2 \in K, \;\; \lambda_1, \lambda_2 \in L.$$

Neka je sada $L$ proširenje polja $K$. $K-$**automorfizam** polja $L$ je automorfizam $\sigma \in Aut(L)$ koji je $K-$homomorfrizam. Označimo sa $Aut_K(L)$ skup svih $K-$automorfizama polja $L$. Očito vrijedi:

$$\sigma, \tau \in Aut_K(L) \quad \Longrightarrow \quad \sigma \circ \tau \in Aut_K(L);$$

Također,

$$\sigma \in Aut_K(L) \quad \Longrightarrow \quad \sigma^{-1} \in Aut_K(L).$$

Dakle, $Aut_K(L)$ je podgrupa grupe $Aut(L)$. $Aut_K(L)$ zove se **Galoisova grupa proširenja** $L$ polja $K$. Za tu su grupu uobičajene i oznake $\mathrm{Gal}(L:K)$, $\mathrm{Gal}(L/K)$, $G(L:K)$ i $G(L/K)$.

Neka je sada $L$ polje i neka je $G$ bilo koja podgrupa grupe $Aut(L)$. Stavimo

$$L^G = \{\lambda \in L;\ \sigma(\lambda) = \lambda,\ \forall \sigma \in G\}.$$

Lako se vidi da vrijedi:

$$\lambda, \mu \in L^G \quad \Longrightarrow \quad \lambda \pm \mu, \lambda\mu \in L^G \qquad \text{i} \qquad \lambda \in L^G,\, \lambda \neq 0 \quad \Longrightarrow \quad \lambda^{-1} \in L^G.$$

Prema tome, $L^G$ je potpolje polja $L$.

**Teorem 5.2.** *Neka je $L$ polje i $G$ konačna podgrupa grupe $Aut(L)$. Tada je $\left[L : L^G\right] = |G|$, odnosno proširenje $L$ polja $L^G$ je konačno i stupanj mu je jednak redu konačne grupe $G$.*

**Dokaz:** Stavimo $|G| = n$ i neka je $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ pri čemu je $\sigma_1$ identiteta, odnosno, jedinica u grupi $G$.

(1) Pretpostavimo da je

$$\left[L : L^G\right] = m < n.$$

Neka je $\{\lambda_1, \lambda_2, \ldots, \lambda_m\}$ baza vektorskog prostora $L$ nad poljem $L^G$. Promatrajmo sada homogeni sustav od $m$ jednadžbi s $n$ nepoznanica $\mu_1, \mu_2, \ldots, \mu_n \in L$ :

$$\begin{aligned}
&\sigma_1(\lambda_1)\mu_1 + \sigma_2(\lambda_1)\mu_2 + \cdots + \sigma_n(\lambda_1)\mu_n = 0\\
&\sigma_1(\lambda_2)\mu_1 + \sigma_2(\lambda_2)\mu_2 + \cdots + \sigma_n(\lambda_2)\mu_n = 0\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&\sigma_1(\lambda_m)\mu_1 + \sigma_2(\lambda_m)\mu_2 + \cdots + \sigma_n(\lambda_m)\mu_n = 0.
\end{aligned}$$

To kraće možemo zapisati ovako:

$$\sum_{j=1}^{n} \mu_j \sigma_j(\lambda_i) = 0 \qquad i = 1, 2, \ldots, m. \tag{5.3}$$

Budući da je $m < n$ iz linearne algebre znamo da taj sustav ima netrivijalno rješenje, tj. postoje $\mu_1, \mu_2, \ldots, \mu_n \in L$, koji nisu svi jednaki nuli, takvi da je sustav jednadžbi (5.3) zadovoljen.

Neka je sada $\lambda \in L$ proizvoljan. Budući da je $\{\lambda_1, \lambda_2, \ldots, \lambda_m\}$ baza vektorskog prostora $L$ nad poljem $L^G$, to za neke $\alpha_1, \alpha_2, \ldots, \alpha_m \in L^G$ vrijedi

$$\lambda = \sum_{i=1}^{m} \alpha_i \lambda_i.$$

Sada zbog (5.3) nalazimo

$$\sum_{j=1}^{n} \mu_j \sigma_j(\lambda) = \sum_{j=1}^{n} \mu_j \sigma_j \left( \sum_{i=1}^{m} \alpha_i \lambda_i \right) = \sum_{j=1}^{n} \sum_{i=1}^{m} \mu_j \alpha_i \sigma_j(\lambda_i) = \sum_{i=1}^{m} \alpha_i \left( \sum_{j=1}^{n} \mu_j \sigma_j(\lambda_i) \right) = 0.$$

Budući da to vrijedi za svaki $\lambda \in L$, zaključujemo da je

$$\mu_1 \sigma_1 + \mu_2 \sigma_2 + \cdots + \mu_n \sigma_n = 0.$$

To znači da su $\sigma_1, \sigma_2, \ldots, \sigma_n$ linearno zavisni nad poljem $L$. No to je nemoguće zbog teorema 5.1. Ova kontradikcija pokazuje da je pretpostavka $\left[L : L^G\right] < n$ nemoguća, odnosno dokazano je da mora biti

$$\left[L : L^G\right] \geq n.$$

(2) Pretpostavimo sada da je

$$\left[L : L^G\right] > n.$$

Tada postoje $\lambda_1, \lambda_2, \ldots, \lambda_{n+1} \in L$ koji su linearno nezavisni nad poljem $L^G$. Homogeni sustav od $n+1$ linearnih jednadžbi s $n$ nepoznanica uvijek ima netrivijalno rješenje. Dakle, postoje $\mu_1, \mu_2, \ldots, \mu_{n+1} \in L$, koji nisu svi jednaki nuli, takvi da vrijedi

$$\sum_{i=1}^{n+1} \mu_i \sigma_j(\lambda_i) = 0, \qquad j = 1, 2, \ldots, n. \tag{5.4}$$

Pretpostavimo sada da smo $\mu_1, \mu_2, \ldots, \mu_{n+1}$ izabrali tako da među svim rješenjima sustava jednadžbi (5.4) ima najmanje članova različitih od nule i neka je taj broj $r$. Zatim promijenimo numeraciju $\mu_i$ (naravno, i $\lambda_i$) tako da bude

$$\mu_1 \neq 0,\ \mu_2 \neq 0,\ \ldots,\ \mu_r \neq 0, \quad \mu_{r+1} = \cdots = \mu_{n+1} = 0.$$

Dobivamo

$$\sum_{i=1}^{r} \mu_i \sigma_j(\lambda_i) = 0, \qquad j = 1, 2, \ldots, n. \tag{5.5}$$

Primijenimo sada na taj sustav bilo koji element $\sigma \in G$. Kako je $\sigma$ automorfizam polja $L$, dobivamo:

$$\sum_{i=1}^{r} \sigma(\mu_i)(\sigma \circ \sigma_j)(\lambda_i) = 0, \qquad j = 1, 2, \ldots, n. \tag{5.6}$$

Kako je $G$ grupa, preslikavanje $\tau \mapsto \sigma \circ \tau$ je bijekcija sa $G$ na $G$, tj. vrijedi

$$\{\sigma \circ \sigma_1, \sigma \circ \sigma_2, \ldots, \sigma \circ \sigma_n\} = G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}.$$

Stoga se jednakosti (5.6) mogu i ovako zapisati:

$$\sum_{i=1}^{r} \sigma(\mu_i)\sigma_j(\lambda_i) = 0, \qquad j = 1, 2, \ldots, n. \tag{5.7}$$

Pomnožimo sada jednakosti u (5.5) sa $\sigma(\mu_1)$ i od tako dobivenih jednakosti oduzmemo odgovarajuće jednakosti u (5.7) pomnožeme sa $\mu_1$. Na taj način dobivamo sljedeći sustav jednakosti:

$$\sum_{i=2}^{r} [\mu_i\sigma(\mu_1) - \mu_1\sigma(\mu_i)]\sigma_j(\lambda_i) = 0, \qquad j = 1, 2, \ldots, n. \tag{5.8}$$

Budući da je $r$ najmanji mogući broj članova različitih od nule u netrivijalnom rješenju homogenog sustava jednadžbi (5.4), zaključujemo da mora biti

$$\mu_i\sigma(\mu_1) - \mu_1\sigma(\mu_i) = 0, \qquad i = 2, \ldots, r,$$

tj.

$$\mu_i\mu_1^{-1} = \sigma(\mu_i\mu_1^{-1}), \qquad i = 2, \ldots, r.$$

Međutim, $\sigma \in G$ je bio proizvoljan. Dakle, gornja jednakost vrijedi za svaki $\sigma \in G$, a to znači da je $\mu_i\mu_1^{-1} \in L^G$ za svaki $i$. Stavimo li $\alpha_i = \mu_i\mu_1^{-1}$, tada su $\alpha_1, \alpha_2, \ldots, \alpha_r \in L^G$ ($\alpha_1 = 1$) i $\mu_i = \alpha_i\mu_1$ za svaki $i$. Uvrstimo li to u jednakosti (5.5) i skratimo sa $\mu_1$, dobivamo

$$\sum_{i=1}^{r} \alpha_i\sigma_j(\lambda_i) = 0, \qquad j = 1, 2, \ldots, n.$$

Budući da je $\sigma_1$ identiteta, za $j = 1$ imamo

$$\alpha_1\lambda_1 + \alpha_2\lambda_2 + \cdots + \alpha_r\lambda_r = 0.$$

No to je suprotno pretpostavci da su $\lambda_1, \lambda_2, \ldots, \lambda_{n+1}$ linearno nezavisni nad polje $L^G$.

Ova kontradikcija pokazuje da je pretpostavka $\left[L : L^G\right] > n$ nemoguća. Time je dokazano da mora biti $\left[L : L^G\right] = n$, odnosno, teorem je dokazan.

**Korolar 5.1.** *Neka je $L$ konačno proširenje polja $K$ i neka je $G$ konačna podgrupa Galoisove grupe $Aut_K(L)$. Tada je*

$$\left[L^G : K\right] = \frac{[L : K]}{|G|}.$$

**Dokaz:** Iz teorema 4.4. i teorema 5.2. slijedi $[L : K] = \left[L : L^G\right] \cdot \left[L^G : K\right] = |G| \cdot \left[L^G : K\right]$.

## 5.2 Separabilna i normalna proširenja

Neka je $K$ polje i neka je $P \in K[X]$ nekonstantni polinom. Označimo sa $L$ polje razlaganja polinoma $P$ nad poljem $K$. Kažemo da je $P$ **separabilan polinom** ako su sve nultočke od $P$ u $L$ jednostruke, odnosno ako je

$$P = a(X - \alpha_1) \cdots (X - \alpha_n), \qquad a \in K, \quad \alpha_1, \ldots, \alpha_n \in L, \quad \alpha_i \neq \alpha_j \quad \text{ako je} \quad i \neq j.$$

Jednostavan kriterij separabilnosti polinoma $P$ dobivamo pomoću pojma derivacije $P'$ tog polinoma definiranog u odjeljku 4.3.

**Propozicija 5.1.** *Nekonstantni polinom $P \in K[X]$ je separabilan ako i samo ako su polinomi $P$ i $P'$ relativno prosti.*

**Dokaz:** Neka je $L$ polje razlaganja polinoma $P$ nad poljem $K$.

Pretpostavimo da su polinomi $P$ i $P'$ relativno prosti u prstenu $K[X]$. To znači da postoje $A, B \in K[X]$ takvi da je $AP + BP' = 1$. Pretpostavimo da polinom $P$ nije separabilan. Tada postoji $\alpha \in L$ takav da je $P$ djeljiv sa $(X - \alpha)^2$ u prstenu $L[X]$. Prema korolaru 4.4. tada je $P(\alpha) = P'(\alpha) = 0$. No to je u suprotnosti s jednakošću $AP + BP' = 1$. Ova kontradikcija pokazuje da je pretpostavka da $P$ nije separabilan nemoguća. Dakle, polinom $P$ je separabilan.

Pretpostavimo sada da je polinom $P$ separabilan. Bez smanjenja općenitosti možemo pretpostaviti da je polinom $P$ normiran. Ako je $n = \deg P$, postoje međusobno različiti $\alpha_1, \ldots, \alpha_n \in L$ takvi da je $P = (X - \alpha_1) \cdots (X - \alpha_n)$. Polinomi $X - \alpha_1, \ldots, X - \alpha_n$ su svi normirani ireducibilni djelitelji od $P$ u prstenu $L[X]$. Nijedan od njih ne dijeli $P'$. Doista, za $j \in \{1, \ldots, n\}$ neka je $Q_j \in L[X]$ kvocijent polinoma $P$ i $X - \alpha_j$ :

$$Q_j = (X - \alpha_1) \cdots (X - \alpha_{j-1})(X - \alpha_{j+1}) \cdots (X - \alpha_n).$$

Tada je $P = (X - \alpha_j)Q$ i $Q(\alpha_j) \neq 0$. Prema propoziciji 4.1. imamo $P' = Q + (X - \alpha_j)Q'$, pa slijedi $P'(\alpha_j) = Q(\alpha_j) \neq 0$. To dokazuje da polinom $P'$ nije djeljiv sa $(X - \alpha_j)$ ni za jedno $j \in \{1, \ldots, n\}$. Zaključujemo da su polinomi $P$ i $P'$ relativno prosti u prstenu $L[X]$. No relativna prostota utvrđuje se Euklidovim algoritmom tijekom kojeg stalno ostajemo u prstenu $K[X]$. Dakle, polinomi $P$ i $P'$ su relativno prosti u prstenu $K[X]$.

Za ireducibilne polinome pitanje separabilnosti posebno je jednostavno:

**Propozicija 5.2.** *Ireducibilan polinom $P \in K[X]$ je separabilan ako i samo ako je $P' \neq 0$.*

**Dokaz:** Možemo pretpostaviti da polinom $P$ normiran. Budući da je polinom $P'$ ireducibilan najveća zajednička mjera $GCD(P, P')$ je ili $P$ ili 1. Ako je $P' = 0$, tada je $GCD(P, P') = P$, dakle, $P$ i $P'$ nisu relativno prosti, pa po propoziciji 5.1. polinom $P$ nije separabilan. Ako je $P' \neq 0$, tada je $0 \leq \deg P' < \deg P$, pa $P$ nije djelitelj od $P'$. To znači da je $GCD(P, P') = 1$, tj. $P$ i $P'$ su relativno prosti. Prema propoziciji 5.1. polinom $P$ je separabilan.

Neka je $L$ proširenje polja $K$. Kažemo da je element $\alpha \in L$ **separabilan nad** $K$ ako je $\alpha$ algebarski nad $K$ i njegov minimalni polinom $\mu_\alpha \in K[X]$ je separabilan. Kažemo da je $L$ **separabilno proširenje polja** $K$ ako je svaki element $\alpha \in L$ separabilan nad $K$.

**Korolar 5.2.** *Neka je $K$ polje karakteristike* 0. *Tada je svako algebarsko proširenje polja $K$ separabilno.*

**Dokaz:** Ako je $P \in K[X]$ ireducibilan polinom, onda je $\deg P = n \geq 1$. Kako je $K$ polje karakteristike 0, očito je $\deg P' = n - 1 \geq 0$, dakle, $P' \neq 0$. Prema propoziciji 5.2. slijedi da je polinom $P$ separabilan. Dakle, svaki ireducibilan polinom u $K[X]$ je separabilan. Posebno, minimalni polinom nad $K$ svakog elementa algebarskog proširenja polja $K$ je separabilan.

Prema tome, samo polja karakteristike $> 0$ mogu eventualno imati algebarska proširenja koja nisu separabilna. To ipak nije tako za konačna polja:

**Korolar 5.3.** *Svako algebarsko proširenje $L$ konačnog polja $K$ je separabilno.*

**Dokaz:** Neka je $L$ algebarsko proširenje konačnog polja $K$ i neka je $\alpha \in L$. Za dokaz da je element $\alpha$ separabilan nad $K$ možemo pretpostavljati da je $L = K(\alpha)$. Tada je $L$ konačno proširenje polja $K$, pa slijedi da je $L$ konačno polje. Prema rezultatima odjeljka 4.3. tada je $|L| = q = p^n$ za neki prost broj $p$ i neki prirodan broj $n$. Nadalje, prema dokazu egzistencije u teoremu 4.12. svaki element polja $L$ je nultočka polinoma $X^q - X$, štoviše, ako je $L = \{\alpha_1, \ldots, \alpha_q\}$, onda je

$$X^q - X = (X - \alpha_1) \cdots (X - \alpha_q).$$

Posebno, polinom $X^q - X$ djeljiv je s minimalnim polinomom $\mu_\alpha \in K[X]$ elementa $\alpha$ nad $K$. Kako polinom $X^q - X$ ima sve nultočke jednostruke, to i $\mu_\alpha$ ima sve nultočke jednostruke, odnosno, polinom $\mu_\alpha$ je separabilan. Dakle, element $\alpha$ je separabilan nad $K$. Kako je $\alpha$ bio proizvoljan element algebarskog proširenja $L$ polja $K$, zaključujemo da je proširenje $L$ separabilno.

Prema tome, jedini kandidati koji mogu imati neseparabilna algebarska proširenja su beskonačna polja karakteristike $p > 0$. Primjer takvog polja je $K = \mathbb{Z}_p(x)$, gdje je element $x \in K$ transcendentan nad $K$. Doista, iz transcendentnosti elementa $x \in K$ nad poljem $\mathbb{Z}_p$ slijedi da je polinom $X^p - x \in K[X]$ ireducibilan u $K[X]$. Dakle, ideal $\mathcal{J} = K[X](X^p - x)$ je maksimalan, pa je kvocijentni prsten $L = K[X]/\mathcal{J}$ polje. $L$ možemo shvaćati, kao u dokazu teorema 4.1. kao proširenje polja $K$. Neka je $\alpha \in L$ klasa polinoma $X$, tj. $\alpha = X + \mathcal{J}$. Tada je $\alpha^p = x$, pa slijedi da je $\mu_\alpha = X^p - x$ minimalni polinom od $\alpha$ nad $K$. Budući da je karakteristika jednaka $p$, derivacija tog polinoma u prstenu $K[X]$ jednaka je 0. Po propoziciji 5.2. polinom $\mu_\alpha$ nije separabilan, odnosno, element $\alpha \in L$ nije separabilan nad $K$.

Pitanje separabilnosti proširenja povezano je s Galoisovom grupom zbog sljedećeg teorema:

**Teorem 5.3.** *Neka su $K \subseteq L \subseteq M$ polja i pretpostavimo da je $M = L(\alpha)$ za neki element $\alpha \in M$ algebarski nad $L$. Neka je $N$ algebarski zatvarač polja $M$ i neka $\mu_\alpha$ minimalni polinom od $\alpha$ nad $L$. Broj $K-$monomorfizama polja $M$ u polje $N$ jednak je umnošku broja nultočaka polinoma $\mu_\alpha$ u polju $N$ i broja $K-$monomorfizama polja $L$ u polje $N$.*

**Dokaz:** Zbog jednostavnijeg pisanja stavimo $\mu_\alpha = P$. Neka je $m$ broj nultočaka polinoma $P$ u polju $N$. Kako je $M = L(\alpha)$, bilo koji monomorfizam $\varphi : M \to N$ jedinstveno je određen sa $\varphi(\alpha)$ i s restrikcijom $\varphi|L$. Stavimo $\sigma = \varphi|L$. Tada jednakost $P(\alpha) = 0$ povlači da vrijedi $P^\sigma(\varphi(\alpha)) = 0$, dakle, $\varphi(\alpha)$ je nužno nultočka polinoma $P^\sigma$. Broj nultočaka polinoma $P^\sigma$ u polju $N$ jednak je broju nultočaka polinoma $P$ u polju $N$, dakle $m$. Prema tome, broj mogućnosti za $\varphi(\alpha)$ je $\leq m$. Zaključujemo da je broj $K-$monomorfizama $M \to N$ manji ili jednak od umnoška broja $K-$monomorfizama $L \to N$ sa $m$.

Da bismo dokazali i obrnutu nejednakost, neka je $\sigma : L \to N$ bilo koji $K-$monomorfizam. Stavimo $L' = \sigma(L)$ i neka je $\beta \in N$ bilo koja nultočka polinoma $P^\sigma$. Formirajmo potpolje $L'(\beta)$ od $N$. Prema teoremu 4.10. postoji izomorfizam (čak jedinstven) $\varphi : L(\alpha) \to L'(\beta)$ takav da je $\varphi|L = \sigma$ i $\varphi(\alpha) = \beta$. Kako je $M = L(\alpha)$, to je $\varphi$ monomorfizam polja $M$ u polje $N$, a kako je

$\varphi|L = \sigma$ $K-$monomorfizam, to je i $\varphi$ $K-$monomorfizam. Prema tome, broj $K-$monomorfizama $M \to N$ je veći ili jednak od umnoška broja $K-$monomorfizama $L \to N$ sa $m$.

**Korolar 5.4.** *Neka je $L = K(\alpha_1, \ldots, \alpha_n)$ konačno algebarsko proširenje polja $K$ i neka je $N$ algebarski zatvarač polja $L$. Tada je broj $K-$monomorfizama $L \to N$ manji ili jednak $[L : K]$. Nadalje, sljedeća su svojstva međusobno ekvivalentna:*

(*a*) *Broj $K-$monomorfizama $L \to N$ jednak je $[L : K]$.*

(*b*) *Element $\alpha_j$ je separabilan nad $K(\alpha_1, \ldots, \alpha_{j-1})$ za svaki $j \in \{1, \ldots, n\}$.*

(*c*) *Elementi $\alpha_1, \ldots, \alpha_n$ su separabilni nad $K$.*

**Dokaz:** Stavimo $K_0 = K$ i za svaki $j \in \{1, \ldots, n\}$ neka je $K_j = K(\alpha_1, \ldots, \alpha_j)$; posebno je $K_n = L$. Nadalje, neka je $P_j$ minimalni polinom od $\alpha_j$ nad poljem $K_{j-1}$ i $d_j = \deg P_j$. Prema teoremu 4.2. je $[K_j : K_{j-1}] = d_j$, pa pomoću teorema 4.4. zaključujemo da je $[L : K] = d_1 \cdots d_n$. Neka je $s_j$ broj nultočaka polinoma $P_j$ u polju $N$. Tada je $s_j \leq d_j$ i vrijedi $s_j = d_j$ ako i samo ako je polinom $P_j$ separabilan, odnosno, ako i samo ako je element $\alpha_j$ separabilan nad poljem $K_{j-1}$. Ponovljenom primjenom teorema 5.3. nalazimo da je broj $K-$monomorfizama $L \to N$ jednak umnošku $s_1 \cdots s_n$. Odatle slijedi prva tvrdnja korolara, a slijedi i da su svojstva $(a)$ i $(b)$ međusobno ekvivalentna.

Svojstvo $(a)$ neovisno je o tome kojim smo redom numerirali elemente $\alpha_1, \ldots, \alpha_n$. Budući da numeraciju možemo izabrati tako da bilo koji izabrani element $\alpha_j$ bude prvi, slijedi da je svojstvo $(a)$ ekvivalentno i svojstvu $(c)$.

**Korolar 5.5.** *Neka je $L = K(\alpha_1, \ldots, \alpha_n)$ konačno algebarsko proširenje polja $K$. Ako je svaki $\alpha_j$ separabilan nad $K$, onda je $L$ separabilno proširenje polja $K$.*

**Dokaz:** Neka je $\beta \in L$. Primijenimo najprije implikaciju $(c) \implies (a)$ iz korolara 5.4. u situaciji $L = K(\alpha_1, \ldots, \alpha_n)$; zaključujemo da je broj $K-$monomorfizama $L \to N$ jednak $[L : K]$. Sada primijenimo implikaciju $(a) \implies (c)$ u situaciji $L = K(\beta, \alpha_1, \ldots, \alpha_n)$; zaključujemo da je element $\beta$ separabilan nad $K$.

**Korolar 5.6.** *Neka je $M$ algebarsko proširenje polja $K$. Tada je skup*

$$L = \{\alpha \in M;\ \alpha \text{ je separabilan nad poljem } K\}$$

*potpolje od $M$.*

**Dokaz:** Neka su $\alpha, \beta \in L$. Tada korolar 5.5. pokazuje da $L$ sadrži potpolje $K(\alpha, \beta)$ generirano sa $\{\alpha, \beta\}$ nad $K$; posebno, $L$ sadrži elemente $\alpha \pm \beta$ i $\alpha\beta$, a također i $\alpha^{-1}$ ako je $\alpha \neq 0$. Dakle, $L$ je potpolje od $M$.

**Propozicija 5.3.** *Neka je $M$ separabilno proširenje polja $K$ i neka je $L$ međupolje, $K \subseteq L \subseteq M$. Tada je $M$ separabilno proširenje od $L$ i $L$ je separabilno proširenje od $K$.*

**Dokaz:** Očito je $L$ separabilno proširenje polja $K$. Razmotrimo sada proširenje $M$ polja $L$. Neka je $\alpha \in M$ i neka je $P$ minimalni polinom od $\alpha$ nad $K$ i $Q$ minimalni polinom od $\alpha$ nad $L$. Kako je $P \in K[X] \subseteq L[X]$ iz $P(\alpha) = 0$ slijedi da je $P$ djeljiv sa $Q$ u prstenu $L[X]$. Kako je proširenje $M$ polja $K$ separabilno, element $\alpha$ je separabilan nad $K$, što znači da je polinom $P$ separabilan. No tada $P$ nema višestrukih nultočaka ni u jednom proširenju od $K$. Kao djelitelj od $P$ niti polinom $Q$ ne može imati višestrukih nultočaka ni u jednom proširenju polja $L \supseteq K$. Stoga je i polinom $Q$ separabilan, što znači da je $\alpha$ separabilan nad $L$. Kako je $\alpha$ bio proizvoljan element od $M$, zaključujemo da je $M$ separabilno proširenje polja $L$.

**Propozicija 5.4.** *Neka je $L$ algebarsko proširenje polja $K$ takvo da je $L = K(\alpha)$ za neki $\alpha \in L$. Neka je $P$ minimalni polinom od $\alpha$ nad $K$. Tada je $|Aut_K(L)| \leq [L : K]$. Nadalje, vrijedi znak jednakosti $|Aut_K(L)| = [L : K]$ ako i samo ako je polinom $P$ separabilan i $L$ je polje razlaganja polinoma $P$ nad $K$.*

**Dokaz:** Svaki element $\varphi \in Aut_K(L)$ preslikava $\alpha$ u neku nultočku $\alpha'$ polinoma $P$ i $\varphi$ je u potpunosti određen sa $\alpha'$ jer je $L = K(\alpha)$. Prema tome, broj $|Aut_K(L)|$ je manji ili jednak broju nultočaka polinoma $P$ u polju $L$. Neka je sada $\alpha' \in L$ bilo koja nultočka polinoma $P$ u polju $L$. Kako je $L = K(\alpha)$, to je $K(\alpha') \subseteq K(\alpha)$. Međutim, $P$ je kao minimalni polinom ireducibilan nad $K$, pa je to ujedno minimalni polinom od $\alpha'$. Prema teoremu 4.2. slijedi $[K(\alpha') : K] = \deg P = [K(\alpha) : K]$, dakle je $K(\alpha') = K(\alpha) = L$. Sada iz teorema 4.7. slijedi da postoji $K-$izomorfizam $\varphi : L \to L$, tj. postoji $\varphi \in Aut_K(L)$, takav da je $\varphi(\alpha) = \alpha'$. Zaključujemo da je broj $|Aut_K(L)|$ elemenata Galoisove grupe točno jednak broju nultočaka polinoma $P$ u polju $L$. Odatle slijede obje tvrdnje propozicije.

Primijetimo da je u slučaju $K = \mathbb{Q}$ i $L = \mathbb{Q}(\sqrt[3]{2})$ polinom $P = X^3 - 2$ minimalni polinom elementa $\sqrt[3]{2}$. Taj se polinom ne razlaže nad $L$ jer je $L \subseteq \mathbb{R}$, a preostale dvije nultočke polinoma $P$ nisu realni brojevi. Prethodna propozicija pokazuje da je u ovom slučaju $|Aut_K(L)| < [L : K] = 3$. Stoga je $|Aut_K(L)| = 1$, tj. identiteta je jedini element Galoisove grupe $Aut_K(L)$.

Pomoću propozicije 5.4. moguće je induktivno istraživati slučaj $L = K(\alpha_1, \ldots, \alpha_n)$, tj. slučaj bilo kojeg konačnog algebarskog proširenja od $K$. Međutim, svako se takvo separabilno proširenje svodi direktno na slučaj iz propozicije 5.4. zbog sljedećeg važnog i netrivijalnog teorema:

**Teorem 5.4.** (**Teorem o primitivnom elementu**) *Neka je $L$ konačno separabilno proširenje polja $K$. Tada postoji $\alpha \in L$ takav da je $L = K(\alpha)$.*

**Dokaz:** Možemo pisati $L = K(\alpha_1, \ldots, \alpha_n)$ za neke $\alpha_1, \ldots, \alpha_n \in L$. Dokaz provodimo indukcijom u odnosu na $n$. Baza indukcije $n = 1$ je trivijalna. Pretpostavimo da je $n \geq 2$ i da je teorem dokazan u svakom slučaju kad je proširenje $L$ generirano sa $n - 1$ elemenata nad $K$. Postoji $\alpha \in K(\alpha_1, \ldots, \alpha_{n-1})$ takav da je $K(\alpha_1, \ldots, \alpha_{n-1}) = K(\alpha)$, pa slijedi $L = K(\alpha, \alpha_n)$. Dakle, korak indukcije svodi se na dokaz tvrdnje:

*Neka je $L$ separabilno proširenje polja $K$ takvo da je $L = K(\alpha, \beta)$ za neke $\alpha, \beta \in L$. Tada postoji $\gamma \in L$ takav da je $L = K(\gamma)$.*

U dokazu možemo pretpostavljati da je polje $K$ beskonačno. Doista, ako je polje $K$ konačno, onda je i polje $L$ konačno. No tada za neki prost broj $p$, za neki $n \in \mathbb{N}$ i za $q = p^n$ vrijedi $L = \mathbb{F}_q$. Tada je $L = \mathbb{F}_p(\alpha)$ za bilo koji generator $\alpha$ cikličke multiplikativne grupe $L^* = L \setminus \{0\}$.

Dokazat ćemo da u slučaju beskonačnog polja $K$ postoji traženi $\gamma$ oblika $\beta + c\alpha$ za neki $c \in K$.

Neka su $P = \mu_\alpha$ i $Q = \mu_\beta$ minimalni polinomi elemenata $\alpha$ i $\beta$ nad $K$. Neka je $M \supseteq L$ polje razlaganja polinoma $PQ$. Tada se oba polinoma $P$ i $Q$ razlažu nad $K$. Neka su $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_m$ sve nultočke od $P$ u polju $M$ i $\beta_1 = \beta, \beta_2, \ldots, \beta_n$ sve nultočke polinoma $Q$ u polju $M$. Sve su te nultočke jednostruke jer su polinomi $P$ i $Q$ separabilni. Za $c \in K$ stavimo $L_c = K(\beta + c\alpha)$. Dokazat ćemo da postoji $c \in K$ takav da je $\alpha \in L_c$; tada će biti i $\beta = \beta + c\alpha - c\alpha \in L_c$, pa će slijediti $L = K(\alpha, \beta) \subseteq L_c \subseteq L$, dakle, $L = L_c = K(\beta + c\alpha)$.

Izračunajmo minimalni polinom od $\alpha$ nad $L_c$. Definiramo $R \in M[X]$ sa $R(X) = Q(\beta + c\alpha - cX)$. Tada je $R(\alpha) = Q(\beta) = 0$, pa slijedi da je polinom $R$ djeljiv sa $X - \alpha$ u $M[X]$. Vrijedi i $P(\alpha) = 0$, pa je i $P$ djeljiv sa $X - \alpha$ u $M[X]$. Odredimo $GCD(P, R)$ u $M[X]$. Budući da je polinom $P$ separabilan, to $P$ nije djeljiv sa $(X - \alpha)^2$. Budući da se $P$ razlaže nad $M$, svaki drugi normiran prosti faktor od $GCD(P, R)$ mora biti oblika $X - \alpha_j$ za $j \geq 2$. Po definiciji polinoma $R$ imamo $R(\alpha_j) = Q(\beta + c\alpha - c\alpha_j)$. Ako je $Q(\beta + c\alpha - c\alpha_j) = 0$, onda je $\beta + c\alpha - c\alpha_j = \beta_i$ za neki $i$, pa

slijedi $c = (\beta_i - \beta)(\alpha - \alpha_j)^{-1}$. Skup

$$\{(\beta_i - \beta)(\alpha - \alpha_j)^{-1};\ 1 \leq i \leq n,\ 2 \leq j \leq m\}$$

je konačan, a kako je polje $K$ beskonačno, postoji $c \in K$ koji nije u tom konačnom skupu. To znači da za takav $c$ vrijedi $R(\alpha_j) \neq 0$ za $j = 2, \ldots, m$. U tom slučaju zaključujemo da je $GCD(P, R) = X - \alpha$ u $M[X]$. No kako su $P, R \in L_c[X]$, slijedi da je i njihova normirana najveća zajednička mjera $X - \alpha \in L_c[X]$, što znači da je $\alpha \in L_c$.

Konačno separabilno proširenje $L$ polja $K$ zove se **normalno proširenje polja** $K$, ako je $L$ polje razlaganja nekog polinoma $P \in K[X]$ nad $K$.

**Propozicija 5.5.** *Neka je $L$ konačno separabilno proširenje polja $K$. Tada su sljedeća četiri svojstva međusobno ekvivalentna:*

(*a*) *$L$ je normalno proširenje polja $K$.*

(*b*) *Ako je $F \in K[X]$ ireducibilni polinom koji ima nultočku u polju $L$, onda se $F$ razlaže nad $L$.*

(*c*) $|Aut_K(L)| = [L : K]$.

(*d*) *Vrijedi* $K = L^{Aut_K(L)} = \{\lambda \in L;\ \sigma(\lambda) = \lambda\ \forall \sigma \in Aut_K(L)\}$.

**Dokaz:** Iz teorema 5.4. slijedi da možemo pretpostavljati da je $L = K(\gamma)$ za neki $\gamma \in L$. Neka $\mu_\gamma$ označava minimalni polinom od $\gamma$ nad $K$.

(1) Pretpostavimo da vrijedi (*a*). Dokazat ćemo da odatle slijedi (*c*). Zbog propozicije 5.4. dovoljno je dokazati da se polinom $\mu_\gamma$ razlaže nad $L$.

Kako je proširenje $L = K(\gamma)$ polja $K$ normalno, postoji $P \in K[X]$ koji se razlaže nad $L$ i vrijedi $L = K(\alpha_1, \ldots, \alpha_n)$, gdje su $\alpha_1, \ldots, \alpha_n$ sve nultočke polinoma $P$ u polju $L$. Možemo pretpostaviti da polinom $P$ nije djeljiv s kvadratom nekog ireducibilnog polinoma iz $K[X]$. Kako je proširenje $L$ separabilno, slijedi da su svi prosti faktori od $P$ separabilni, pa zaključujemo da je polinom $P$ separabilan, tj. sve su njegove nultočke $\alpha_1, \ldots, \alpha_n$ jednostruke. Imamo $\gamma \in L$ i $L = K(\alpha_1, \ldots, \alpha_n)$, dakle, postoji polinom $Q \in K[X_1, \ldots, X_n]$ takav da je $\gamma = Q(\alpha_1, \ldots, \alpha_n)$. Neka je $L'$ konačno proširenje od $L$ nad kojim se polinom $\mu_\gamma$ razlaže. Neka je $\gamma' \in L'$ bilo koja nultočka polinoma $\mu_\gamma$. Treba dokazati da je $\gamma' \in L$, jer će to značiti da se polinom $\mu_\gamma$ razlaže nad $L$. Prema teoremu 4.10. postoji $K-$izomorfizam $\varphi : K(\gamma) \to K(\gamma')$, takav da je $\varphi(\gamma) = \gamma'$. Budući da je za svaki $i \in \{1, \ldots, n\}$ $\varphi(\alpha_i)$ nultočka polinoma $P^\varphi = P$, slijedi da je $\varphi(\alpha_i) = \alpha_{j(i)}$ za jedinstven $j(i) \in \{1, \ldots, n\}$. Prema tome, $\varphi$ permutira skup $\{\alpha_1, \ldots, \alpha_n\}$. Stoga je

$$\gamma' = \varphi(\gamma) = \varphi(Q(\alpha_1, \ldots, \alpha_n)) = Q_1(\alpha_1, \ldots, \alpha_n)$$

za neki $Q_1 \in K[X_1, \ldots, X_n]$. Dakle, $\gamma' \in K(\alpha_1, \ldots, \alpha_n) = L$. Time je dokazano da vrijedi (*c*).

(2) Pretpostavimo sada da vrijedi (*c*) i dokažimo (*a*). Propozicija 5.4. zbog separabilnosti proširenja $L$ od $K$ povlači da je $L$ polje razlaganja za polinom $\mu_\gamma$ nad poljem $K$. No to znači da vrijedi (*a*).

(3) Pretpostavimo ponovo da vrijedi (*a*). Dokazat ćemo da tada vrijedi (*d*). Neka je $K' = L^{Aut_K(L)}$. Tada je svaki element od $Aut_K(L)$ ne samo $K-$automorfizam, nego i $K'-$automorfizam. Dakle je $Aut_K(L) \subseteq Aut_{K'}(L)$. Nadalje, svojstvo (*a*) za proširenje $L$ polja $K$ povlači da $L$ ima isto svojstvo i kao proširenje polja $K'$. Prema propoziciji 5.3. $L$ je separabilno proširenje polja $K'$. Budući da prema (1) svojstvo (*a*) povlači svojstvo (*c*), zaključujemo da svojstvo (*c*) vrijedi i za $L$ nad $K$ i za $L$ nad $K'$. Dakle,

$$[L : K] = |Aut_K(L)| \leq |Aut_{K'}(L)| = [L : K'].$$

Budući da je očito $K \subseteq K'$, gornja nejednakost dimenzija povlači jednakost i $K' = K$. Time je dokazano $(d)$.

(4) Pretpostavimo sada da vrijedi $(d)$ i dokažimo $(b)$. Neka je $F \in K[X]$ normiran ireducibilni polinom koji ima nultočku $\alpha \in L$. Tada je $F$ minimalni polinom od $\alpha$ nad $K$. Neka je $G = Aut_K(L)$, $|G| = n$ i $G = \{\varphi_1, \ldots, \varphi_n\}$. Stavimo $\alpha_i = \varphi_i(\alpha)$. Tada je

$$\{\varphi(\alpha);\ \varphi \in G\} = \{\alpha_1, \ldots, \alpha_n\}$$

i pri tome može biti i ponavljanja. Stavimo

$$J = \prod_{i=1}^{n}(X - \alpha_i) \in L[X].$$

Tada imamo

$$J = X^{|G|} - \left(\sum_i \alpha_i\right) X^{|G|-1} + \left(\sum_{i<j} \alpha_i\alpha_j\right) X^{|G|-2} - \cdots\cdots \pm \alpha_1\alpha_2\cdots\alpha_n.$$

Budući da svaki element $\varphi \in G$ permutira element $\alpha_i$ vidimo da za svaki koeficijent $\beta$ polinoma $J$ vrijedi $\varphi(\beta) = \beta\ \ fa\beta \in G$. Prema $(d)$ to znači da je $\beta \in K$. Prema tome je $J \in K[X]$. Budući da je $J(\alpha) = 0$, minimalni polinom $F$ elementa $\alpha$ nad $K$ dijeli polinom $J$ u $K[X]$. No kako se $J$ po definiciji razlaže nad $L$, zaključujemo da se i $F$ razlaže nad $L$. Dakle, vrijedi $(b)$.

(5) Napokon, pretpostavimo da vrijedi $(b)$. Polinom $\mu_\gamma$ je ireducibilan u $K[X]$ i ima nultočku $\gamma \in L$. Prema $(b)$ polinom $\mu_\gamma$ se razlaže nad $L$. No kako je $L = K(\gamma)$, $L$ je polje razlaganja polinoma $\mu_\gamma$ nad $K$. Dakle, vrijedi $(a)$.

Time je propozicija 5.5. u potpunosti dokazana.

**Korolar 5.7.** *Neka je $L$ normalno proširenje polja $K$ i neka je $M$ međupolje, $K \subseteq M \subseteq L$. Tada je $L$ normalno proširenje polja $M$ i vrijedi*

$$|Aut_M(L)| \cdot [M : K] = |Aut_K(L)|.$$

**Dokaz:** Prema propoziciji 5.3. $L$ je separabilno proširenje polja $M$. Nadalje, $L$ je polje razlaganja nekog polinoma $P \in K[X] \subseteq M[X]$, pa je $L$ polje razlaganja od $P$ nad $M$. Dakle, $L$ je normalno proširenje polja $M$. No tada iz propozicije 5.5. nalazimo da vrijedi $|Aut_M(L)| = [L : M]$. Dakle,

$$|Aut_M(L)| \cdot [M : K] = [L : M] \cdot [M : K] = [L : K] = |Aut_K(L)|.$$

**Korolar 5.8.** *Neka je $L$ separabilno proširenje polja $K$ i neka je $H$ konačna podgrupa grupe $Aut_K(L)$. Tada je $L$ normalno proširenje polja $L^H$ i vrijedi $H = Aut_{L^H}(L)$ i $[L : L^H] = |H|$.*

**Dokaz:** Prema propoziciji 5.3. $L$ je separabilno proširenje polja $L^H$. Neka je $x \in L$. Formirajmo polinom $P \in L[X]$ ovako:

$$P = \prod_{\varphi \in H}(X - \varphi(x)).$$

Za $\psi \in H$ je $\varphi \to \psi \circ \varphi$ bijekcija sa $H$ na $H$. Dakle,

$$P^\psi = \prod_{\varphi \in H}(X - (\psi \circ \varphi)(x)) = \prod_{\varphi \in H}(X - \varphi(x)) = P.$$

Budući da to vrijedi za svaki $\psi \in H$, slijedi da je $P \in L^H[X]$. Polinom $P$ ima nultočku $x$ i razlaže se nad $L$. Neka je $\mu_x \in L^H[X]$ minimalni polinom od $x$ nad $L^H$. Tada $\mu_x$ dijeli $P$ u prstenu

$L^H[X]$, pa slijedi da se i polinom $\mu_x$ razlaže nad $L$. Time je dokazano da proširenje $L$ polja $L^H$ ima svojstvo $(b)$. Nadalje, prema teoremu 5.2. vidimo da je $L$ konačno proširenje od $L^H$ i vrijedi $[L : L^H] = |H|$. Prema propoziciji 5.3. $L$ je normalno proširenje polja $L^H$.

Treba još samo dokazati da je $H = Aut_{L^H}(L)$. No iz definicije polja $L^H$ je očito da je $H \subseteq Aut_{L^H}(L)$. Jednakost slijedi iz jednakosti $|H| = [L : L^H]$, jer prema propoziciji 5.3. je i $|Aut_{L^H}(L)| = [L : L^H]$.

## 5.3 Fundamentalni teorem Galoisove teorije

Neka je $L$ konačno proširenje polja $K$. Označimo sa $\mathcal{F} = \mathcal{F}(L:K)$ skup svih međupolja $M$, $K \subseteq M \subseteq L$. Nadalje, označimo sa $\mathcal{G} = \mathcal{G}(L:K)$ skup svih podgrupa Galoisove grupe $Aut_K(L)$. Za svaku $H \in \mathcal{G}$ stavimo

$$\Psi(H) = L^H = \{\lambda \in L;\ \sigma(\lambda) = \lambda\ \forall \sigma \in H\}.$$

Tada je očito $\Psi(H) \in \mathcal{F}$, dakle, $\Psi$ je preslikavanje sa $\mathcal{G}$ u $\mathcal{F}$. Nadalje, ako je $M \in \mathcal{G}$, definiramo

$$\Phi(M) = Aut_M(L) = \{\sigma \in Aut_K(L);\ \sigma(\alpha) = \alpha\ \forall \alpha \in M\}.$$

Tada je $\Phi(M) \in \mathcal{G}$, dakle, $\Phi$ je preslikavanje sa $\mathcal{F}$ u $\mathcal{G}$.

**Teorem 5.5.** (**Fundamentalni teorem Galoisove teorije**) *Neka je $L$ normalno proširenje polja $K$. Uz uvedene oznake $\Phi$ i $\Psi$ su međusobno inverzne bijekcije. Nadalje za $M, M' \in \mathcal{F}$ je $M \subseteq M'$ ako i samo ako je $\Phi(M) \supseteq \Phi(M')$ i za $H, H' \in \mathcal{G}$ je $H \subseteq H'$ ako i samo ako je $\Psi(H) \supseteq \Psi(H')$.*

**Dokaz:** Za svako međupolje $M \in \mathcal{F}$ prema korolaru 5.7. $L$ je normalno proširenje polja $M$ i prema propoziciji je $M = L^{Aut_M(L)}$. To pokazuje da je preslikavanje $\Phi$ injekcija sa $\mathcal{F}$ u $\mathcal{G}$. Nadalje, ako je $H \in \mathcal{G}$, prema korolaru 5.8. je $H = Aut_{L^H}(L)$, dakle je $\Phi$ i surjekcija sa $\mathcal{F}$ na $\mathcal{G}$. Sasvim analogno se vidi i da je $\Psi$ bijekcija sa $\mathcal{G}$ na $\mathcal{F}$. Nadalje, relacija $H = Aut_{L^H}(L)$ pokazuje da su te bijekcije međusobno inverzne.

Napokon, iz $M \subseteq M'$ očito slijedi $\Phi(M) \supseteq \Phi(M')$ a također iz $H \subseteq H'$ slijedi $\Psi(H) \supseteq \Psi(H')$. Budući da su preslikavanja $\Phi$ i $\Psi$ međusobno inverzna, slijede i obrnute implikacije.

**Teorem 5.6.** *Neka je $L$ normalno proširenje polja $K$ i neka je $M \in \mathcal{F}$ međupolje, $K \subseteq M \subseteq L$. Tada je $M$ normalno proširenje polja $K$ ako i samo ako je $Aut_M(L)$ normalna podgrupa grupe $Aut_K(L)$. U tom je slučaju grupa $Aut_K(M)$ izomorfna kvocijentnoj grupi $Aut_K(L)/Aut_M(L)$.*

**Dokaz:** Stavimo $H = \Phi(M) = Aut_M(L)$. Prema teoremu 5.5. je $M = \Psi(H) = L^H$. Ako je $\varphi \in Aut_K(L)$ onda je

$$L^{\varphi H \varphi^{-1}} = \{\lambda \in L;\ \varphi(\psi(\varphi^{-1}(\lambda))) = \lambda\ \forall \psi \in H\} = \{\varphi(\lambda') \in L;\ \varphi(\psi(\lambda')) = \varphi(\lambda')\ \forall \psi \in H\} =$$

$$= \{\varphi(\lambda') \in L;\ \psi(\lambda') = \lambda'\ \forall \psi \in H\} = \varphi\left(L^H\right) = \varphi(M).$$

Budući da u teoremu 5.5. imamo bijekcije, vidimo da je $\varphi H \varphi^{-1} = H$ ako i samo ako je $\varphi(M) = M$. Prema tome, $H$ je normalna podgrupa od $Aut_K(L)$ ako i samo ako je $\varphi(M) = M\ \ \forall \varphi \in Aut_K(L)$.

Pretpostavimo da je $H$ normalna podgrupa od $Aut_K(L)$. Upravo smo vidjeli da je tada $\varphi(M) = M\ \ \forall \varphi \in Aut_K(L)$. Stoga je za svaki $\varphi \in Aut_K(L)$ restrikcija $\varphi|M$ element grupe $Aut_K(M)$. Očito je $\varphi \mapsto \varphi|M$ homomorfizam grupa. Jezgra tog homomorfizma je

$$\{\varphi \in Aut_K(L);\ \varphi|M = id_M\} = Aut_M(L).$$

Stoga prijelazom na kvocijent dobivamo monomorfizam grupe $Aut_K(L)/Aut_M(L)$ u grupu $Aut_K(M)$. Posebno, vrijedi

$$\frac{|Aut_K(L)|}{|Aut_M(L)|} = |Aut_K(L)/Aut_M(L)| \leq |Aut_K(M)|.$$

Kako je $|Aut_K(L)| = [L:K]$ i $|Aut_M(L)| = [L:M]$, primjenom propozicije 5.4. i teorema 5.4. na proširenje $M$ od $K$ nalazimo

$$[M:K] = \frac{[L:K]}{[L:M]} = \frac{|Aut_K(L)|}{|Aut_M(L)|} \leq |Aut_K(M)| \leq [M:K]$$

s jednakošću umjesto prvog znaka $\leq$ ako i samo ako je gore definirani monomorfizam grupa $Aut_K(L)/Aut_M(L) \to Aut_K(M)$ izomorfizam i s jednakošću umjesto drugog znaka $\leq$ ako i samo ako je $M$ normalno proširenje polja $K$. No budući da su krajnji brojevi jednaki, na oba mjesta mora vrijediti znak jednakosti. Zaključujemo da je proširenje $M$ polja $K$ normalno i da je grupa $Aut_K(M)$ izomorfna kvocijentnoj grupi $Aut_K(L)/Aut_M(L)$.

Treba još dokazati da iz normalnosti proširenja $M$ polja $K$ slijedi da je $H = Aut_M(L)$ normalna podgrupa od $Aut_K(L)$. Dakle, neka je $M \in \mathcal{F}$ normalno proširenje polja $K$. Prema prvom odlomku u dokazu dovoljno je dokazati da je tada $\varphi(M) = M \ \ \forall \varphi \in Aut_K(L)$. Po definiciji normalnog proširenja $M$ je polje razlaganja nekog polinoma $P \in K[X]$. Možemo pretpostaviti da je polinom $P$ normiran. Tada je

$$P = (X - \alpha_1) \cdots (X - \alpha_n), \qquad \alpha_1, \ldots, \alpha_n \in M.$$

Ako je $\varphi \in Aut_K(L)$, onda je $P^\varphi = P$, pa imamo

$$P = (X - \varphi(\alpha_1)) \cdots (X - \varphi(\alpha_n))$$

s tim da samo znamo da su $\varphi(\alpha_1), \ldots, \varphi(\alpha_n) \in L$. Međutim, zbog jedinstvenosti faktorizacije u $L[X]$ zaključujemo da je $(\varphi(\alpha_1), \ldots, \varphi(\alpha_n))$ neka permutacija od $(\alpha_1, \ldots, \alpha_n)$. Posebno, $\varphi(\alpha_i) \in M$ za svako $i$, a kako je polje $M$ generirano sa $\alpha_1, \ldots, \alpha_n$ nad $K$, zaključujemo da je $\varphi(M) \subseteq M$. Budući da je i $\varphi^{-1}(M) \subseteq M$, slijedi jednakost $\varphi(M) = M \ \ \forall \varphi \in Aut_K(L)$.

## 5.4 Rješivost u radikalima

Za **proširenje** $L$ **polja** $K$ kažemo da je **radikalno** ako postoje $\alpha_1, \alpha_2, \ldots, \alpha_m \in L$ i prirodni brojevi $n_1, n_2, \ldots, n_m$ takvi da vrijedi

$$L = K(\alpha_1, \alpha_2, \ldots, \alpha_m) \qquad \text{i} \qquad \alpha_1^{n_1} \in K, \quad \alpha_j^{n_j} \in K(\alpha_1, \ldots, \alpha_{j-1}) \quad \text{za} \quad j = 2, \ldots, m.$$

Tada za takav niz $\alpha_1, \alpha_2, \ldots, \alpha_m$ kažemo da je **radikalni niz** proširenja $L$ polja $K$, a za niz $n_1, n_2, \ldots, n_m$ zažemo da je odgovarajući **niz radikalnih stupnjeva**.

Neka je $K \subseteq \mathbb{C}$ polje, $P \in K[X]$ polinom s koeficijentima iz polja $K$ i neka je $L$ polje razlaganja polinoma $P$. Kažemo da je **polinom** $P$ **rješiv u radikalima nad poljem** $K$, ako postoji radikalno proširenje $M$ polja $K$ koje sadrži $L$. Dakle, polinom $P$ rješiv je u radikalima, ako postoji radikalno proširenje polja $K$ nad kojim se polinom $P$ razlaže.

Glavni rezultat u vezi s pitanjem rješivosti polinoma u radikalima je sljedeći teorem koji navodimo bez dokaza:

**Teorem 5.7.** *Neka su $K \subseteq L \subseteq M \subseteq \mathbb{C}$ polja i pretpostavimo da je $M$ radikalno proširenje polja $K$. Tada je Galoisova grupa $Aut_K(L)$ proširenja $L$ polja $K$ rješiva.*

Neka je $K \subseteq \mathbb{C}$ polje i neka je $L$ polje razlaganja polinoma $P \in K[X]$. Tada se $Aut_K(L)$ zove **Galoisova grupa polinoma** $P$ **nad poljem** $K$ i označava $Gal(P : K)$. Neka je tada $\alpha \in L$ nultočka polinoma $P$ i neka $\sigma \in Aut_K(L)$. Tada je

$$0 = \sigma(P(\alpha)) = P(\sigma(\alpha)).$$

Dakle, ako je $\mathcal{N}(P) = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ skup svih nultočaka polinoma $P$, onda je

$$\{\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_n)\} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\} \qquad \text{za svaki} \quad \sigma \in Aut_K(L).$$

To znači da svaki $\sigma \in Aut_K(L)$ određuje neku permutaciju skupa $\mathcal{N}(P)$ svih nultočaka polinoma $P$. Budući da je polje $L$ generirano skupom $\mathcal{N}(P)$ nad $K$, $L = K(\mathcal{N}(P))$, jasno je da je svaki $\sigma \in Aut_K(L)$ u potpunosti određen tom permutacijom. Dakle, Galoisova grupa polinoma $P$ izomorfna je nekoj podgrupi grupe permutacija skupa $\mathcal{N}(P)$, odnosno, podgrupi grupe $S_n$ permutacija skupa $\{1, 2, \ldots, n\}$, gdje je $n = |\mathcal{N}(P)| \leq \deg P$. Galois je o onome što danas zovemo Galoisovom grupom razmišljao upravo na taj način, kao o nekoj grupi permutacija nultočaka polinoma $P$. Tek kasnije se upravo na poticaj Galoisovih rezultata razvila teorija grupa i teorija proširenja polja.

Primijenimo sada teorem 5.7. na Galoisovu grupu nekog polinoma. Tada se može dokazati da vrijedi i obrat, tj. imamo:

**Teorem 5.8.** *Neka je $K \subseteq \mathbb{C}$ polje i neka je $P \in K[X]$. Polinom $P$ rješiv je u radikalima nad poljem $K$ ako i samo ako je njegova Galoisova grupa $Gal(P : K)$ rješiva.*

Sljedeća lema omogućit će nam da napišemo polinom petog stupnja koji nije rješiv u radikalima.

**Lema 5.1.** *Neka je $p$ prost broj i neka je $P \in \mathbb{Q}[T]$ ireducibilan polinom stupnja $p$ koji ima točno dvije nerealne nultočke u $\mathbb{C}$. Tada je njegova Galoisova grupa $Gal(P : \mathbb{Q})$ izomorfna grupi permutacija $S_p$.*

**Dokaz:** Neka je $L$ polje razlaganja polinoma $P$ i neka je

$$G = Gal(P:\mathbb{Q}) = Aut_{\mathbb{Q}}(L)$$

Galoisova grupa polinoma $P$ nad poljem $\mathbb{Q}$. Tu grupu možemo identificirati s nekom podgrupu grupe permutacija $S_p$ skupa nultočaka polinoma $P$. Neka je $\alpha$ bilo koja nultočka polinoma $P$. Prema teoremu 4.2. imamo $[\mathbb{Q}(\alpha):\mathbb{Q}] = p$. Prema teoremu 4.4. imamo

$$[L:\mathbb{Q}] = [L:\mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha):\mathbb{Q}] = [L:\mathbb{Q}(\alpha)] \cdot p.$$

Dakle, stupanj proširenja $[L:\mathbb{Q}]$ djeljiv je s $p$. Prema tvrdnji $(c)$ propozicije 5.5. vrijedi $[L:\mathbb{Q}] = |G|$. Dakle, red grupe $G$ djeljiv je s $p$. Prema Cauchyjevom teoremu 2.7. grupa $G$ sadrži neku permutaciju $\sigma \in S_p$ čiji je eksponent $p$. Ali $p-$ciklusi su jedine permutacije u grupi $S_p$ čiji je eksponent $p$. Dakle, grupa $G$ sadrži neki $p-$ciklus.

Kompleksno konjugiranje je $\mathbb{Q}-$automorfizam polja $\mathbb{C}$, a njegova restrikcija na $L$ definira element grupe $Aut_{\mathbb{Q}}(L) = G$. Taj element grupe $G$ ostavlja fiksnim sve nultočke od $P$ osim dvije koje zamjenjuje. Dakle, kompleksno konjugiranje definira $2-$ciklus koji je element grupe $G$.

Nultočke polinoma $P$ možemo tako numerirati da su prve dvije upravo nerealne nultočke od $P$. Dakle, $2-$ciklus $\tau = (12)$ je element grupe $G$. Nadalje, za $p-$ciklus $\omega \in G$ i za $1 \leq j \leq p-1$ je i $\omega^j \in G$ $p-$ciklus. Odatle se vidi da preostale nultočke od $P$ možemo tako numerirati da je $p-$ciklus $\sigma = (1, 2, \ldots, p)$ element grupe $G$.

Dokazat ćemo sada da te permutacije $\tau$ i $\sigma$ generiraju cijelu grupu $G$. Lako se vidi da za svaki $j \in \{1, 2, \ldots, p-2\}$ vrijedi $\sigma^{-1}(j, j+1)\sigma = (j+1, j+2)$. Dakle, $(12), (23), (34), \ldots, (p-1, p) \in G$. Nadalje, imamo

$$(12)(23)(12) = (13), \quad (13)(34)(13) = (14), \quad \ldots\ldots, \quad (1j)(j, j+1)(1j) = (1, j+1), \quad \ldots\ldots$$

Dakle, $G$ sadrži sve transpozicije oblika $(1j)$, $j = 2, \ldots, p$. Napokon, $(1j)(1i)(1j) = (ij)$, dakle, grupa $G$ sadrži sve transpozicije. Kako se svaka permutacija može napisati kao produkt transpozicija, zaključujemo da je $G = S_p$.

**Teorem 5.9.** *Polinom $P = T^5 - 6T + 3$ nije rješiv u radikalima nad poljem $\mathbb{Q}$.*

**Dokaz:** Po Eisensteinovom kriteriju (teorem 3.10.) polinom $P$ je ireducibilan. Dokazat ćemo da polinom $P$ ima točno tri realne nultočke koje su sve jednostruke jer je polinom $P$ ireducibilan. Dakle, moći ćemo zaključiti da polinom $P$ ima točno dvije nerealne nultočke, dakle, prema lemi 5.1. Galoisova grupa $Gal(P:\mathbb{Q})$ polinoma $P$ nad poljem $\mathbb{Q}$ izomorfna je simetričnoj grupi $S_5$. Prema korolaru 2.1. $Gal(P:\mathbb{Q})$ nije rješiva, a tada iz teorema 5.8. slijedi da polinom $P$ nije rješiv u radikalima nad poljem $\mathbb{Q}$.

Dokažimo da polinom $P$ ima točno tri realne nultočke, uočimo da je

$$P(-2) = -17, \quad P(-1) = 8, \quad P(0) = 3, \quad P(1) = -2 \quad \text{i} \quad P(2) = 23.$$

To pokazuje da $P$ ima barem tri realne nultočke. Kako su nultočke od $P$ jednostruke i stupanj od $P$ je neparan, broj realnih nultočaka je neparan, pa zaključujemo da $P$ ima ili tri ili pet realnih nultočaka. Drugu mogućnost odbacit ćemo na temelju Rolleovog teorema iz matematičke analize, prema kojem se između svakih dviju susjednih realnih nultočaka polinoma $P$ nalazi jedna nultočka njegove derivacije $P'$. Kako je $P' = 5T^4 - 6$, vidimo da $P'$ ima dvije realne nultočke $\pm\sqrt[4]{6/5}$. Zaključujemo da $P$ ima točno tri realne nultočke.

# Bibliografija


[1] R.B. Ash, *Basic Abstract Algebra*, Dover Publications, Inc., Mineola, New York, 2007.

[2] J. Bewersdorff, *Galois Theory for Beginners*, American Mathematical Society, Providence, Rhode Island, 2006.

[3] G. Birkhoff, S. MacLane, *A Survey of Modern Algebra*, Macmillan, New York, 1965.

[4] J.M. Howie, *Fields and Galois Theory*, Springer−Verlag, New York, 2006.

[5] T.W. Hungerford, *Algebra*, Rinehart&Winston, New York, 1974; Springer−Verlag, New York, 2003.

[6] A.W. Knapp, *Basic Algebra*, Birkh auser, Boston − Basel − Berlin, 2006.

[7] S. Lang, *Algebra*, Addison−Wesley, Reading, Massachussetts, 1965.

[8] I. Stewart, *Galois Theoty*, Chapmann and Hall, London, 1973.

[9] B.L. van der Warden, *Algebra I,II*, Springer−Verlag, New York − Berlin − Heidelberg, 1971.