Osnovne algebarske strukture

Počet ćemo s uvođenjem fundamentalnih algebarskih struktura na kojima ćemo zatim dalje graditi i čija svojstva ćemo proučavati.

Grupoid je neprazan skup G sa zadanom binarnom operacijom, odnosno sa zadanim preslikavanjem $G \times G \to G$.

Primijetimo kako za algebarske strukture uvijek tražimo da budu neprazne. Prilikom zadavanja binarnih operacija koristimo nekoliko notacija:

1. Multiplikativna notacija (najčešća): $(a, b) \mapsto a \cdot b$ ili jednostavno $(a, b) \mapsto ab$ (govorimo: produkt elemenata a i b iz G)
2. Aditivna notacija: $(a, b) \mapsto a + b$ (govorimo: suma elemenata a i b iz G)
3. Neke posebne notacije, poput $(a, b) \mapsto a \circ b$ (npr. u slučaju da promatramo kompoziciju funkcija, a G je skup svih funkcija s nekog nepraznog skupa u samog sebe).

Primjer.
Uređeni parovi $(\mathbb{N}, +)$ i $(\mathbb{N}, -)$ su grupoidi, dok $(\mathbb{N}, -)$ nije grupoid (razlika dvaju prirodnih brojeva ne mora biti prirodan broj).

Polugrupa je grupoid G u kome je operacija asocijativna, odnosno u kome vrijedi $a(bc) = (ab)c$, za sve $a, b, c \in G$.

Radi jednostavnosti zapisa, obično grupoid, koji je uređen par $(G, \cdot)$ kratko označavamo samo s G, pri čemu podrazumijevamo da koristimo multiplikativnu notaciju.

Primjer.
Grupoidi $(\mathbb{N}, +)$ i $(\mathbb{N}, -)$ su polugrupe. Uređen par $(\mathbb{Z}, -)$ je grupoid koji nije polugrupa. Još jedan primjer grupoid koji nije polugrupa je skup vektora u prostoru s binarnom operacijom vektorskog produkta vektora (sjetimo se kako je vektorski produkt vektora u prostoru opet vektor, ali vektorsko množenje vektora nije asocijativno).

Lijeva jedinica u grupoidu G je svaki element a takav da je $ac = c$, za sve $c \in G$. **Desna jedinica** u grupoidu G je svaki element b takav da je $cb = c$, za sve $c \in G$.

Propozicija.
Neka je G grupoid te označimo s $\mathcal{L}(G)$ skup svih lijevih jedinica u G te s $\mathcal{R}(G)$ skup svih desnih jedinica u G. Pretpostavimo da je $\mathcal{L}(G) \neq \emptyset$ i $\mathcal{R}(G) \neq \emptyset$. Tada je $\mathcal{L}(G) = \mathcal{R}(G)$ i $|\mathcal{L}(G)| = 1$.
`Dokaz:`
Sa $|S|$ označavamo broj elemenata skupa S. Neka je $a \in \mathcal{L}(G)$ te $b \in \mathcal{R}(G)$. Tada vrijedi $ab = a$ (jer je b desna jedinica) te $ab = b$ (jer je a lijeva jedinica), odnosno $a = b$ te $\mathcal{L}(G) = \mathcal{R}(G)$ pa je svaka lijeva/desna jedinica također i obostrana jedinica, ili kraće jedinica.

Neka su $a_1, a_2 \in \mathcal{L}(G)$. Tada je $a_1 a_2 = a_2$ i $a_1 a_2 = a_1$ (jer je a_2 i desna jedinica) pa je $a_1 = a_2$ te je $|\mathcal{L}(G)| = 1$.

Jedini element skupa $\mathcal{L}(G) = \mathcal{R}(G)$ nazivamo **jedinica, neutralni ili jedinični element** grupoida G. Najčešće oznake su e, 1 (u slučaju korištenja multiplikativne notacije) te 0 (u slučaju korištenja aditivne notacije, tada neutralni element također nazivamo i nula u G). Ukoliko želimo naglasiti o kojem se grupoidu radi, koristimo oznake $e_G, 1_G$ i 0_G.

Monoid je polugrupa G s jedinicom (neutralnim elementom).

Primjer.
Polugrupe $(\mathbb{N}, \cdot)$ i $(\mathbb{Z}, +)$ su monoidi (s jedinicama 1, odnosno 0). Polugrupa $(\mathbb{N}, +)$ nije monoid, ali $(\mathbb{N} \cup \{0\}, +)$ je monoid.

Neka je G monoid s jedinicom e i neka je $a \in G$. **Lijevi inverz** od a je svaki $b \in G$ takav da je $ba = e$. **Desni inverz** od a je svaki $b \in G$ takav da je $ab = e$.

Propozicija.
Neka je G monoid s jedinicom e te neka je $a \in G$. Označimo s $\mathcal{L}(a)$ skup svih lijevih inveraza od a u G te s $\mathcal{R}(a)$ skup svih desnih inveraza od a u G. Pretpostavimo da je $\mathcal{L}(a) \neq \emptyset$ i $\mathcal{R}(a) \neq \emptyset$. Tada je $\mathcal{L}(a) = \mathcal{R}(a)$ i $|\mathcal{L}(a)| = 1$.
Dokaz:
Za $b \in \mathcal{L}(a)$ i $c \in \mathcal{R}(a)$ redom imamo $b = be = b(ac) = (ba)c = ec = c$ (primijetimo da smo kod treće jednakosti koristili asocijativnost) pa je $b = c$ te $\mathcal{L}(a) = \mathcal{R}(a)$.

Neka su $b_1, b_2 \in \mathcal{L}(a)$. Kako je $\mathcal{L}(a) = \mathcal{R}(a)$, imamo $b_1 = b_1 e = b_1(ab_2) = (b_1 a)b_2 = b_2$ te je $|\mathcal{L}(a)| = 1$.

Jedini element skupa $\mathcal{L}(a)$ nazivamo (obostrani) inverz elementa a. Dio *obostrani* obično izostavljamo. U slučaju korištenja multiplikativne notacije inverz od a označavamo s a^{-1}, dok u slučaju korištenja aditivne notacije inverz od a označavamo s $-a$. U tom slučaju umjesto $a + (-b)$ kratko pišemo $a - b$.

Kažemo da je element a monoida G **invertibilan** ako ima inverz, odnosno ako postoji $a^{-1} \in G$ takav da je $aa^{-1} = a^{-1}a = e$. S $G^\times$ označavamo skup svih invertibilnih elemenata u G.

Grupa je monoid G u kome je svaki element invertibilan, tj. u kojem vrijedi $G^\times = G$.

Primjer.
Monoid $(\mathbb{N}, \cdot)$ nije grupa jer je $\mathbb{N}^\times = \{1\}$. $(\mathbb{Z}, +)$ je grupa. $(\mathbb{Q}, +)$ i $(\mathbb{R}, +)$ su grupe, kao i $(\mathbb{Q} \setminus \{0\}, \cdot)$.

Iz jedinstvenosti inverza slijedi da jednadžba oblika $ax = e$ u monoidu G s neutralnim elementom e ima jedinstveno rješenje $x = a^{-1}$. Primjenom ove činjenice dobivamo iduću propoziciju.

Propozicija.
Neka je G monoid s neutralnim elementom e.

1. Za svaki $a \in G^\times$ je $a^{-1} \in G^\times$ te vrijedi $(a^{-1})^{-1} = a$.
2. Za sve $a, b \in G^\times$ je $ab \in G^\times$ te vrijedi $(ab)^{-1} = b^{-1}a^{-1}$.
3. $e \in G^\times$ te $e^{-1} = e$.

Kažemo da je polugrupa G komutativna ako je operacija u G komutativna, odnosno ako za sve $a, b \in G$ vrijedi $ab = ba$. Komutativnu grupu nazivamo i **Abelova grupa** (po norveškom matematičaru Nielsu Henriku Abelu).

Red grupe G je broj elemenata skupa G, odnosno $|G|$. Kažemo da je grupa G konačna ukoliko je skup G konačan, te da je grupa beskonačna ukoliko nije konačna.

U nastavku ćemo pogledati nekoliko primjera grupa.

Primjeri. Do sad promatrane grupe $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ su sve bile Abelove i beskonačne.

- Skup $\{1, -1\}$ je konačna Abelova grupa uz množenje (primijetimo da je -1 inverz samom sebi).

- Neka je n prirodan broj. Definiramo $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ (skup ostataka pri dijeljenju s n). Na tom skupu definiramo binarnu operaciju *zbrajanja modulo* n, u oznaci $+_n$, s $a +_n b =$ ostatak pri dijeljenju od $a + b$ s n. Sada je $(\mathbb{Z}_n, +_n)$ konačna Abelova grupa reda n. Na primjer, u $\mathbb{Z}_6$ vrijedi $1 +_6 5 = 0$, $3 +_6 3 = 0$ i $2 +_6 4 = 0$, odnosno u $\mathbb{Z}_6$ je 5 inverz od 1 te 4 inverz od 2, dok je 3 inverz samom sebi. Primijetimo: za svaki prirodan broj n postoji grupa reda n.

- Neka je n prirodan broj. S $M_n(\mathbb{R})$ označimo skup svih $n \times n$ matrica čiji elementi su realni brojevi (tj. skup svih realnih kvadratnih matrica n-tog reda). Obzirom na zbrajanja matrica je $M_n(\mathbb{R})$ beskonačna Abelova grupa. Obzirom na množenje matrica je ovaj skup monoid, u kojem je neutralni element jedinična matrica, te je ovaj monoid nekomutativan za $n \geq 2$. Skup svih regularnih matrica u $M_n(\mathbb{R})$ (matrice determinante različite od 0) označavamo s $GL_n(\mathbb{R})$. Uređen par $(GL_n(\mathbb{R}), \cdot)$ je grupa, koju nazivamo *opća linearna grupa*, i koja je nekomutativna za $n \geq 2$.

- Neka je $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : detA = 1\}$. Ovaj skup nazivamo *specijalna linearna grupa*, te se za $n \geq 2$ također radi o nekomutativnoj grupi.

- Neka je $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ (Gaussovi cijeli brojevi). Tada je skup $\mathbb{Z}[i]$ grupa obzirom na zbrajanje.

- Neka je n prirodan broj koji nije potpun kvadrat. Definiramo $S = \{(x, y) \in \mathbb{Z}^2 : x^2 - ny^2 = 1\}$ (skup rješenja Pellove jednadžbe). Na skupu S definiramo binarnu operaciju s $(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 + ny_1y_2, x_1y_2 + x_2y_1)$ (Brahmaguptino kompoziciono pravilo). Uz ovu binarnu operaciju skup S postaje Abelova grupa, s neutralnim elementom $(1, 0)$ te za $(x, y) \in S$ vrijedi $(x, y)^{-1} = (x, -y)$.

- Neka je zadan kvadrat u pravokutnom koordinatnom sustavu tako da njegove stranice leže na pravcima paralelnim koordinatnim osima. Označimo s 1 vrh kvadrata koji se nalazi u drugom kvadrantu, s 2 vrh koji se nalazi u prvom kvadrantu, s 3 vrh koji se nalazi u četvrtom kvadrantu te s 4 vrh koji se nalazi u trećem kvadrantu. Označimo s $D_4^{\times}$ skup transformacija ovog kvadrata (koje preslikavaju kvadrat u samog sebe): $D_4^{\times} = \{I, R, R^2, R^3, T_x, T_y, T_{1,3}, T_{2,4}\}$,

pri čemu je I identiteta, R^i rotacija oko ishodišta za $i \cdot 90^\circ$ $(i = 1, 2, 3)$, T_x refleksija oko x-osi, T_y refleksija oko y-osi, $T_{1,3}$ refleksija oko pravca na kojem leži dijagonala kroz vrhove 1 i 3 te $T_{2,4}$ refleksija oko pravca na kojem leži dijagonala kroz vrhove 2 i 4. Uređen par $(D_4^\times, \circ)$ je neabelova grupa reda 8 (binarna operacija $\circ$ je kompozicija).

Neka je G grupa i $H \subseteq G$, $H \neq \emptyset$. Kažemo da je H **podgrupa grupe** G ako je H grupa obzirom na istu operaciju kao i G. Ako je H podgrupa od G, pišemo $H \leq G$. Ako je $H \leq G$ i $H \neq G$, pišemo $H < G$.

Trivijalni primjeri podgrupa grupa G su $\{e\}$ (pri čemu je s e označen neutralni element grupe G) te G (svaka je grupa ujedno i podgrupa same sebe).

Podgrupu H grupe G koja je različita od G nazivamo i **prava podgrupa**.

Primjeri.

- Neka je n prirodan broj te neka je $n\mathbb{Z} = \{nx : x \in \mathbb{Z}\}$. Tada je $n\mathbb{Z} \leq \mathbb{Z}$.
- $\{0, 3\}$ i $\{0, 2, 4\}$ su prave podgrupe grupe $\mathbb{Z}_6$.

Teorem.
Neka je G grupa i $H \subseteq G$, $H \neq \emptyset$. H je podgrupa od G ako i samo ako je $ab^{-1} \in H$ za sve $a, b \in H$.
`Dokaz:`
Ako je $H \leq G$, tada je H grupa pa za sve $a, b \in H$ vrijedi $b^{-1} \in H$ te $ab^{-1} \in H$.

Obratno, pretpostavimo da je $ab^{-1} \in H$ za sve $a, b \in H$. Kako je $H \neq \emptyset$, postoji $a \in H$. Uzmemo li $b = a$, slijedi $aa^{-1} = e \in H$. Također, uzmemo li sada $a = e$, za svaki $b \in H$ vrijedi $eb^{-1} = b^{-1} \in H$. Sada za $a, b \in H$, zbog $b^{-1} \in H$ vrijedi $ab = a(b^{-1})^{-1} \in H$. Konačno, binarna operacija u H je asocijativna, jer je asocijativna i na G (podsjetimo da je $H \subseteq G$ pa je svojstvo asocijativnosti naslijeđeno). Iz pokazanih svojstava slijedi da je H grupa te je $H \leq G$.

U nastavku ćemo promatrati preslikavanja između grupa koja su u skladu s binarnim operacijama.

Neka su G_1, G_2 grupe, redom uz binarne operacije $\cdot_1$ i $\cdot_2$. Kažemo da je preslikavanje $\varphi : G_1 \to G_2$ **homomorfizam grupa** ako za sve $a, b \in G_1$ vrijedi $\varphi(a \cdot_1 b) = \varphi(a) \cdot_2 \varphi(b)$. (Kratko pišemo $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ podrazumijevajući o kojim se binarnim operacijama radi.)

Injektivni homomorfizam grupa nazivamo **monomorfizam grupa**, surjektivni homomorfizam grupa nazivamo **epimorfizam grupa**.

Ako su G_1, G_2 i G_3 grupe te $\varphi : G_1 \to G_2$ i $\psi : G_2 \to G_3$ grupe, tada je njihova kompozicija $\psi \circ \varphi : G_1 \to G_3$ homomorfizam grupa:

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

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

1. $\varphi(e_{G_1}) = e_{G_2}$,
2. $\varphi(a^{-1}) = \varphi(a)^{-1}, \forall a \in G_1$.

Dokaz:
Iz

$$\varphi(e_{G_1}) = \varphi(e_{G_1}e_{G_1}) = \varphi(e_{G_1})\varphi(e_{G_1})$$

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

Iz

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

slijedi $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Homomorfizam grupa koji je bijekcija nazivamo **izomorfizam grupa**. Kažemo da je grupa G_1 izomorfna grupi G_2 ako postoji izomorfizam s grupe G_1 u grupu G_2. Tada pišemo $G_1 \cong G_2$. Relacija 'biti izomorfan' je relacija ekvivalencije pa obično kažemo da su grupe G_1 i G_2 **izomorfne** umjesto da je grupa G_1 izomorfna grupi G_2.

Neka je $\varphi : G_1 \to G_2$ homomorfizam grupa. Skup $\{\varphi(a) : a \in G_1\}$ nazivamo **slika od** φ te označavamo s $Im\varphi$. Skup $\{a \in G_1 : \varphi(a) = e_{G_2}\}$ nazivamo **jezgra od** φ te označavamo s $Ker\varphi$.

Propozicija.
Neka je $\varphi : G_1 \to G_2$ homomorfizam grupa. Tada je $Ker\varphi \leq G_1$ i $Im\varphi \leq G_2$.
Dokaz:
Dokažimo samo za jezgru. Iskoristit ćemo prethodni teorem. Neka su $a, b \in Ker\varphi$. Tada je

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

pa je i $ab^{-1} \in Ker\varphi$ te je $Ker\varphi \leq G_1$.

Primjeri.

- Neka je r pozitivan realan broj, $r \neq 1$. Definirajmo preslikavanje $\varphi : \mathbb{R} \to \mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ s $\varphi(t) = r^t$. Kako je $\varphi(t_1 + t_2) = r^{t_1+t_2} = r^{t_1} + r^{t_2} = \varphi(t_1) + \varphi(t_2)$, ovo preslikavanje je homomrofizam grupa $(\mathbb{R}, +)$ i $(\mathbb{R}^\times, \cdot)$.

- Prema Binet-Cauchyjevu teoremu je determinanta homomorfizam grupa $GL_n(\mathbb{R})$ i $(\mathbb{R}^\times, \cdot)$. Jezgra ovog homomorfizma je upravo grupa $SL_n(\mathbb{R})$.

- Neka je n prirodan broj. Definiramo preslikavanje $\varphi_n : \mathbb{Z} \to n\mathbb{Z}$ s $\varphi_n(x) = n \cdot x$. Ovo preslikavanje je izomorfizam grupe $\mathbb{Z}$ i njene podgrupe $n\mathbb{Z}$.

Na kraju ovog potpoglavlja ćemo se upoznati s jednim posebno važnim primjerom grupe. Neka je T neprazan skup. Označimo s T^T skup svih funkcija sa skupa T u samog sebe. S binarnom operacijom kompozicije funkcije skup T^T postaje monoid u kojem je neutralni element identiteta, funkcija $id_T : T \to T$ takva da je $id_T(x) = x$ za sve $x \in T$.

Sada je $(T^T)^\times$ skup svih bijekcija sa skupa T u samog sebe, te je uz binarnu operaciju kompozicije funkcija skup svih bijekcija sa skupa T u samog sebe grupa, koju nazivamo **grupa permutacija skupa** T. Ova grupa je nekomutativna za $|T| \geq 3$.

Ako je $|T| = n$, tada grupu permutacija skupa T nazivamo simetrična grupa n-tog reda te ju označavamo sa S_n. U tom slučaju možemo uzeti da je $T = \{1, 2, \ldots, n\}$.

Za $\sigma, \tau \in S_n$ ćemo kompoziciju $\sigma \circ \tau$ kraće označavati sa $\sigma\tau$ te nazivati **produkt permutacija** σ i τ.

Neka je n prirodan broj te k prirodan broj takav da je $2 \leq k \leq n$. Kažemo da je permutacija $\sigma \in S_n$ k-**ciklus** ukoliko σ ostavlja fiksnim $n - k$ elemenata dok preostalih k elemenata u nekom poretku ciklički permutira, odnosno postoje $c_1, c_2, \ldots, c_k$, $c_i \neq c_j$ za $i \neq j$, takvi da je $\sigma(c_1) = c_2$, $\sigma(c_2) = c_3, \ldots, \sigma(c_{k-1}) = c_k$, $\sigma(c_k) = c_1$ te $\sigma(x) = x$ za sve $x \notin \{c_1, c_2, \ldots, c_k\}$. Kažemo da su ciklusi **disjunktni** ukoliko su odgovarajući podskupovi koje ciklički permutiraju disjunktni. 2-ciklus zovemo **transpozicija**.

Primijetimo da disjunktni ciklusi komutiraju.

Propozicija.
Svaka permutacija $\sigma \in S_n$ je ili ciklus ili produkt međusobno disjunktnih ciklusa, koji su jedinstveno određeni sa σ. Svaka permutacija $\sigma \in S_n$, $\sigma \neq id$, je ili transpozicija ili produkt transpozicija.

Kažemo da je permutacija parna ako se može zapisati u obliku produkta parno mnogo transpozicija. Kažemo da je permutacija neparna ako se može zapisati u obliku produkta neparno mnogo transpozicija. Ako je permutacija σ parna, tada kažemo da je predznak permutacije σ jednak 1, te pišemo $sgn(\sigma) = 1$. Ako je permutacija σ neparna, tada kažemo da je predznak permutacije σ jednak -1, te pišemo $sgn(\sigma) = -1$.

Propozicija.

1. Permutacija σ ne može istovremeno biti parna i neparna.
2. $sgn(id) = 1$.
3. Za $\sigma, \tau \in S_n$ vrijedi $sgn(\sigma\tau) = sgn(\sigma)sgn(\tau)$.
4. Za $\sigma \in S_n$ vrijedi $sgn(\sigma^{-1}) = sgn(\sigma)$.

Red grupe S_n je jednak $n!$ (primijetimo da se naziv simetrična grupa n-tog reda ne odnosi na sam red grupe S_n, već na broj elemenata skupa nad kojim je ta grupa definirana). Skup svih parnih permutacija u S_n označavamo s A_n. Grupa A_n se naziva alternirajuća grupa (n-tog reda), A_n je prava podgrupa od S_n te je red od A_n jednak $\frac{n!}{2}$.

Normalne podgrupe i kvocijente grupe

U ovom potpoglavlju dobivamo prve rezultate o strukturi konačnih grupa.

Neka je G grupa i H podgrupa od G. Neka su $a, b \in G$. Kažemo da je a **desno kongruentan** b **modulo** H, u oznaci $a \sim^H b$, ako je $b^{-1}a \in H$.

Primjer.
Neka je n prirodan broj. Tada je $n\mathbb{Z}$ podgrupa od $\mathbb{Z}$. Neka su $a, b \in \mathbb{Z}$ takvi da je a desno kongruentan b modulo $n\mathbb{Z}$. Tada je $(-b) + a \in n\mathbb{Z}$, odnosno n dijeli $a - b$. Drugim riječima, tada je a kongruentno b modulo n.

Lema.

1. Biti desno kongruentan modulo H je relacija ekvivalencije na G.

2. Ako s $[a]$ označimo klasu ekvivalencije elementa $a \in G$, tada je

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

(aH je samo oznaka za skup $\{ah : h \in H\}$)

`Dokaz:`
Relacija ekvivalencije je refleksivna, simetrična i tranzitivna. Neka je $a \in G$ te označimo neutralni element grupe G s e. Kako je H podgrupa od G, vrijedi $a^{-1}a = e \in H$ pa je $a \sim^H a$ i relacija je refleksivna.

Neka su sada $a, b \in G$ te neka je $a \sim^H b$. Tada je $b^{-1}a \in H$, a kako je H grupa slijedi $(b^{-1}a)^{-1} = a^{-1}b \in H$, odnosno $b \sim^H a$ te je relacija i simetrična.

Konačno, neka su $a, b, c \in G$ takvi da je $a \sim^H b$ i $b \sim^H c$. Tada je $b^{-1}a, c^{-1}b \in H$ te korištenjem asocijativnosti i činjenice da je H grupa pa sadrži produkt svojih elemenata dobivamo $(c^{-1}b)(b^{-1}a) = c^{-1}(b^{-1}b)a = c^{-1}a \in H$, te je relacija i tranzitivna.

Neka je $a \in G$. Iz definicije i svojstva simetričnosti slijedi

$$[a] = \{b \in G : a \sim^H b\} = \{b \in G : b \sim^H a\} = \{b \in G : a^{-1}b \in H\} =$$
$$\{b \in G : a^{-1}b = h, \text{za neki } h \in H\} = \{b \in G : b = ah, \text{za neki } h \in H\} = \{ah : h \in H\}.$$

Klase ekvivalencije aH, $a \in G$, nazivamo **desne klase u** G **u odnosu na podgrupu** H, ili, kraće, **desne** H**-klase u** G. Grupa G je disjunktna unija svih svojih desnih H-klasa.

Analogno relaciji biti desno kongruentan modulo H definiramo i relaciju biti lijevo kongruentan modulo H, u oznaci ${}^H\!\sim$:

Neka je G grupa i H podgrupa od G. Neka su $a, b \in G$. Kažemo da je a **lijevo kongruentan** b **modulo** H ako je $ab^{-1} \in H$.

Opet se radi o relaciji ekvivalencije na G, klasa ekvivalencije elementa $a \in G$ jednaka je $\{ha : h \in H\}$, označava se s Ha te ju nazivamo lijeva H-klasa u G.

Lema.
Za svaki $a \in G$ vrijedi

$$|aH| = |H| = |Ha|.$$

Dokaz:
Primijetimo da su preslikavanja $Ha \to H$ dano s $ha \mapsto h$ i $aH \to H$ dano s $ah \mapsto h$ bijekcije.

Teorem (Lagrange). Neka je G konačna grupa i H podgrupa od G. Tada je red grupe G djeljiv redom grupe H, odnosno $|H|$ dijeli $|G|$. Preciznije, ako je $|G| = n$, $|H| = k$ i ako je broj desnih H-klasa u G jednak p, tada je $n = p \cdot k$.
Dokaz:
Neka su $a_1, a_2, \ldots, a_p$ predstavnici svih desnih H-klasa u G. Tada je

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

pri čemu se radi o disjunktnoj uniji. Zato je

$$|G| = |a_1H| + |a_2H| + \cdots + |a_pH|$$

te iz prethodne leme slijedi $|G| = p|H|$, odnosno $n = p \cdot k$.

Kažemo da je podgrupa H grupe G podgrupa konačnog indeksa ako postoji (samo) konačno mnogo različitih desnih H-klasa u G (kako je broj lijevih H-klasa je jednak broju desnih H-klasa, svejedno je koristimo li lijeve ili desne H-klase u definiciji). Broj desnih H-klasa u G označavamo s $[G : H]$ te nazivamo **indeks od** H **u** G. Ukoliko je grupa G konačna, prema Lagrangeovu teoremu vrijedi

$$[G : H] = \frac{|G|}{|H|}.$$

Kažemo da je podgrupa H grupe G **normalna podgrupa** ako je $Hc = cH$ za sve $c \in G$. Ukoliko je H normalna podgrupa od G, tada pišemo

$$H \trianglelefteq G.$$

Jednakost $Hc = cH$ je jednakost skupova: $\{hc : h \in H\} = \{ch : h \in H\}$. Zato je u Abelovoj grupi svaka podgrupa normalna.

Definirajmo $cHc^{-1} = \{chc^{-1} : h \in H\}$. Tada je H normalna podgrupa od G ako i samo ako za svaki $c \in G$ vrijedi $cHc^{-1} = H$. Zaista, neka je najprije H normalna podgrupa od G te neka je $c \in G$ i $h_1 \in H$. Iz $Hc = cH$ slijedi da postoji $h_2 \in H$ takav da je $ch_1 = h_2c$, odakle je $ch_1c^{-1} = h_2$ pa je $cHc^{-1} \subseteq H$. Slično, uvrstimo li c^{-1} umjesto c, dobivamo da postoji $h_2 \in H$ takav da je $c^{-1}h_1 = h_2c^{-1}$, odakle je $h_1 = ch_2c^{-1}$ te je $H \subseteq cHc^{-1}$ te iz dobivenih dvaju inkluzija slijedi $cHc^{-1} = H$. Pretpostavimo sada da je $cHc^{-1} = H$ za sve $c \in G$. Neka su $h_1 \in H$ i $c \in G$. Tada postoji $h_2 \in H$ za koji je $ch_1c^{-1} = h_2$, odakle je $ch_1 = h_2c$, odakle je $cH \subseteq Hc$. Također, postoji i $h_3 \in H$ takav da je $c^{-1}h_1c = h_3$, odakle je $h_1c = ch_3$ te $Hc \subseteq cH$. Iz dobivenih inkluzija slijedi $cH = Hc$ pa je H normalna podgrupa od G.

Neka je $H \trianglelefteq G$. S G/H označavamo skup svih H-klasa u G. Primijetimo da iz definicije normalne podgrupe slijedi da se lijeve i desne H-klase u G podudaraju, zato nije potrebno napomenuti radi li se o skupu svih lijevih ili desnih H-klasa u G. Na skupu G/H definiramo binarnu operaciju:

$$(aH)(bH) = abH, a, b \in G.$$

Najprije trebamo provjeriti da li je ova operacija dobro definirana, tj. da ne ovisi o odabiru predstavnika H-klase. Neka su $a, b, a', b' \in G$ takvi da je

$$aH = a'H$$
$$bH = b'H.$$

Tada su a i a' te b i b' predstavnici istih H-klasa, odnosno postoje $h_1, h_2 \in H$ takvi da je $a^{-1}a' = h_1$ i $b^{-1}b' = h_2$ (jer su, kao predstavnici istih H-klasa a i a' te b i b' međusobno desno kongruentni modulo H). Odatle slijedi $a' = ah_1$ i $b' = bh_2$ (primijetimo da se predstavnici istih H-klasa razlikuju za element iz H).

Sada je

$$a'b' = ah_1bh_2 = abb^{-1}h_1bh_2$$

a kako je H normalna podgrupa od G slijedi $b{-}1h_1b \in H$ te postoji $h_3 \in H$ takav da je

$$a'b' = abh_3h_2.$$

Sada iz $h_2, h_3 \in H$ slijedi $h_3h_2 \in H$ te $abH = a'b'H$, jer se ab i $a'b'$ također razlikuju za element iz H.

Sada G/H postaje grupe, s neutralnim elementom $eH = H$, pri čemu je, za $a \in G$, inverz elementa aH jednak $a^{-1}H$ (primijetimo da je

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

pa je $(aH)^{-1} = a^{-1}H$).

Grupu G/H nazivamo **kvocijentna grupa grupe G po normalnoj podgrupi H**.

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

1. $Ker\varphi$ je normalna podgrupa grupe G_1. Označimo jezgru od φ s H.
2. Preslikavanje $\Phi : G_1/H \to Im\varphi$ definirano s $\Phi(aH) = \varphi(a), a \in G_1$, je izomorfizam kvocijentne grupe G_1/H na grupu $Im\varphi$.

Drugi dio ovog teorema nazivamo **Prvi teorem o izomorfizmu** (postoje još dva teorema o izomorfizmu).
`Dokaz:`
Dokažimo najprije da je jezgra homomorfizma normalna podgrupa. Kao i u iskazu, označimo jezgru od φ s H. Neka su $c \in G_1$ i $h \in H$. Tada je

$$\varphi(chc^{-1}) = \varphi(c)\varphi(h)\varphi(c^{-1}) = \varphi(c)\varphi(c^{-1}) = \varphi(cc^{-1}) = \varphi(e_{G_1}) = e_{G_2}.$$

Zato je $chc^{-1} \in H$, odakle slijedi $cHc^{-1} \subseteq H$. Uvrstimo li c^{-1} umjesto c (što možemo učiniti jer prethodna relacija vrijedi za svaki element grupa G_1), slijedi da postoji $h' \in H$ takav da je $c^{-1}hc = h'$, odakle je $h = ch'c^{-1}$ te $H \subseteq cHc^{-1}$, odakle je $H = cHc^{-1}$ i H je normalna podgrupa od G_1.

Pokažimo sada drugi dio teorema. Kako je preslikavanje Φ definirano na predstavniku klase ekvivalencije, opet najprije treba provjeriti da definicija ne ovisi o

odabiru predstavnika. Neka su $a, a' \in G_1$ takvi da je $aH = a'H$, tj. neka su aH i $a'H$ predstavnici iste klase ekvivalencije. Tada postoji $h \in H$ takav da je $a' = ah$ pa je

$$\Phi(a'H) = \varphi(a') = \varphi(ah) = \varphi(a)\varphi(h) = \varphi(a) = \Phi(aH)$$

te je preslikavanje Φ dobro definirano.

Za $a, b \in G_1$ vrijedi

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

pa je Φ homomorfizam grupa. Iz definicije preslikavanja Φ direktno slijedi da je Φ surjekcija, jer je kodomena od Φ upravo slika od φ. Preostaje dokazati da je Φ injekcija. Neka su $aH, bH \in G_1/H$ takvi da je $\Phi(aH) = \Phi(bH)$. Tada je $\varphi(a) = \varphi(b)$, odakle množenjem obiju strana prethodne jednakosti s $\varphi(b)^{-1} = \varphi(b^{-1})$ s lijeva slijedi

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

odakle je $b^{-1}a \in H$ te $a \sim^H b$, odnosno $aH = bH$. Time je pokazano da je Φ izomorfizam grupa.

Primjer.
Neka je n prirodan broj. Tada je $n\mathbb{Z}$ normalna podgrupa od $\mathbb{Z}$, jer je grupa $\mathbb{Z}$ Abelova. Definiramo preslikavanje $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ s $\varphi(a) =$ ostatak pri dijeljenju od a s n. Tada je φ epimorfizam grupa i jezgra od φ je jednaka $n\mathbb{Z}$. Prema Prvom teoremu o izomorfizmu je

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n.$$

Neka je G grupa. Podskup $Z(G) = \{x \in G : xa = ax \forall a \in G\}$ nazivamo **centar grupe** G. Centar grupe G sadrži upravo one elemente iz G koji komutiraju sa svim elementima iz G. Zato je $e \in Z(G) \subseteq G$ te $Z(G) = G$ ako i samo ako je G Abelova.

Centar grupe G je normalna komutativna podgrupa od G. Ako je H podgrupa od G i $H \subseteq Z(G)$, tada je H normalna podgrupa od G i takvu podgrupu nazivamo **centralna podgrupa grupe** G.

Primjer.

1. $Z(GL_n(\mathbb{R})) = \{\lambda I_n : \lambda \in \mathbb{R} \setminus \{0\}\}$ (I_n je jedinična matrica reda n)
2. $Z(SL_n(\mathbb{R})) = \{I_n\}$ ukoliko je n neparan te $Z(SL_n(\mathbb{R})) = \{I_n, -I_n\}$ ukoliko je n paran.
3. $Z(S_2) = S_2$, $Z(S_n) = \{id\}$ za $n \geq 3$.

Cikličke grupe

Neka je G grupa, e neutralni element u grupi G te neka je $a \in G$. Definirajmo potencije elementa a: $a^0 = e$, $a^1 = a$, $a^n = a^{n-1} \cdot a$ za $n \in \mathbb{N}$, $n \geq 2$. Ovim su definirane sve nenegativne potencije od a. Također, za $n \in \mathbb{N}$ definiramo $a^{-n} = (a^n)^{-1}$ te smo na taj način definirali sve cjelobrojne potencije od a.

Prethodnu definiciju ćemo iskoristiti za definiciju preslikavanja $\Phi_a : \mathbb{Z} \to G$, $\Phi_a(n) = a^n$. Primijetimo da za cijele brojeve m i n vrijedi $\Phi_a(m+n) = a^{m+n} = a^m \cdot a^n = \Phi_a(m) \cdot \Phi_a(n)$ pa je Φ_a homomorfizam s grupe cijelih brojeva u grupu G. Sliku ovog homomorfizma označavamo s $\langle a \rangle$. Očito je $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$, $\langle a \rangle$ je podgrupa od G te je $\langle a \rangle$ i najmanja podgrupa od G koja sadrži element a (ako je $H \leq G$ i $a \in H$, tada je i $a^n \in H$, za sve $n \in \mathbb{Z}$, tj. $\langle a \rangle \subseteq H$).

Za podgrupu $\langle a \rangle$ kažemo da je *generirana elementom* a. Primijetimo da je $\langle a \rangle$ Abelova grupa, jer vrijedi $a^m \cdot a^n = a^n \cdot a^m$, za sve cijele brojeve m i n.

Općenito, ako je $S \subseteq G$, $S \neq \emptyset$, za najmanju podgrupu od G koja sadrži skup S kažemo da je *generirana skupom* S te takvu podgrupu označavamo sa $\langle S \rangle$. Ako je S jednočlan skup, $S = \{a\}$, koristimo notaciju $\langle a \rangle = \langle \{a\} \rangle$. Primijetimo da vrijedi $\langle S \rangle = \{a_1^{n_1} \cdot a_2^{n_2} \cdots a_k^{n_k} : a_i \in S, n_i \in \mathbb{Z}, k \in \mathbb{N}\}$.

Grupu generiranu jednim elementom nazivamo **ciklička grupa**.

Slika preslikavanja Φ_a je ciklička grupa $\langle a \rangle$, a jezgra tog preslikavanja je $Ker\Phi_a = \{n \in \mathbb{Z} : a^n = e\}$. Prema Prvom teoremu o izomorfizmu vrijedi

$$\mathbb{Z}/Ker\Phi_a \cong \langle a \rangle.$$

Za opis cikličkih grupa nam je prema tome potreban opis podgrupa grupe cijelih brojeva, jer je $Ker\Phi_a$ podgrupa od $\mathbb{Z}$.

Lema.
Neka je K podgrupa od $\mathbb{Z}$. Tada je ili $K = \{0\}$ ili postoji prirodan broj n takav da je $K = n\mathbb{Z}$.

Dokaz:
Neka je $K \neq \{0\}$. Tada postoji $m \in K$ takav da je $m \neq 0$. Kako je K grupa, slijedi $m, -m \in K$ te je $K \cap \mathbb{N} \neq \emptyset$. Svaki neprazan podskup skupa prirodnih brojeva sadrži najmanji element, pa postoji i najmanji element skupa $K \cap \mathbb{N}$. Označimo ga s n. Kako je $n \in K$ i K je grupa, odmah slijedi da je $n\mathbb{Z} \subseteq K$. S druge strane, neka je $k \in K$. Prema Teoremu o dijeljenju s ostatkom, postoje cijeli brojevi p, q takvi da je $k = p \cdot n + q$ i $0 \leq q < n$. Odatle je $q = k - p \cdot n$, a kako su i k i n elementi grupe K slijedi da je i q element iz K. Iz definicije od n slijedi $q = 0$ pa je k djeljiv s n, tj. $k \in n\mathbb{Z}$ te $K \subseteq n\mathbb{Z}$. Iz prethodnih dviju inkluzija slijedi $K = n\mathbb{Z}$.

Prema prethodnoj lemi, ciklička je grupa $\langle a \rangle$ izomorfna ili $\mathbb{Z}/0$ ili $\mathbb{Z}/n\mathbb{Z}$. Prisjetimo se da je $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. S druge strane, preslikavanje $\varphi : \mathbb{Z} \to \mathbb{Z}$ dano s $\varphi(x) = x$, je izomorfizam i ima trivijalnu jezgru pa Prvi teorem o izomorfizmu povlači da je $\mathbb{Z}/\{0\} \cong \mathbb{Z}$. Time smo dokazali idući teorem:

Teorem.
Neka je G grupa i $a \in G$. Tada vrijedi jedno od idućeg:

- Ciklička grupa $\langle a \rangle$ je beskonačna grupa. Tada je $\langle a \rangle \cong \mathbb{Z}$ i Φ_a je injekcija, tj. $a^n \neq a^m$ za $n \neq m$. Primijetimo da je tada i $a^n \neq e$ za $n \neq 0$.
- Ciklička grupa $\langle a \rangle$ je konačna grupa. Tada je $\langle a \rangle \cong \mathbb{Z}_n$ i $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$, za neki prirodan broj n.

Primjer
Neka je n prirodan broj koji nije potpun kvadrat. Ranije smo vidjeli da rješenja Pellove jednadžbe $x^2 - ny^2 = 1$ čine grupu. Kako se sva rješenja Pellove jednadžbe mogu dobiti iz najmanjeg netrivijalnog rješenja, ova grupa je generirana takvim rješenjem pa je ciklička. Osim toga, Pellova jednadžba ima beskonačno mnogo rješenja pa ova grupa nije konačna te je izomorfna grupi cijelih brojeva.

Neka je G grupa i $a \in G$. **Red elementa** a je red cikličke grupe $\langle a \rangle$. Ako je grupa $\langle a \rangle$ konačna, tada je red elementa a najmanji prirodan broj k za koji vrijedi $a^k = e$ te za $0 \leq i, j < k$, $i \neq j$, vrijedi $a^i \neq a^j$.

Jedinica $e \in G$ je jedini element reda 1. Prema Lagrangeovu teoremu, red elementa dijeli red grupe. Ako je $|G|$ prost broj, tada je red elementa $a \in G$, $a \neq e$, jednak $|G|$, tj. $\langle a \rangle = G$, za svaki $a \in G$, $a \neq e$. Dobivamo sljedeći rezultat:
Propozicija.
Neka je G grupa prostog reda. Tada je svaki $a \in G$, $a \neq e$, generator grupe G, $\langle a \rangle = G$. Svaka grupa prostog reda je ciklička pa i Abelova.

Propozicija.
Neka je G ciklička grupa i H podgrupa od G. Tada su i grupe H i G/H cikličke.
`Dokaz:`
Primijetimo da je G Abelova grupa pa je H i normalna podgrupa te je definirana kvocijentna grupa G/H.

Ako G nije konačna grupa, tada je G izomorfna grupi cijelih brojeva. Podgrupe grupe cijelih brojeva su oblika $n\mathbb{Z}$, a kvocijentne grupe su oblika $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ pa su i podgrupe i kvocijente grupe cikličke ($n\mathbb{Z} = \langle n \rangle$, $\mathbb{Z}_n = \langle 1 \rangle$).

Pretpostavimo sada da je G konačna ciklička grupa i neka je $a \in G$ takav da je $G = \langle a \rangle$. Kvocijentna grupa G/H je očito generirana s aH pa je ciklička. Ako je $H = \{e\}$, H je očito ciklička. Ako je $H \neq \{e\}$, tada postoji $n \in \mathbb{N}$ takav da je $a^n \in H$. Skup svih prirodnih brojeva n za koje je $a^n \in H$ je zato neprazan pa sadrži najmanji element, kojeg ćemo označiti s m. Kako je $a^m \in H$, slijedi i $\langle a^m \rangle \subseteq H$. Uzmimo sada neki element $b \in H$. Kako je H podgrupa od G, slijedi da je $b = a^n$ za neki nenegativan cijeli broj n. Prema Teoremu o dijeljenju s ostatkom, postoje nenegativni cijeli brojevi p i q takvi da je $n = p \cdot m + q$ i $0 \leq q < m$. Sada je $b = a^n = a^{p \cdot m + q} = (a^m)^p \cdot a^q$. Odavde je $a^q = b \cdot ((a^m)^p)^{-1}$ pa je i $a^q \in H$ te zbog $0 \leq q < m$ slijedi $q = 0$. Zato je $b = a^n = (a^m)^q \in \langle a^m \rangle$. Sada dobivamo $H \subseteq \langle a^m \rangle$ te $\langle a^m \rangle = H$. Time je propozicija dokazana.

Djelovanje grupa

Posebno važna primjena grupa se očituje pri njihovom djelovanju 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 element a grupe G zadana bijekcija $\varphi_a : S \to S$ te za $a, b \in G$ vrijedi $\varphi_a \circ \varphi_b = \varphi_{ab}$. Primijetimo da s φ_a označavamo element grupe permutacija skupa S, tj. bijekciju sa skupa S u samog sebe, koji je pridružen elementu a grupe G. Činjenica da za $a, b \in G$ vrijedi $\varphi_a \circ \varphi_b = \varphi_{ab}$ znači da je ovo pridruživanje homomorfizam. Iz svojstava homomorfizma slijedi $\varphi_e = id_S$, gdje je e neutralni element grupe G, a id_S identiteta na skupu S ($id_S(x) = x, \forall x \in S$).

Najčešće se zadano djelovanje grupe G na nekom skupu zapisuje bez posebnih oznaka za funkciju φ_a te za $a \in G$ i $x \in S$ definiramo $ax = \varphi_a(x)$. Koristeći ovaj zapis, djelovanje grupe G na skupu S možemo opisati zadavanjem preslikavanja s $G \times S$ u S, koje uređenom paru $(a, x) \in G \times S$ pridružuje ax, sa sljedećim svojstvima:

1. za svaki $a \in G$ je pridruživanje $x \mapsto ax$ bijekcija sa S na S,
2. za sve $a, b \in G$ i $x \in S$ vrijedi $a(bx) = (ab)x$.

Primjer
Simetrična grupa n-tog reda S_n djeluje na skupu $I_n = \{1, 2, \ldots, n\}$ na način da je uređenom paru $(\sigma, x) \in S_n \times I_n$ pridruženo $\sigma(x)$.

Primjer
Neka je H podgrupa grupe G. Jedno djelovanje grupe H na skupu G je dano pridruživanjem $(h, x) \mapsto hx$, gdje je hx uobičajeni produkt u G. Ranije smo vidjeli, prije dokaza Lagrangeova teorema, da je za $a \in G$ preslikavanje $G \to G$ dano s $x \mapsto ax$ bijekcija. Ovo djelovanje nazivamo *lijeva translacija*.

Djelovanje grupe G na skupu S zadaje relaciju ekvivalencije na S: za $x, y \in S$ stavljamo $x \sim y$ (x je u relaciji s y, x je ekvivalentno y) ako postoji $a \in G$ takav da je $y = ax$.

Provjerimo svojstva relacije ekvivalencije:

- refleksivnost: za $x \in S$ je $ex = x$ pa je $x \sim x$ (sjetimo se da je, prema našim oznakama, $ex = \varphi_e(x) = id_S(x) = x$).
- simetričnost: neka su $x, y \in S$ takvi da je $x \sim y$. Tada je $y = ax$ za neki $a \in G$. Djelovanjem s a^{-1} na prethodnu jednakost, dobivamo $a^{-1}y = a^{-1}(ax) = (a^{-1}a)x = x$ pa je $y \sim x$.
- tranzitivnost: neka su $x, y, z \in S$ takvi da je $x \sim y$ i $y \sim z$. Tada postoje $a, b \in G$ takvi da je $y = ax$ i $z = by$ te iz svojstava djelovanja grupe na skupu slijedi $z = (ba)x$ te $x \sim z$.

Klase ekvivalencije u skupu S obzirom na ovu relaciju nazivamo G-**orbite**. Dakle, G-orbita elementa $x \in S$ je skup

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

Za svaki $x \in S$ je $x \in O(x)$.

Za $x \in S$ također definiramo i $G_x = \{a \in G : ax = x\}$.

Lema.
Za $x \in S$ je G_x podgrupa od G.
Dokaz:
Neka su $a, b \in G_x$. Iz $bx = x$, djelovanjem s b^{-1}, dobivamo $x = b^{-1}x$ pa je i $b^{-1} \in G_x$. No, tada vrijedi i $(ab^{-1})x = a(b^{-1}x) = ax = x$ te je i $ab^{-1} \in G_x$ i prema ranijem kriteriju je G_x podgrupa od G.

Grupu G_x nazivamo **stabilizator od** x **u** G.

Propozicija.
Neka je zadano djelovanje grupe G na skupu S i neka je $x \in S$. Tada je preslikavanje zadano s $aG_x \mapsto ax$ bijekcija sa skupa svih desnih G_x-klasa u grupi G na G-orbitu $O(x)$ elementa $x \in S$. Posebno, ako je grupa G konačna, tada je broj elemenata G-orbite $O(x)$ jednak $[G : G_x]$, indeksu stabilizatora G_x od x u grupi G.
Dokaz:
Označimo skup svih desnih G_x-klasa u grupi G s G/G_x. Provjerimo najprije da je preslikavanje $G/G_x \to O(x)$ dano s $aG_x \mapsto ax$ dobro definirano, tj. da ne ovisi o odabiru predstavnika: neka su $a, b \in G$ takvi da je $aG_x = bG_x$ (drugim riječima, a i b su predstavnici iste desne G_x-klase u grupi G). Po definiciji desne G_x-klase je $a \sim_{G_x} b$ te je $b^{-1}a \in G_x$. Zato je $b^{-1}ax = x$ te $ax = bx$, što je i trebalo pokazati.

Preslikavanje $G/G_x \to O(x)$ dano s $aG_x \mapsto ax$ je očito surjekcija. Preostaje provjeriti da je i injekcija. Neka su $aG_x, bG_x \in G/G_x$ takvi da je $ax = bx$. Tada je i $b^{-1}ax = x$ pa je $a \sim_{G_x} b$ te $aG_x = bG_x$ i promatrano preslikavanje je bijekcija.

Drugi dio propozicije je direktna posljedica Lagrangeova teorema.

Nešto kasnije ćemo iskoristiti iduću posljedicu prethodne propozicije.

Korolar.
Neka je p prost broj i n prirodan broj. Ako grupa G reda p^n djeluje na konačnom skupu S i ako sa S_0 označimo $\{x \in S : ax = x, \forall a \in G\}$, tada je

$$|S| \equiv |S_0| \pmod{p}.$$

Dokaz:
Ako je $x \in S_0$, tada G-orbita $O(x)$ sadrži samo jedan element, tj. $O(x) = \{x\}$ ako i samo je $x \in S_0$. Prema tome, za $y \in S \setminus S_0$ je $|O(y) \geq 2$.

Skup S možemo prikazati kao disjunktnu uniju svih klasa ekvivalencije obzirom na relaciju ekvivalenciju dobivenu djelovanjem grupe G na skupu S te postoje $x_1, x_2, \ldots, x_m$ takvi da je $S = S_0 \cup O(x_1) \cup O(x_2) \cup \ldots \cup O(x_m)$ (disjunktna unija) te $|O(x_i)| \geq 2$ za $i = 1, 2, \ldots, m$.

Za $i = 1, 2, \ldots, m$, prema prethodnoj propoziciji je $|O(x_i| = [G : G_{x_i}]$, a prema Lagrangeovu teoremu $[G : G_{x_i}]$ dijeli $|G| = p^n$. Slijedi da $|O(x_i)|$ dijeli

p^n, za $i = 1, 2, \ldots, m$, a kako je $|O(x_i)| \geq 2$ dobivamo da p dijeli $|O(x_i)|$ te je $|O(x_i)| \equiv 0 \pmod{p}$.

Iz svojstva disjunktne unije je $|S| = |S_0| + |O(x_1)| + |O(x_2)| + \cdots + |O(x_m)|$ pa je $|S| \equiv |S_0| + |O(x_1)| + |O(x_2)| + \cdots + |O(x_m)| \pmod{p}$ te $|S| \equiv |S_0| \pmod{p}$.

Idući rezultat prikazuje posebnu važnost grupe permutacija.

Teorem (Cayley).
Neka je G grupa. Označimo sa $S(G)$ grupu permutacija skupa G. Tada postoji monomorfizam s G u $S(G)$. Prema tome, svaka grupa je izomorfna podgrupi grupe permutacija. Posebno, svaka konačna grupa reda n je izomorfna nekoj podgrupi od simetrične grupe n-tog reda S_n.

Dokaz:
Promatramo djelovanje grupe G na samu sebe lijevom translacijom. Za $a \in G$, označimo s φ_a preslikavanje s G u G definirano s $\varphi_a(g) = ag$, za $g \in G$. Tada je preslikavanje $a \mapsto \varphi_a$ homomorfizam s G u $S(G)$, jer za $a, b \in G$ vrijedi $\varphi_{ab} = \varphi_a \circ \varphi_b$.

Pokažimo da je ovo preslikavanje i injekcija: neka su $a, b \in G$ takvi da je $\varphi_a = \varphi_b$. Tada je $ag = bg$ za $g \in G$, odakle slijedi $a = b$ te smo pokazali da je preslikavanje injektivno.

Kako je ovo preslikavanje injektivno, ima trivijalnu jezgru jednaku $\{e\}$, gdje je e neutralni element grupe G. Označimo li sliku ovog preslikavanja s H, iz Prvog teorema o izomorfizmu slijedi $G/\{e\} \cong H \leq S(G)$. Kako je $G/\{e\} \cong G$, pokazali smo da je grupa G je izomorfna podgrupi grupe permutacija skupa G. Ako je red grupe G jednak n, tada je grupa $S(G)$ izomorfna grupi S_n, čime je teorem dokazan.

Pogledajmo još neke primjere djelovanja grupa.

Najprije pogledajmo djelovanje grupe G na samu sebe koje nazivamo **konjugiranje**. Tada za $a \in G$ bijekciju $\varphi_a : G \to G$ pridruženu elementu a definiramo s $\varphi_a(x) = axa^{-1}$. Može se direktno provjeriti da je ovo preslikavanje bijekcija, dok za $a, b \in G$ vrijedi $\varphi_a(\varphi_b(x)) = \varphi_a(bxb^{-1}) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = \varphi_{ab}(x)$.

Za elemente koji se ekvivalentni obzirom na ovo djelovanje kažemo da su G-konjugirani. Dakle, $x, y \in G$ su G-konjugirani ako postoji $a \in G$ takav da je $x = aya^{-1}$. Za $x \in G$ orbitu $O(x) = \{axa^{-1} : a \in G\}$ nazivamo *klasa konjugiranosti*. Stabilizator elementa $x \in G$ označavamo sa $C_G(x)$ i nazivamo *centralizator elementa* x. Primijetimo da je $C_G(x) = \{a \in G : axa^{-1} = x\} = \{a \in G : ax = xa\}$ te

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

gdje je $Z(G)$ centar grupe G.

Grupa G također djeluje konjugiranjem i na skupu $\mathcal{G}$ svih podgrupa od G: za $a \in G$ i $H \in \mathcal{G}$ $(H \leq G)$ definiramo $\Phi_a(H) = aHa^{-1} = \{aha^{-1} : h \in H\}$. Tada je i $\Phi_a(H) \leq G$ te $\Phi_{ab} = \Phi_a \circ \Phi_b$.

Kažemo da su podgrupe H i K grupe G *konjugirane* u grupi G ako postoji $a \in G$ takav da je $K = aHa^{-1} = \Phi_a(H)$. Stabilizator podgrupe $H \in \mathcal{G}$ označavamo s $N_G(H)$ te nazivamo *normalizator podgrupe H u grupi G*. Dakle, $N_G(H) = \{a \in G : aHa^{-1} = H\}$ te je $N_G(H)$ najveća podgrupa od G koja sadrži H i u kojoj je

H normalna podgrupa. Drugim riječima, H je normalna podgrupa od $N_G(H)$ i ako je $K \leq G$ takva da je H normalna podgrupa od K, tada je $K \subseteq N_G(H)$. Također, H je normalna podgrupa grupe G ako i samo ako je $N_G(H) = G$. G-orbite u skupu $\mathcal{G}$ nazivamo *klase konjugiranosti podgrupa grupe* G.

Sylowljevi teoremi

U ovoj ćemo temi otići korak dalje u proučavanju strukturne teorije konačnih grupa. Prema Lagrangeovu teoremu, ako je H podgrupa konačne grupe G tada $|H|$ dijeli $|G|$, no ovaj rezultat ne govori mnogo o egzistenciji netrivijalnih podgrupa konačne grupe, osim u slučaju grupa prostog reda. Početni korak u tom smjeru daje iduće teorem:

Teorem (Cauchy).
Neka je G konačna grupa čiji je red djeljiv prostim brojem p. Tada G sadrži podgrupu reda p.
Dokaz:
Dovoljno je dokazati da G sadrži element reda p, jer tada taj element generira cikličku podgrupu reda p. Označimo red grupe G s n.

Neka je $S = \{(a_1, a_2, \ldots, a_p) : a_i \in G, a_1 a_2 \cdots a_p = e\}$, pri čemu je e neutralni element u G. Očito je $a_p = (a_1 a_2 \cdots a_{p-1})^{-1}$ te je a_p potpuno određen s $a_1, a_2, \ldots, a_{p-1}$. Kako svaki od ovih $p-1$ elemenata možemo odabrati na n načina, prema pravilu produkta je $|S| = n^{p-1}$.

Neka grupa $\mathbb{Z}_p$ djeluje na skupu S cikličkim permutacijama, tj. neka za $k \in \mathbb{Z}_p$ vrijedi

$$k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, \ldots, a_k).$$

Primijetimo da je

$$(a_{k+1}a_{k+2}\cdots a_p)(a_1 \cdots a_k) = (a_1 \cdots a_k)^{-1}(a_1 \cdots a_k)(a_{k+1}a_{k+2}\cdots a_p)(a_1 \cdots a_k) = e$$

te $(k+k')(a_1, a_2, \ldots, a_p) = k(k'(a_1, a_2, \ldots, a_p))$ za $k, k' \in \mathbb{Z}_p$ pa je ovo djelovanje dobro definirano.

Definiramo $S_0 = \{(a_1, a_2, \ldots, a_p) \in S : k(a_1, a_2, \ldots, a_p) = (a_1, a_2, \ldots, a_p), \forall k \in \mathbb{Z}_p\}$. Iz $1(a_1, a_2, \ldots, a_p) = (a_2, a_3, \ldots, a_p, a_1)$ slijedi da je $(a_1, a_2, \ldots, a_p) \in \mathbb{Z}_p$ ako i samo ako je $a_1 = a_2 = \ldots = a_p$. Kako je $(e, e, \ldots, e) \in S_0$, slijedi $|S_0| \geq 1$.

Prema korolaru iz potpoglavlja *Djelovanje grupa* je $|S| \equiv |S_0| \pmod p$, a kako p dijeli $|S| = n^{p-1}$ slijedi da p dijeli i $|S_0|$ te je $|S_0| \geq p \geq 2$. Dakle, postoji $a \in G$, $a \neq e$, takav da je $(a, a, \ldots, a) \in S$ te $a^p = e$.

Označimo red od a s m. Tada je $2 \leq m \leq p$ te postoje prirodni brojevi q i r, $0 \leq r < m$ takvi da je $p = q \cdot m + r$. Iz $a^p = a^m = e$ dobivamo $e = a^p = (a^m)^q \cdot a^r = a^r$ te je zbog $r < m$ nužno $r = 0$. Prema tome, m dijeli p, a kako je p prost i $m > 1$ slijedi $m = p$. Dakle, a je element reda p koji generira podgrupu reda p.

Primijetimo da u grupi G postoji barem $p - 1$ elemenata reda p.

Neka je p prost broj. Ako je G konačna grupa reda p^n za neki prirodan broj n, kažemo da je G p-**grupa**. Kažemo da je podgrupa H konačne grupe G p-**podgrupa** ako je H p-grupa.

Lema.
Konačna grupa G je p-grupa ako i samo ako je svaki $g \in G$ reda p^k za neki nenegativan cijeli broj k.
Dokaz:

Ako je G p-grupa, tada je $|G| = p^n$ za neki $n \in \mathbb{N}$. Prema Lagrangeovu teoremu, red elementa dijeli red grupe, a jedini djelitelji od p^n su oblika p^k, pri čemu je $0 \leq k \leq n$.

Obratno, neka je svaki $g \in G$ reda p^k za neki nenegativan cijeli broj k. Pretpostavimo da G nije p-grupa. Tada postoji prost broj q, $q \neq p$, koji dijeli $|G|$. Prema Cauchyjevu teoremu tada postoji element iz G reda q, što nije moguće. Dakle, G je p-grupa.

Neka je p prost broj. Kažemo da je podgrupa H konačne grupe G **Sylowljeva p-podgrupa** od G ako je H p-podgrupa i ako indeks $[G : H]$ nije djeljiv s p. Kako je, prema Lagrangeovu teoremu, $[G : H] = \frac{|G|}{|H|}$, znači da je $|H| = p^n$ i $|G| = p^n \cdot m$ pri čemu je p ne dijeli m te je Sylowljeva p-podgrupa maksimalna p-podgrupa od G.

O egzistenciji Sylowljevih p-podgrupa govori Prvi Sylowljev teorem.

Teorem (Prvi Sylowljev teorem).
Neka je G konačna grupa reda $p^n \cdot m$, p prost, $n \in \mathbb{N}$, p ne dijeli m. Tada za svaki $i = 1, 2, \ldots, n$ grupa G sadrži podgrupu reda p^i te je za $i = 1, 2, \ldots, n-1$ svaka podgrupa od G reda p^i normalna podgrupa neke podgrupe reda p^{i+1}.

Ako je $|G| = p^n \cdot m$ (p prost, $n \in \mathbb{N}$, p ne dijeli m), tada je H Sylowljeva p-podgrupa od G ako i samo ako je $|H| = p^n$. Ako su podgrupe H i K konjugirane (tj. postoji $a \in G$ takav da je $K = aHa^{-1}$), H je Sylowljeva p-podgrupa ako i samo ako je K Sylowljeva p-podgrupa, jer konjugirane podgrupe imaju jednako elemenata. Postoji i jača veza između Sylowljevih p-podgrupa:

Teorem (Drugi Sylowljev teorem).
Neka je G konačna grupa i p prost broj koji dijeli red od G. Sve Sylowljeve p-podgrupe od G su međusobno konjugirane, tj. ako su H i K Sylowljeve p-podgrupe od G tada postoji $a \in G$ takav da je $K = aHa^{-1}$.

Idući rezultat govori o broju Sylowljevih p-podgrupa.

Teorem (Treći Sylowljev teorem).
Neka je G konačna grupa reda n i p prost broj koji dijeli n. Broj Sylowljevih p-podgrupa od G dijeli n te je oblika $k \cdot p + 1$, za neki nenegativan cijeli broj k.

Primjer
Neka je $|G| = 15$. Broj Sylowljevih 3-podgrupa od G je oblika $3k + 1$ te dijeli 15, pa postoji jedinstvena Sylowljeva 3-podgrupa od G. Slično, broj Sylowljevih 5-podgrupa od G je oblika $5k + 1$ te dijeli 15, pa postoji i jedinstvena Sylowljeva 5-podgrupa od G.
Ako je $|G| = 18$, broj Sylowljevih 2-podgrupa je oblika $2k + 1$ te dijeli 18, pa G može imati 1, 3 ili 9 Sylowljevih 2-podgrupa.

Rješive i proste grupe

Neka je G grupa, te $a, b \in G$. Element $aba^{-1}b^{-1}$ nazivamo **komutator elemenata** a **i** b.

Primijetimo da je $aba^{-1}b^{-1} = e$, pri čemu je e neutralni element u G, ako i samo ako je $ab = ba$, tj. ako i samo ako a i b komutiraju.

Neka je

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

Dakle, $C(G)$ je podgrupa od G generirana svim komutatorima elemenata iz G. Podgrupu $C(G)$ nazivamo **komutatorska podgrupa grupe** G i $C(G) = \{e\}$ ako i samo ako je G Abelova grupa.

Propozicija.
Neka je G grupa. Tada je $C(G) \trianglelefteq G$ i kvocijentna grupa $G/C(G)$ je Abelova. Nadalje, ako je $H \trianglelefteq G$ takva da je kvocijentna grupa G/H Abelova, tada je $C(G) \subseteq H$.
`Dokaz:`
Neka je $S = \{aba^{-1}b^{-1} : a, b \in G\}$. Za $a, b, c \in G$ je

$$c(aba^{-1}b^{-1})c^{-1} = (cac^{-1})(cbc^{-1})(cac^{-1})^{-1}(cbc^{-1})^{-1}$$

pa je $cSc^{-1} \subseteq S$, gdje je $cSc^{-1} = \{csc^{-1} : s \in S\}$.

Neka je $s_1 \in S$. Tada je i $cs_1c^{-1} \in S$ pa je $cs_1c^{-1} = s_2$, za neki $s_2 \in S$ i $s_1 = c^{-1}s_2c$. Uvrstimo li c^{-1} umjesto c, dobivamo da je $s_1 \in cSc^{-1}$ te je i $S \subseteq cSc^{-1}$. Slijedi $S = cSc^{-1}$, za sve $c \in G$. Kako je $C(G) = \langle S \rangle$ i $cC(G)c^{-1} = \langle cSc^{-1} \rangle$, dobivamo $C(G) = cC(G)c^{-1}$ za sve $c \in G$ te $C(G) \trianglelefteq S$.

Neka su sada $aC(G)$ i $bC(G)$ iz kvocijentne grupe $G/C(G)$. Tada vrijedi

$$\begin{aligned}(aC(G))(bC(G))(aC(G))^{-1}(bC(G))^{-1} &= (aC(G))(bC(G))(a^{-1}C(G))(b^{-1}C(G)) \\ &= (aba^{-1}b^{-1})C(G) = C(G),\end{aligned}$$

jer je $aba^{-1}b^{-1} \in C(G)$. Množenjem s $(bC(G))(a(CG))$ s desna, dobivamo $(aC(G))(bC(G)) = (bC(G))(aC(G))$ pa je kvocijentna grupa $G/C(G)$ Abelova.

Neka je $H \trianglelefteq G$ takva da je G/H Abelova. Tada za $a, b \in H$ vrijedi $abH = (aH)(bH) = (bH)(aH) = baH$ te je, po definiciji H-klasa u G, $(ab)(ba)^{-1} = aba^{-1}b^{-1} \in H$ te je $S \subseteq H$ i $C(G) \subseteq H$.

Jednako kao i za grupu G, tako i za svaku podgrupu H od G možemo definirati kvocijentnu grupu $C(H)$: to je podgrupa generirana skupom $\{hkh^{-1}k^{-1} : h, k \in H\}$ svih komutatora elemenata iz H. Induktivno definiramo podgrupe $C^k(G)$, $k \in \mathbb{N} : C^1(G) = C(G)$ i $C^k(G) = C(C^{k-1}(G))$ za $k \geq 2$.

Kažemo da je grupa G **rješiva** ako postoji $n \in \mathbb{N}$ takav da je $C^n(G) = \{e\}$.

Ako je grupa G Abelova, tada je $C(G) = \{e\}$ pa je svaka Abelova grupa rješiva.

Teorem.
Grupa G je rješiva ako i samo ako postoji konačan rastući niz podgrupa $\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_{n-1} \subseteq G_n = G$ takav da je $G_i \trianglelefteq G_{i+1}$ i kvocijentna grupa G_{i+1}/G_i

je Abelova za $i = 0, 1, \ldots, n-1$.
Dokaz:
Neka je najprije G rješiva grupa i neka je $n \in \mathbb{N}$ takav da je $C^n(G) = \{e\}$. Definiramo $G_i = C^{n-i}(G)$ za $i = 0, 1, \ldots, n-1$ te $G_n = G$. Tada je $G_i = C(C^{n-i-1}(G)) = C(G_{i+1})$ za sve i te imamo rastući niz podgrupa $\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_{n-1} \subseteq G_n = G$ takav da je $G_i = C(G_{i+1}) \trianglelefteq G_{i+1}$ i kvocijentna grupa $G_{i+1}/G_i = G_{i+1}/C(G_{i+1})$ je Abelova za $i = 0, 1, \ldots, n-1$.
Pretpostavimo sada da imamo rastući niz grupa kao u iskazu teorema. Kako je kvocijentna grupa G_{i+1}/G_i Abelova, prema prethodnoj propoziciji je $C(G_{i+1}) \subseteq G_i$. Primijetimo da je $C^1(G) = C(G) = C(G_n) \subseteq G_{n-1}$. Ako je $k \geq 2$, tada iz pretpostavke da je $C^{k-1}(G) \subseteq G_{n-k+1}$ slijedi $C^k(G) = C(C^{k-1}(G)) \subseteq C(G_{n-k+1}) \subseteq G_{n-k}$. Na ovaj način induktivno dobivamo $C^n(G) \subseteq G_0 = \{e\}$ pa je grupa G rješiva.

Teorem.
Neka je G grupa, $H \leq G$ i $N \trianglelefteq G$.

1. Ako je G rješiva, tada je i H rješiva.
2. Ako je G rješiva, tada je i G/N rješiva.
3. Ako su N i G/N rješive, tada je i G rješiva.

Dokaz:
Ako je G rješiva, tada iz $C^k(H) \subseteq C^k(G)$ za sve k, slijedi da je i H rješiva.

Neka je sada G rješiva grupa i $N \trianglelefteq G$. Označimo s $\pi : G \to G/N$ *kvocijentni epimorfizam* definiran s $\pi(a) = aN$. Primijetimo da je $Ker\pi = N$. Kako za $a, b \in G$ vrijedi $\pi(aba^{-1}b^{-1}) = \pi(a)\pi(b)\pi(a)^{-1}\pi(b)^{-1}$, slijedi da je skup $\{\pi(aba^{-1}b^{-1}) : a, b \in G\}$ upravo skup svih komutatora u grupi G/N. Zato je $C(G/N) = \pi(C(G))$. Sada induktivno dobivamo $C^k(G/N) = \pi(C^k(G))$ za sve $k \in \mathbb{N}$. Zato za $n \in \mathbb{N}$ takav da je $C^n(G) = \{e\}$ vrijedi $C^n(G) = \pi(\{e\}) = \{N\}$. Kako je $N = e_{G/N}$, i kvocijentna grupa G/N je rješiva.

Neka je $N \trianglelefteq G$ takva da su N i G/N rješive. Neka su $m, n \in \mathbb{N}$ takvi da je $C^n(N) = \{e\}$ i $C^m(G/N) = \{N\}$. Slijedi da je $\pi(C^m(G)) = C^m(G/N) = \{N\}$ pa je $C^m(G) \subseteq Ker\pi = N$. Sada je $C^{m+n}(G) = C^n(C^m(G)) \subseteq C^n(N) = \{e\}$ te je i G rješiva.

Kažemo da je grupa G **prosta** ako su jedine njene normalne podgrupe $\{e\}$ i G, tj. ako nema netrivijalnih normalnih podgrupa.

Teorem.
Rješiva grupa G, $G \neq \{e\}$,je prosta ako i samo ako je ciklička i red joj je prost broj.
Dokaz:
Neka je G rješiva i prosta. Tada je $C^n(G) = \{e\}$ za neki $n \in \mathbb{N}$ pa je $C(G) \neq G$, jer bi inače imali $C^n(G) = G$ za sve $n \in \mathbb{N}$. Kako je $C(G)$ normalna podgrupa od G, slijedi da je $C(G) = \{e\}$ pa je G Abelova. No, kako je u Abelovoj grupi svaka podgrupa normalna, slijedi da za $a \in G, a \neq e$ vrijedi $\langle a \rangle = G$ te je G ciklička. Ako G nije konačna, tada je izomorfna grupi cijelih brojeva i ima beskonačno mnogo normalnih podgrupa, što nije moguće. Dakle, G je konačna i neka je $|G| = n$ te

$G = \{e, a, a^2, \ldots, a^{n-1}\}$. Ako je $n = k \cdot m$ za $k, m \geq 2$, tada je $\langle a^m \rangle$ netrivijalna podgrupa od G, što nije moguće. Prema tome, n je prost broj.
Ako je G grupa prostog reda, tada je G ciklička i prema Lagrangeovu teoremu nema netrivijalnih podgrupa pa je G prosta grupa.

Primjer.
Alternirajuća grupa A_4 je rješiva. Ako je $n \geq 5$, tada je alternirajuća grupa A_n prosta pa grupa permutacija S_n nije rješiva za $n \geq 5$ (ako bi S_n bila rješiva, tada bi i A_n bila rješiva, što nije moguće prema prethodnom teoremu jer je A_n prosta grupa čiji red je jednak $\frac{n!}{2}$, što nije prost broj).

Ovaj primjer ima posebnu povijesnu važnost jer je pomoću tog rezultata pokazano da ne postoji formula za određivanje rješenja polinomijalne jednadžbe stupnja većeg ili jednakog 5 (Abel-Ruffinijev teorem).

KOMUTATIVNI PRSTENI
Prsteni i moduli

Definicija.
Prsten je neprazan skup R na kome su zadane dvije binarne operacije, zbrajanje ($(a,b) \in R \times R \mapsto a+b$) i množenje ($(a,b) \in R \times R \mapsto ab$) sa sljedećim svojstvima:

1. u odnosu na zbrajanje je R Abelova grupa; neutralni element u odnosu na zbrajanje označavamo s 0 i nazivamo nula (ili nula prstena R);
2. u odnosu na množenje je R polugrupa (tj. množenje je asocijativno);
3. množenje je slijeva i zdesna distributivno u odnosu na zbrajanje, tj. za sve $a, b, c \in R$ vrijedi $a(b+c) = ab + ac$ i $(a+b)c = ac + bc$.

Kažemo da je prsten komutativan ako je množenje u tom prstenu komutativno.

Primijetimo da za svaki $a \in R$ vrijedi $0 \cdot a = 0$ (slijedi direktno iz $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$ - ovdje koristimo upravo svojstvo distributivnosti). Distributivnost prilikom množenja omogućuje raspisivanje produkta u obliku "svaki sa svakim".

Kažemo da je R *prsten s jedinicom*, ili unitalni prsten, ako je R u odnosu na množenje monoid, tj. postoji element $1 \in R$ takav da je $a \cdot 1 = 1 \cdot a = a$, $\forall a \in R$. Takav je element nužno jedinstven i nazivamo ga *jedinica* prstena R.

U prstenu R je $0 = 1$ ako i samo ako je $R = \{0\}$, tada kažemo da je R trivijalni prsten.

Potprsten prstena R je podskup S od R koji je i sam prsten u odnosu na zadane binarne operacije. Sada možemo generalizirati i kriterij iz slučaja podgrupa: $S \subseteq R$ je potprsten ako i samo ako je $S \neq \emptyset$ te za sve $a, b \in S$ vrijedi $a - b \in S$ i $ab \in S$. Primijetimo da dio $a - b \in S$ ustvari znači da je S (aditivna) podgrupa od R, dok uvjet $ab \in S$ znači da množenje na R inducira binarnu operaciju i na S (asocijativnost i distributivnost su naslijeđene s R).

Ako je R prsten s jedinicom 1 i S potprsten od R, kažemo da je S potprsten s jedinicom ako je $1 \in S$.

Kažemo da je element a prstena s jedinicom R *invertibilan* ako postoji $b \in R$ takav da je $a \cdot b = b \cdot a = 1$. Takav element b obično označavamo s a^{-1}. Skup invertibilnih elemenata prstena s jedinicom R označavamo s $R^\times$.

Primjeri.
$\mathbb{Z}$ je komutativan prsten s jedinicom 1 (prsten cijelih brojeva). Jedini invertibilnih elementi su 1 i -1. Prsten $\{0\}$ je trivijalni potprsten od $\mathbb{Z}$. Za $n \in \mathbb{N}$ je $n\mathbb{Z}$ potprsten od $\mathbb{Z}$. Također, $n\mathbb{Z}$ je potprsten s jedinicom jedino ako je $n = 1$. Na ovaj način smo nabrojali sve potprstene od $\mathbb{Z}$, jer smo naveli sve podgrupe.

Neka je $n \in \mathbb{N}$, $n \geq 2$. Na skupu $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ definiramo množenje modulo n s: $a \cdot_n b =$ ostatak pri dijeljenju broja $a \cdot b$ s n, za $a, b \in \mathbb{Z}_n$. Sada je $\mathbb{Z}_n$ komutativan prsten s jedinicom, u odnosu na zbrajanje modulo n i množenje modulo n. Na primjer, u $\mathbb{Z}_4$ vrijedi $2 \cdot_4 2 = 0$, dok u $\mathbb{Z}_6$ vrijedi $2 \cdot_6 3 = 0$. Invertibilni elementi u $\mathbb{Z}_4$ su 1 i 3, a u $\mathbb{Z}_6$ su invertibilni elementi 1 i 5.

Neka je R prsten. Polinom P oblika $P = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, gdje su $a_0, a_1, \ldots, a_n \in R$, možemo identificirati s nizom $(a_0, a_1, a_2, \ldots, a_{n-1}, a_n, 0, 0, \ldots)$ njegovih koeficijenata. Sada ćemo uvesti pojam *prstena polinoma* u jednoj varijabli s koeficijentima iz prstena R. Označimo s $R[x]$ skup svih nizova $(a_0, a_1, \ldots)$ elemenata iz R takvih da je $a_i = 0$ za sve osim konačno mnogo indekasa i. Drugim riječima, od nekog mjesta nadalje svih elementi u nizu moraju biti jednaki 0 (nakon što indeks premaši stupanj polinoma). Skup $R[x]$ je prsten uz zbrajanje i množenje definirano s

$$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots),$$

$$(a_0, a_1, a_2, \ldots) \cdot (b_0, b_1, b_2, \ldots) = (c_0, c_1, c_2, \ldots),$$

gdje je

$$c_n = a_0b_n + a_1b_{n-1} + \cdots + a_{n-1}b_1 + a_nb_0 = \sum_{i=0}^{n} a_ib_{n-i}.$$

Nula u prstenu $R[x]$ je nul-polinom $0 = (0, 0, \ldots)$. Ako je R prsten s jedinicom 1, tada je i $R[x]$ prsten s jedinicom $(1, 0, 0, \ldots)$. Ako je R komutativan prsten, tada je i $R[x]$ komutativan prsten.

Prsten polinoma u više varijabli se definira induktivno, npr. prsten polinoma u dvije varijable $R[x_1, x_2] = (R[x_1])[x_2]$, jer polinom u varijablama x_1 i x_2 možemo promatrati kao polinom u varijabli x_2 čiji su koeficijenti polinomi u varijabli x_1.

Neka je R prsten. Označimo s $R[[x]]$ skup svih nizova $(a_0, a_1, \ldots)$ elemenata iz R. Tada je $R[[x]]$ prsten u odnosu na jednake operacije kao i $R[x]$. Prsten $R[[x]]$ nazivamo *prsten formalnih redova* i $R[x]$ je potprsten od $R[[x]]$. Na primjer, funkcije izvodnice su formalni redovi.

Definicija.
Neka su R i S prsteni. Kažemo da je preslikavanje $\varphi : R \to S$ homomorfizam prstena ako za sve $a, b \in R$ vrijedi $\varphi(a + b) = \varphi(a) + \varphi(b)$ i $\varphi(ab) = \varphi(a)\varphi(b)$.

Iz svojstava homomorfizama grupa slijedi $\varphi(0) = 0$ i $\varphi(-a) = -\varphi(a)$, za $a \in R$. Ako su R i S prsteni s jedinicama 1_R i 1_S, kažemo da je homomorfizam $\varphi : R \to S$ unitalan ako vrijedi $\varphi(1_R) = 1_S$.

Injektivni homomorfizam prstena nazivamo monomorfizam prstena, surjektivni homomorfizam prstena nazivamo epimorfizam prstena, a bijektivni homomorfizam prstena nazivamo izomorfizam prstena. Kažemo da su prsteni R i S izomorfni, te pišemo $R \cong S$, ako postoji izomorfizam $\varphi : R \to S$.

Ako je $\varphi : R \to S$ homormofizam prstena, tada je slika od φ, $Im\varphi = \{\varphi(a) : a \in R\}$, potprsten od S. Jezgra od φ, $Ker\varphi = \{a \in R : \varphi(a) = 0\}$, je potprsten od R.

Uočimo da za sve $a \in Ker\varphi$ i $b \in R$ vrijedi $\varphi(ab) = \varphi(a)\varphi(b) = 0\varphi(b) = 0$ i $\varphi(ba) = \varphi(b)\varphi(a) = \varphi(b)0 = 0$, pa su $ab, ba \in Ker\varphi$. Zato je jezgra homomorfizma primjer *ideala*.

Definicija.
Kažemo da je aditivna podgrupa I prstena R lijevi ideal u prstenu R ako za $a \in I$ i $b \in R$ vrijedi $ba \in I$. Kažemo da je aditivna podgrupa I prstena R desni ideal

u prstenu R ako za $a \in I$ i $b \in R$ vrijedi $ab \in I$. Ako je I i lijevi i desni ideal u prstenu R, kažemo da je I obostrani ideal u R ili samo ideal u R. Nadalje ćemo za obostrani ideal govoriti samo ideal. Primijetimo da je u komutativnom prstenu svaki lijevi ideal ujedno i desni ideal, i obratno.

Neka je R prsten te I ideal u R. Tada je I normalna podgrupa aditivne grupe prstena R, jer je u Abelovoj grupi svaka podgrupa normalna. Zato možemo formirati kvocijentnu grupu R/I, čiji elementi su skupovi oblika $a + I = a + b : b \in I$ i zbrajanje je dano s $(a + I) + (b + I) = a + b + I$, $a, b \in R$.

Možemo definirati i množenje na R/I s $(a + I)(b + I) = ab + I$, za $a, b \in R$. Pokažimo da je ova operacija dobro definirana, tj. da ne ovisi o odabiru predstavnika.

Neka su $a', b' \in R$ takvi da je $a + I = a' + I$ te $b + I = b' + I$. Tada je $a-a', b-b' \in I$. Sada je $ab-a'b' = ab-ab'+ab'-a'b' = a(b-b')+(a-a')b' \in I$, jer je I ideal pa su $a(b-b'), (a-a')b' \in I$ te i njihova suma. zato je $ab+I = a'b'+I$.

Može se direktno provjeriti (iz definicije i svojstava prstena R) da je ovako definirano množenje asocijativno i distributivno u odnosu na zbrajanje. Prema tome, R/I je prsten koji nazivamo *kvocijentni prsten* prstena R po idealu I.

Ukoliko je R prsten s jedinicom 1, tada je i R/I prsten s jedinicom $1 + I$.

Na isti način kao i u slučaju grupa se pokazuje idući teorem:

Teorem (Prvi teorem o izomorfizmu za prstene).
Neka je $\varphi : R \to S$ homomorfizam prstena. Neka je $I = Ker\varphi$. Preslikavanje $\Phi : R/I \to Im\varphi$, definirano s $\Phi(a+I) = \varphi(a)$, je izomorfizam kvocijentnog prstena R/I na prsten $Im\varphi$. Ako je homomorfizam φ unitala, tada je $Im\varphi$ potprsten s jedinicom prstena S i izomorfizam Φ je unitalan.

Definicija.
Kažemo da je komutativan prsten R s jedinicom *polje* ako je $R^\times = R \setminus \{0\}$.

Prema tome, u polju je svaki nenul element invertibilan. Najpoznatiji primjeri polja su polje racionalnih brojeva $\mathbb{Q}$, polje realnih brojeva $\mathbb{R}$ i polje kompleksnih brojeva $\mathbb{C}$.

Na primjer, prsten cijelih brojeva $\mathbb{Z}$ nije polje. Ako je p prost broj, tada je i $\mathbb{Z}_p$ polje. Zaista, ako je $a \in \mathbb{Z}_p$, $a \neq 0$, tada su a i p relativno prosti pa postoje $x, y \in \mathbb{Z}$ takvi da je $ax + py = 1$, odnosno $ax \equiv 1 \pmod p$. Uzmemo li umjesto x ostatak koji x daje pri dijeljenju s p, dobivamo inverz od a pa je svaki nenul element u $\mathbb{Z}_p$ invertibilan.

Definicija.
Neka je R prsten. *Lijevi R-modul* je aditivna Abelova grupa V na kojoj je definirana operacija množenja elemenata iz V elementima iz R, $R \times V \to V$, $(a, v) \mapsto av$, sa sljedećim svojstvima:

1. distributivnost u odnosu na zbrajanje u R: $(a+b)v = av+bv$, $\forall a, b \in R, v \in V$;
2. distributivnost u odnosu na zbrajanje u V: $a(u+v) = au+av$, $\forall a \in R, u, v \in V$;
3. kvaziasocijativnost: $(ab)v = a(bv)$, $\forall a, b \in R, v \in V$.

Na analogan način se definira i desni R-modul (tada imamo preslikavanje $R \times V \to V$, $(a, v) \mapsto va$). Ako je R prsten s jedinicom, kažemo da je lijevi R-modul *unitalan* ako $\forall v \in V$ vrijedi $1 \cdot v = v$.

Ako su V i W lijevi R-moduli, kažemo da je preslikavanje $\varphi : V \to W$ homomorfizam R-modula ako $\forall a \in R, u, v \in V$ vrijedi $\varphi(u + v) = \varphi(u) + \varphi(v)$ i $\varphi(av) = a\varphi(v)$.

Ako je R polje, tada unitalni lijevi R-modul nazivamo *vektorski prostor*.

Integralne domene i polja kvocijenata

Definicija.
Neka je R komutativan prsten s jedinicom 1, $1 \neq 0$. Kažemo da je element $a \in R$, $a \neq 0$, *djelitelj nule* ako postoji $b \in R$, $b \neq 0$, takav da je $a \cdot b = 0$.

Na primjer, 2 i 3 su djelitelji nule u prstenu $\mathbb{Z}_6$, jer je $2 \cdot_6 3 = 0$.

Definicija.
Integralna domena je komutativan prsten s jedinicom 1, $1 \neq 0$, u kome nema djelitelja nule.

Pokazali smo da $\mathbb{Z}_6$ nije integralna domena. Također, niti $\mathbb{Z}_4$ nije integralna domena, niti $\mathbb{Z}_n$ za složen broj n, jer tada n možemo zapisati u obliku $n = k \cdot l$, pri čemu je $1 < k, l < n$ te vrijedi $k \cdot_n l = 0$ te su k i l djelitelji nule u $\mathbb{Z}_n$. S druge strane, prsten cijelih brojeva $\mathbb{Z}$ je integralna domena, jer ako za dva cijela broja a i b vrijedi $a \cdot b = 0$ tada je $a = 0$ ili $b = 0$.

Primijetimo da u integralnoj domeni vrijedi $a \cdot b = 0$ ako i samo ako $a = 0$ ili $b = 0$. Općenito, u prstenu koji nije integralna domena ne možemo zaključiti da iz $a \cdot b = 0$ slijedi $a = 0$ ili $b = 0$.

Također, općenito u prstenu ne možemo skraćivati, tj. zaključiti da iz $a \cdot b = a \cdot c$, pri čemu je $a \neq 0$, slijedi $b = c$. Na primjer, u prstenu $\mathbb{Z}_6$ vrijedi $3 \cdot_6 2 = 3 \cdot_6 4$.

Ali, ako je R integralna domena te $a, b, c \in R$, $a \neq 0$, takvi da je $a \cdot b = a \cdot c$, tada je $a \cdot b - a \cdot c = 0$ te $a(b-c) = 0$, odakle slijedi da je ili $a = 0$, što nije moguće, ili $b - c = 0$. Dakle, slijedi da je $b - c = 0$ odnosno $b = c$ pa u integralnoj domeni možemo skraćivati.

Nadalje, ako je R integralna domena, tada je i prsten polinoma $R[x]$ također integralna domena te za $P, Q \in R[x]$, $P \neq 0, Q \neq 0$, vrijedi da je stupanj polinoma $P \cdot Q$ jednak sumi stupnjeva polinoma P i Q. Primijetimo da ta jednakost ne vrijedi općenito. Na primjer, za polinome $P = 2x^3 + x$ i $Q = 3x^2$ u $\mathbb{Z}_6[x]$ vrijedi $P \cdot Q = 3x^3$.

Svako polje je integralna domena. Ako u polju R vrijedi $a \cdot b = 0$ za neki $a \in R$, $a \neq 0$, tada množenjem s a^{-1} (u polju je svaki nenul element invertibilan) dobivamo $b = 0$ pa ne postoje djelitelji nule.

Potprsten s jedinicom integralne domene je opet integralna domena pa je i svaki potprsten s jedinicom nekog polja također integralna domena (ako djelitelja nule nema u većem skupu, neće ih biti niti u manjem, kao u slučaju $\mathbb{Z} \subset \mathbb{Q}$).

Pokazat ćemo da vrijedi i jedna varijanta obrat, krenut ćemo od integralne domene te pomoću njenih elemenata konstruirati polje, slično kao da iz cijelih brojeva konstruiramo racionalne.

Neka je R integralna domena. Definiramo

$$\widetilde{K} = R \times (R \setminus \{0\}) = \{(a, b) : a, b \in R, b \neq 0\}.$$

Na ovom skupu uvedimo relaciju $\sim$ na sljedeći način: za $(a, b), (c, d) \in \widetilde{K}$ je

$$(a, b) \sim (c, d) \Leftrightarrow a \cdot d = b \cdot c.$$

Ova relacija je relacija ekvivalencije na skupu $\widetilde{K}$ (radi se o imitacije klasične jednakosti razlomaka). Označimo s K skup svih klasa ekvivalencije u skupu $\widetilde{K}$ u odnosu na uvedenu relaciju. Klasu ekvivalencije elementa $(a,b) \in \widetilde{K}$ ćemo označavati s $\frac{a}{b}$. Prema tome,

$$K = \left\{ \frac{a}{b} : a, b \in R, b \neq 0 \right\},$$

pri čemu je

$$\frac{a}{b} = \{(c,d) : c, d, \in R, d \neq 0, a \cdot d = b \cdot c\}.$$

Na skupu K definiramo binarne operacije zbrajanja i množenja: za $\frac{a}{b}, \frac{c}{d} \in K$ stavimo

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd},$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Primijetimo da je za definiciju ovih binarnih operacija ključno da je R integralna domena, jer iz $b \neq 0$ i $d \neq 0$ slijedi $bd \neq 0$.

Ove operacije su dobro definirane, tj. ne ovise o odabiru predstavnika, te obzirom na njih K postaje komutativan prsten (komutativnost slijedi iz $\frac{ac}{bd} = \frac{ca}{db}$, jer je R komutativan).

Ulogu nule u prstenu K ima klasa

$$\frac{0}{1} = \{(0,c) : c \in R, c \neq 0\},$$

jer je $\frac{a}{b} + \frac{0}{1} = \frac{a \cdot 1 + b \cdot 0}{b \cdot 1} = \frac{a}{b}$ te $(0,1) \sim (0,c)$ zbog $0 \cdot c = 1 \cdot 0$.

Ulogu jedinice u prstenu K ima klasa

$$\frac{1}{1} = \{(c,c) : c \in R, c \neq 0\},$$

jer je $\frac{a}{b} \cdot \frac{1}{1} = \frac{a \cdot 1}{b \cdot 1} = \frac{a}{b}$ te $(1,1) \sim (c,c)$ zbog $1 \cdot c = 1 \cdot c$.

Neka je $\frac{a}{b}$ nenul element iz K. Tada je $b \neq 0$, dok iz $\frac{a}{b} \neq \frac{0}{1}$ slijedi $a \cdot 1 \neq b \cdot 0$ odnosno $a \neq 0$. Tada je i $\frac{b}{a} \in K$ te vrijedi

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1}$$

jer je $ab = ba \neq 0$. Prema tome, element $\frac{a}{b}$ je invertibilan te vrijedi $K^\times = K \setminus \{\frac{0}{1}\}$ i K je polje.

Ovako definirano polje K nazivamo *polje kvocijenata* ili *polje razlomaka integralne domene* R.

Preslikavanje $\varphi : R \to K$ definirano s $\varphi(a) = \frac{a}{1}$, $a \in R$, je unitalni monomorfizam prstenova te element $a \in R$ možemo na ovaj način identificirati s klasom $a = \frac{a}{1} \in K$. Kažemo da se integralna domena R *ulaže* u svoje polje kvocijenata K, u oznaci $R \hookrightarrow K$.

Ako je R integralna domena, tada je prsten polinoma $R[x]$ integralna domena, čije polje kvocijenata označavamo s $R(x)$ i nazivamo *polje racionalnih funkcija* u jednoj varijabli s koeficijentima iz R.

Teorem.
Neka je R integralna domena i K njeno polje kvocijenata. Neka je ψ unitalni monomorfizam prstena R u neko polje L. Tada postoji jedinstveni unitalni monomorfizam prstena $\Psi : K \to L$ koji proširuje ψ, tj. takav da je $\Psi|_R = \psi$, koji je dan s $\Psi(\frac{a}{b}) = \psi(a)\psi(b)^{-1}$, $\frac{a}{b} \in K$. Preslikavanje Ψ je također injektivno.

Prosti i maksimalni ideali

U ovom će potpoglavlju čitavo vrijeme R označavati komutativan prsten s jedinicom 1, $1 \neq 0$.

Počnimo s nekoliko definicija.

Definicija.
Kažemo da je ideal I u prstenu R **prost** ako je $I \neq R$ te iz $a \cdot b \in I$ slijedi $a \in I$ ili $b \in I$.

Neka je $a \in R$. S (a) označavamo ideal u R generiran elementom a, tj. najmanji ideal u R koji sadrži a. Drugim riječima, (a) je ideal, $a \in (a)$, te ako je I ideal u R za koji vrijedi $a \in I$, tada je i $(a) \subseteq I$.

Ideal generiran jednim elementom nazivamo **glavni ideal**, tj. ideal I u prstenu R je glavni ideal ako postoji $a \in R$ takav da je $I = (a)$.

Primijetimo da je

$$(a) = \{ar : r \in R\} = aR.$$

S jedne strane, kako je $a \in (a)$ i (a) je ideal, iz definicije ideala slijedi da je i $ar \in (a)$ za svaki $r \in R$ pa je $\{ar : r \in R\} \subseteq (a)$. S druge strane, kako je $a = a \cdot 1$ slijedi da je $a \in \{ar : r \in R\}$. Također, skup $\{ar : r \in R\}$ je ideal u R: za $r_1, r_2 \in R$ je $ar_1 - ar_2 = a(r_1 - r_2) \in \{ar : r \in R\}$ te je $r_1(ar_2) = a(r_1 \cdot r_2) \in \{ar : r \in R\}$. Prema tome, $(a) \subseteq \{ar : r \in R\}$ pa slijedi $(a) = \{ar : r \in R\}$.

Primjer.
Nul-ideal, $\{0\} = (0)$, je prost ideal u svakoj integralnoj domeni, jer iz $ab \in (0)$ slijedi $ab = 0$, odakle je $a = 0$ ili $b = 0$, odnosno $a \in (0)$ ili $b \in (0)$.

Primjer.
Ako je $p \in \mathbb{Z}$, p prost broj, tada je glavni ideal (p) prost ideal u $\mathbb{Z}$ jer iz $ab \in (p)$ slijedi da je $ab = pk$, za neki cijeli broj k, te kako je p prost broj dobivamo da p dijeli a ili p dijeli b, odnosno $a \in (p)$ ili $b \in (p)$. S druge strane, ideal (6) nije prost jer je $2 \cdot 3 = 6$, ali $2 \notin (6)$ i $3 \notin (6)$.

Primijetimo da za ideal I vrijedi $I = R$ ako i samo ako je $1 \in I$. Očito $I = R$ povlači $1 \in I$. Obratno, ako je $1 \in I$ tada za svaki $r \in R$ vrijedi $r = r \cdot 1 \in I$ pa je $R \subseteq I$ te $I = R$.

Propozicija.
Ideal I u prstenu R je prost ako i samo ako je kvocijentni prsten R/I integralna domena.

Dokaz:
Pokažimo najprije da ako je ideal I prost tada R/I mora biti integralna domena. Pretpostavimo suprotno, tj. neka je I prost, ali R/I nije integralna domena. Tada u R/I postoje djelitelji nule, dakle postoje $a+I, b+I \in R/I$, $a+I \neq I$, $b+I \neq I$ takvi da je $(a+I)(b+I) = I$, jer je I nula u kvocijentnom prstenu R/I. Kako je $a + I \neq I$, slijedi $a \notin I$. Na isti način dobivamo i $b \notin I$. Iz $(a+I)(b+I) = I$ je $ab + I = I$, odakle je $ab \in I$ pa ideal I nije prost, što je u suprotnosti s pretpostavkom. Dakle, R/I je integralna domena.
Pokažimo sada da ako je R/I integralna domena tada I mora biti prost ideal. Pretpostavimo suprotno, neka ideal I nije prost. Tada postoje $a, b \in R$, $a \notin I$,

$b \notin I$, takvi da je $ab \in I$. Slijedi $a+I \neq I$, $b+I \neq I$ te $(a+I)(b+I) = ab+I = I$ pa su $a+I$, $b+I$ djelitelji nule u R/I, što nije moguće jer je R/I integralna domena. Dakle, ideal I je prost.

Definicija.
Kažemo da je ideal I u prstenu R **maksimalan** ako je $I \neq R$ te ne postoji ideal J u prstenu R takav da je $I \subsetneq J \subsetneq R$.

Primjer.
Ideal (4) nije maksimalan ideal u prstenu $\mathbb{Z}$ jer je $(4) \subsetneq (2) \subsetneq \mathbb{Z}$.
Ako je p prost broj, tada je glavni ideal (p) maksimalan ideal u $\mathbb{Z}$. Kako bi to pokazali, neka je J ideal u $\mathbb{Z}$ takav da je $(p) \subsetneq J$. Treba pokazati da je tada $J = \mathbb{Z}$. Kako je $(p) \subsetneq J$, postoji $r \in J \setminus (p)$. Prema tome, p ne dijeli r pa su p i r relativno prosti. Zato postoje cijeli brojevi x, y takvi da je $px+ry = 1$. Iz $p \in (p) \subset J$ slijedi da je i $px \in J$, dok iz $r \in J$ slijedi $ry \in J$, jer je J ideal. Prema tome, $px+ry \in J$, dakle $1 \in J$ pa je $J = \mathbb{Z}$. Dakle, ideal (p) je maksimalan.

Propozicija.
U prstenu R postoji barem jedan maksimalan ideal. Štoviše, za svaki ideal I u prstenu R, $I \neq R$, postoji maksimalan ideal u R koji sadrži I.
Napomenimo kako formalan dokaz ove tvrdnje koristi neke elemente teorije skupova. Ugrubo, ako je I ideal u R, $I \neq R$, tada je unija svih ideala u R koji sadrži ideal I maksimalan ideal u R koji sadrži ideal I.

Ako su I, J ideali u R, tada je suma ideala $I + J = \{a + b : a \in I, b \in J\}$ ideal u R. Zaista, za $x_1, x_2 \in I + J$ te $r \in R$ postoje $a_1, a_2 \in I$, $b_1, b_2 \in J$ takvi da je $x_1 = a_1 + b_1$ i $x_2 = a_2 + b_2$, odakle je $x_1 - x_2 = (a_1 - a_2) + (b_1 - b_2) \in I + J$ te $rx_1 = ra_1 + rb_1 \in I + J$. Primijetimo da za svaki ideal I vrijedi $I + I \subseteq I$.

Slično, ako su I, J ideali u R, tada je produkt ideala $I \cdot J = \{a \cdot b : a \in I, b \in J\}$ ideal u R. Zaista, za $x_1, x_2 \in I \cdot J$ te $r \in R$ postoje $a_1, a_2 \in I$, $b_1, b_2 \in J$ takvi da je $x_1 = a_1 \cdot b_1$ i $x_2 = a_2 \cdot b_2$, odakle je $x_1 - x_2 = a_1 \cdot b_1 - a_2 \cdot b_2 = a_1 \cdot b_1 - a_1 \cdot b_2 + a_1 \cdot b_2 - a_2 \cdot b_2 = a_1(b_1 - b_2) + (a_1 - a_2)b_2 \in I \cdot J$ te $x_1 \cdot x_2 = (a_1 b_1)(a_2 b_2) = (a_1 a_2)(b_1 b_2) \in I \cdot J$. Primijetimo da je $I \cdot J \subseteq I$, $I \cdot J \subseteq J$.

Teorem.
Svaki maksimalan ideal I u prstenu R je prost.
Dokaz:
Pretpostavimo suprotno, neka je I maksimalan ideal koji nije prost. Dakle, postoje $a, b \in R$, $a \notin I$, $b \notin I$ takvi da je $ab \in I$. Tada su $I+(a), I+(b)$ također ideal u R. Za $x \in I$ vrijedi $x = x+0 \in I+(a)$ pa je $I \subseteq (a)$. No, kako je $a = 0+a \in I+(a)$, slijedi da je $a \in I + (a)$, no zbog $a \notin I$ slijedi $I \subsetneq I + (a)$. Kako je I maksimalan ideal, dobivamo $I + (a) = R$. Na isti način slijedi i $I + (b) = R$.
Zbog komutativnosti od R i $ab \in I$ dobivamo

$$(a)(b) = \{(ar_1)(br_2) : r_1, r_2 \in R\} = \{(ab)r_1 r_2 : r_1, r_2 \in R\} \subseteq \{(ab)r : r \in R\} = (ab) \subseteq I.$$

Kako je $1 \in R$, dobivamo $R \cdot R = R$, jer za svaki $r \in R$ vrijedi $r = r \cdot 1 \subset \{r_1 r_2 : r_1, r_2 \in R\} = R \cdot R$. Sada je

$$R = R \cdot R = (I+(a))(I+(b)) \subseteq I \cdot I + (a) \cdot I + I \cdot (b) + (a) \cdot (b) \subseteq I + I + I + I \subseteq I,$$

odakle je $I = R$, što nije moguće, pa je maksimalan ideal I prost.

Obrat prehodnog teorema na vrijedi. Na primjer, $(0) \subset \mathbb{Z}$ je prost ideal koji nije maksimalan.

Primjer.
Neka je u prstenu $R = \mathbb{Z}[x]$ dano $I = \{P \in \mathbb{Z}[x] : P(0) = 0\}$ i $J = \{P \in \mathbb{Z}[x] : 2|P(0)\}$. Tada su I, J ideali u R. Primijetimo da se u I nalaze svi polinomi (u jednoj varijabli, s cjelobrojnim koeficijentima) čiji je slobodni član jednak nuli, dok se u J nalaze polinomi čiji je slobodni koeficijent paran. Lako se može vidjeti da je razlika dva polinoma iz I opet polinom iz I te da množenjem polinoma iz I nekim drugim polinomom iz R opet dobivamo polinom iz I. Slično vrijedi i za J. Očito je I pravi podskup od J. Ideal I je prost: ako je slobodni koeficijent produkta dva polinoma jednak nuli, tada je i slobodni koeficijent nekog od tih faktora jednak nuli. Prema tome, I je nenul prost ideal koji nije maksimalan.

Propozicija.
Ideal I u prstenu R je maksimalan ako i samo ako je kvocijentni prsten R/I polje.
`Dokaz:`
Neka je najprije I maksimalan ideal. Vidjeli smo da je tada ideal I i prost te da je R/I integralna domena. Preostaje pokazati da je svaki nenul element u R/I invertibilan. Neka je $a + I \neq I$ nenul element u R/I. Tada je $a \in R \setminus I$. Kao u dokazu prethodnog teorema slijedi $(a) + I = R$ pa postoje $r \in R$ i $x \in I$ takvi da je $ar + x = 1$, jer se svaki element iz R može prikazati u obliku sume elementa iz (a) i elementa iz I, a svaki element iz (a) je oblika ra. Kako je $x \in I$, slijedi $ar + x + I = ar + I$ (jer je $ar + x - ar = x \in I$). Dakle, $(a + I)(r + I) = ar + I = ar + x + I = 1 + I$ pa je element $a + I$ invertibilan, s inverzom $r + I$.
Obratno, neka je R/I polje i neka je J ideal u R takav da je $I \subsetneq J$. Treba pokazati da je $J = R$, odnosno $1 \in J$. Znamo da je $J \setminus I \neq \emptyset$ te neka je $a \in J \setminus I$. Tada je $a + I \neq I$ pa je $a + I$ nenul element u R/I. Kako je po pretpostavci R/I polje, postoji $b + I$ takav da je $(a + I)(b + I) = 1 + I$. odnosno $ab + I = 1 + I$. Slijedi $ab - 1 \in I$. Kako je $I \subset J$ te $a \in J$, slijedi $ab - 1 \in J$, $ab \in J$ pa je i $1 \in J$ te $J = R$ i ideal I je maksimalan.

Pomoću ideala dobivamo iduću karakterizaciju polja:

Propozicija.
Prsten 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 ideal u R, $I \neq \{0\}$. Tada postoji $a \in I$, $a \neq 0$. Kako je R polje, postoji $a^{-1} \in R$ pa je $a \cdot a^{-1} = 1 \in I$ te je $I = R$.
Obratno, neka su $\{0\}$ i R jedini ideali u R. Tada za $a \in R$, $a \neq 0$, vrijedi $(a) = R$ jer je (a) ne-nul ideal. Prema tome, $1 \in (a)$ te postoji $r \in R$ takav da je $1 = a \cdot r$ pa je a invertibilan i R je polje.

Primijetimo da je prsten (komutativan, s jedinicom 1, $1 \neq 0$) polje ako i samo ako je nul-ideal maksimalan ideal u R.

Sada ćemo uvesti jednu klasu prstenova u kojima postoji specifičan odnos između prostih i maksimalnih ideala.

Definicija.
Kažemo da je prsten R **prsten glavnih ideala** ako je svaki ideal u R glavni. **Domena glavnih ideala** je integralna domena koja je prsten glavnih ideala.

Propozicija.
Neka je R domena glavnih ideala. Tada je svaki nenul prost ideal u R maksimalan.
`Dokaz:`
Neka je $I \neq (0)$ prost ideal u R. Tada postoji $a \in R$, $a \neq 0$, takav da je $I = (a)$. Neka je J ideal u R koji sadrži I. Postoji i $b \in R$ takav da je $J = (b)$. Zbog $I \subseteq J$ je $a \in J = (b)$ pa postoji $r \in R$ takav da je $a = br$. Kako je ideal I prost, slijedi da je $b \in I$ ili $r \in I$. Ako je $b \in I$, tada je $J = (b) \subseteq I$ pa je $I = J$. Ako je $r \in I = (a)$, tada je $r = as$ za neki $s \in R$. Uvrštavanjem u $a = br$ dobivamo $a = bsa$ pa je $bs = 1$, jer je R integralna domena. No, kako je $b \in J$ slijedi $1 = bs \in J$ pa je $J = R$. Prema tome, jedini ideali koji sadrže ideal I, $I \neq R$, su R i I pa je ideal I maksimalan.

Vidjeli smo da u prstenu $\mathbb{Z}[x]$ postoji nenul prost ideal koji nije maksimalan pa prsten $\mathbb{Z}[x]$ nije domena glavnih ideala. Česti su i primjeri prstena koji jesu domene glavnih ideala.

Propozicija.
Prsteni $\mathbb{Z}$ i $K[x]$, gdje je K polje, su domene glavnih ideala.
`Dokaz:`
Kako je svaka podgrupa od $\mathbb{Z}$ oblika $m\mathbb{Z}$, i svaki ideal u prstenu $\mathbb{Z}$ je oblika (m), odnosno glavni ideal pa je $\mathbb{Z}$ domena glavnih ideala.
Neka je K polje i I ideal u $K[x]$. Pretpostavimo da je $I \neq (0)$ te neka je $P \in I$, $P \neq 0$, takav da za $Q \in I$, $Q \neq 0$, vrijedi da je stupanj od P manji ili jednak stupnju od Q (tj. P je nenul element iz I minimalnog stupnja). Zbog $P \in I$ odmah slijedi $(P) \subseteq I$. Neka je sada $Q \in I$. Tada postoje $A, B \in K[x]$ takvi da je $Q = A \cdot P + B$, pri čemu je stupanj od B strogo manji od stupnja od P.
(Ovaj rezultat nazivamo *Teorem o dijeljenju s ostatkom za polinome* i ključno je da je K polje, tj. da su koeficijenti polinoma iz polja. Primjerice, za $P = 2x^2$ i $Q = x^3$ u $\mathbb{Q}[x]$ vrijedi $x^3 = (\frac{1}{2}x) \cdot (2x^2) + 0$, dok bi za iste polinome u $\mathbb{Z}[x]$ imali $x^3 = 0 \cdot (2x^2) + x^3$ te prilikom dijeljenja polinoma nad prstenom stupanj ostatka ne mora biti manji od stupnja djelitelja.)
Kako je $Q \in I$ i $P \in I$, slijedi $B = Q - AP \in I$ pa je, zbog definicije od P, $B = 0$. Prema tome, $Q = AP$, odnosno $Q \in (P)$ i $I \subseteq P$. Sada je $I = (P)$ pa je I glavni ideal te je $K[x]$ domena glavnih ideala.

Faktorijalni prsteni

Definicija.
Neka je R komutativan prsten te $a, b \in R$, $a \neq 0$. Kažemo da a **dijeli** b te pišemo $a|b$ ako postoji $x \in R$ takav da je $b = ax$. Kažemo da su elementi $a, b \in R$ **asocirani** ako a dijeli b i b dijeli a.

Propozicija.
Neka je R komutativan prsten s jedinicom 1, $1 \neq 0$. Neka su $a, b \in R$. Tada vrijedi:

1. a dijeli b ako i samo ako je $(b) \subseteq (a)$.
2. a i b su asocirani ako i samo ako je $(a) = (b)$.
3. u je invertibilan ako i samo ako u dijeli r, za svaki $r \in R$.
4. u je invertibilan ako i samo ako je $(u) = R$.

`Dokaz:`
1. Ako a dijeli b, tada je $b = ax \in (a)$ pa je i $(b) \subseteq (a)$. Obratno, ako je $(b) \subseteq (a)$, tada je i $b \in (b) \subseteq (a)$ te postoji $x \in R$ takav da je $b = ax$ pa a dijeli b. Dio 2. slijedi direktno iz dijela 1.
3. Ako je u invertibilan, tada za svaki $r \in R$ vrijedi $r = (ru^{-1})u$ pa u dijeli r. Obratno, ako u dijeli svaki $r \in R$, tada u dijeli i 1 pa je $1 = ux$ za neki $x \in R$ te je u invertibilan.
4. Ako je u invertibilan, tada je $1 = uu^{-1} \in (u)$ pa je $(u) = R$. Obratno, ako je $(u) = R$ tada je $1 \in (u)$ te $1 = ux$ za neki $x \in R$ te je u invertibilan.

Ako je R integralna domena te a, b asocirani elementi iz R, tada iz $a = bx$ i $b = ay$ slijedi $a = axy$ te $xy = 1$ pa su x i y invertibilni, odnosno asocirani elementi se u integralnoj domeni razlikuju za invertibilan element.

Definicija.
Neka je R komutativan prsten s jedinicom 1, $1 \neq 0$. Kažemo da je element $c \in R$ **ireducibilan** ako vrijedi:

1. c je različit od nule i c nije invertibilan,
2. ako je $c = ab$ za neke $a, b \in R$, tada je ili a invertibilan ili b invertibilan.

Primijetimo da ako je c ireducibilan i $c = ab$ tada je točno jedan od elemenata a, b invertibilan. Iz definicije slijedi da barem jedan od tih elemenata mora biti invertibilan, a ako bi oba bili invertibilan tada bi i njihov produkt $ab = c$ bio invertibilan (s inverzom $b^{-1}a^{-1}$), što nije moguće.

Za element koji nije ireducibilan kažemo da je **reducibilan**.

Definicija.
Neka je R komutativan prsten s jedinicom 1, $1 \neq 0$. Kažemo da je element $p \in R$ **prost** ako vrijedi:

1. p je različit od nule i c nije invertibilan,
2. ako c dijeli ab za neke $a, b \in R$, tada p dijeli a ili p dijeli b.

Primjer.
Neka je $p \in \mathbb{Z}$, p prost broj. Tada su p i $-p$ ireducibilni i prosti elementi u prstenu $\mathbb{Z}$.
U prstenu $\mathbb{Z}_6$ je 2 prost, ali nije ireducibilan, jer je $2 = 2 \cdot 4$, a niti 2 niti 4 nisu invertibilni u $\mathbb{Z}_6$.

Teorem.
Neka su p i c nenul elementi u integralnoj domeni R. Tada vrijedi:

1. Element p je prost ako i samo ako je (p) prost ideal.
2. Element c je ireducibilan ako i samo ako je ideal (c) maksimalan u skupu glavnih ideala u R (tj. ne postoji glavni ideal I takav da je $(c) \subsetneq I \subsetneq R$).
3. Svaki prost element u R je ireducibilan.
4. Ako je R domena glavnih ideala, element p je prost ako i samo ako je ireducibilan.

Dokaz:
1. Pretpostavimo najprije da je p prost te neka su $a, b \in R$ takvi da je $ab \in (p)$. Tada je $ab = px$, za neki $x \in R$ pa p dijeli ab. Kako je p prost, tada p dijeli a ili p dijeli b, tj. a je iz (p) ili je b iz (p) pa je ideal (p) prost.
Neka je sada ideal (p) prost te neka p dijeli ab. Tada je $ab \in (p)$ pa je $a \in (p)$ ili $b \in (p)$ te p dijeli a ili p dijeli b te je i element p prost.
2. Neka je c ireducibilan. Te neka je I glavni ideal koji sadrži (c). Treba pokazati da je tada ili $I = (c)$ ili $I = R$. Kako je I glavni ideal, postoji $d \in R$ takav da je $I = (d)$. Iz $(c) \subseteq (d)$ slijedi $c \in (d)$ pa je $c = dx$ za neki $x \in R$. Kako je c ireducibilan, ili je d invertibilan ili je x invertibilan. Ako je d invertibilan, tada je $I = (d) = R$ (prva propozicija, dio 4.). Ako je x invertibilan, tada je $d = cx^{-1}$. Iz $c = dx$ i $d = cx^{-1}$ slijedi da su c i d asocirani pa je $(c) = (d) = I$ (prva propozicija, dio 2.).
Obratno, neka je ideal (c) maksimalan ideal u skupu glavnih ideala u R i neka je $c = ab$. Tada je $c \in (a)$ i $c \in (b)$ pa je $(c) \subseteq (a)$ i $(c) \subseteq (b)$. Ako a nije invertibilan, tada je $(a) \neq R$ pa je $(c) = (a)$ te je i $a \in (c)$. Prema tome, postoji $x \in R$ takav da je $a = cx$. Uvrštavanjem u $c = ab$ dobivamo $c = cxb$, odakle je $xb = 1$ (jer je R integralna domena). Slijedi da je b invertibilan pa je c ireducibilan.
3. Neka je p prost element i neka je $p = ab$. Iz $ab = p \cdot 1$ slijedi da p dijeli ab pa p dijeli a ili p dijeli b. Uzmimo da p dijeli a. Tada je $a = px$, za neki $x \in R$ pa dobivamo $p = pxb$ te $xb = 1$ i b je invertibilan pa je p ireducibilan.
4. Kako je domena glavnih ideala integralna domena, jedan smjer je dokazan u dijelu 3.. Preostaje dokazati suprotan smjer. Neka je p ireducibilan element. Kako je R domena glavnih ideala, iz 2. slijedi da je ideal (p) maksimalan pa je i prost, no tada dio 1. povlači da je i p prost.

Definicija.
Kažemo da je integralna domena R **faktorijalan prsten** ili **domena jedinstvene faktorizacije** ako ima sljedeća dva svojstva:

1. Svaki neinvertibilan element $a \in R$, $a \neq 0$, se može prikazati u obliku

$$a = c_1 c_2 \cdots c_n,$$

gdje su $c_1, c_2, \ldots, c_n$ ireducibilni.

2. Faktorizacija iz $1.$ je jedinstvena do na poredak i množenje pojedinih faktora invertibilnim elementima, tj. ako je $a = c_1 c_2 \cdots c_n$ i $a = d_1 d_2 \cdots d_m$, pri čemu su svi c_i, d_j ireducibilni, tada je $n = m$ te postoji permutacija $\sigma \in S_n$ takva da su c_i i $d_{\sigma(i)}$ asocirani za sve $i = 1, 2, \ldots, n$.

Dio pod $1.$ daje egzistenciju rastava odnosno prikaza svakog nenul neinvertibilnog elementa u obliku produkta ireducibilnih elemenata, dok dio $2.$ daje jedinstvenost takvog prikaza. Na primjer, u prstenu cijelih brojeva $\mathbb{Z}$ imamo iduće rastave broja 15:

$$15 = 3 \cdot 5 = 5 \cdot 3 = (-3) \cdot (-5) = (-5) \cdot (-3).$$

Permutacija iz definicije nam u rastavu omogućava zamjenu poretka, a asociranost pojedinih faktora u integralnoj domeni daje njihovu vezu množenjem invertibilnim elementima (prisjetimo se da su jedini invertibilni elementi u $\mathbb{Z}$ upravo 1 i -1).

Primijetimo da je u faktorijalnom prstenu svaki ireducibilan element ujedno i prost: neka je r ireducibilan element koji dijeli produkt ab, tada je $ab = rx$, za neki $x \in R$. Ako je $a = 0$ ili $b = 0$, tada odmah slijedi da r dijeli a ili r dijeli b. Zato pretpostavim da je $a \neq 0$ i $b \neq 0$. Neka je $a = c_1 \cdot c_n$ i $b = d_1 \cdots d_m$, pri čemu su svi c_i, d_j ireducibilni (ako je a ili b invertibilan, uzmimo rastav samo jednog od njih). Tada je

$$rx = c_1 \cdots c_n \cdot d_1 \cdots d_m.$$

Iz jedinstvenosti rastava na produkt ireducibilnih elemenata slijedi da r mora dijeliti neki od faktora s desne strane prethodne jednakosti. Ako r dijeli neki c_i, tada r dijeli a. Ako r dijeli neki d_j, tada r dijeli b. Prema tome, r je prost.

Lema.
Neka je R domena glavnih ideala i $(a_1) \subseteq (a_2) \subseteq \cdots$ rastući niz ideala u R. Tada postoji neki prirodan broj n takav da je $(a_i) = (a_n)$ za sve $i \geq n$.
`Dokaz:`
Neka je

$$A = \bigcup_{i \geq 1} (a_i).$$

Za $b, c \in A$ postoji j takav da su $b, c \in (a_j)$ pa je i $b - c \in (a_j) \subseteq A$. Također, za $r \in R$ je tada i $br \in (a_j) \subseteq A$, pa je A ideal. Kako je R domena glavnih ideala, postoji $a \in R$ takav da je $A = (a)$. Zbog $a \in A = \bigcup_{i \geq 1} (a_i)$, postoji n takav da je $a \in (a_n)$. Slijedi $(a) \subseteq (a_n)$ te $A = (a_n)$.

Teorem.
Neka je R domena glavnih ideala. Tafa je R faktorijalan prsten.
`Dokaz:`
Označimo sa S skup svih nenul neinvertibilnih elemenata iz R koji se ne mogu prikazati u obliku produkta konačno mnogo ireducibilnih elemenata. Tvrdimo da je

$S = \emptyset$. Pretpostavimo suprotno i neka je $a \in S$. Tada a nije ireducibilan (jer bi se inače mogao na trivijalan način prikazati kao produkt ireducibilnih elemenata) pa ideal (a) nije maksimalan. Ideal (a) je sadržan u nekom maksimalnom idealu pa postoji ireducibilan element $c \in R$ takav da je $a \in (c)$ i $a = cx$ za neki $x \in R$. Slijedi da je i $x \in S$, jer bi inače x mogli prikazati u obliku $x = c_1 \cdots c_n$, gdje su svi c_i ireducibilni, što povlači da je $a = cc_1 \cdots c_n$, produkt ireducibilnih elemenata, što nije moguće.
Također, x dijeli a pa je $(a) \subseteq (x)$. Kada bi vrijedilo $(a) = (x)$, x bi morao biti oblika ay za neki $y \in R$, što povlači $a = acy$ te $cy = 1$, što nije moguće jer je c ireducibilan pa nije invertibilan. Dakle, $(a) \subsetneq (x)$. Označimo li x s a_1, dobivamo element $a_1 \in S$ takav da je $(a) \subsetneq (a_1)$ te ponovimo li isti postupak s elementom a_1 dobivamo element $a_2 \in S$ takav da je $(a_1) \subsetneq (a_2)$. Induktivno dobivamo rastući niz ideala $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots$, što nije moguće prema prethodnoj lemi. Dakle, $S = \emptyset$.
Preostaje još dokazati jedinstvenost rastava. Neka je

$$a = c_1 c_2 \cdots c_n = d_1 d_2 \cdots d_m,$$

pri čemu su svi c_i, d_j ireducibilni. Kako c_1 dijeli $c_1 c_2 \cdots c_n$, slijedi da c_1 dijeli i $d_1 d_2 \cdots d_m$. Vidjeli smo da je ireducibilan element u domeni glavnih ideala ujedno i prost, pa postoji $i \in \{1, 2, \ldots, m\}$ takav da c_1 dijeli d_i. Zato je $d_i = x_1 c_1$, a kako je d_i ireducibilan x_1 mora biti invertibilan (jer jedan od elemenata x_1 i c_1 mora biti invertibilan, a c_1 je ireducibilan pa nije invertibilan). Sada je

$$c_1 c_2 \cdots c_n = d_1 d_2 \cdots d_{i-1} x_1 c_1 d_{i+1} \cdots d_m,$$

a kako je R integralna domena slijedi

$$c_2 \cdots c_n = x_1 d_1 d_2 \cdots d_{i-1} d_{i+1} \cdots d_m.$$

Ostatak dokaza sada slijedi induktivno.

Faktorizacija u prstenima polinoma

Ako je K polje, ranije smo vidjeli da je tada $K[x]$ domena glavnih ideala. Prema tome, $K[x]$ je i faktorijalan prsten. Dakle, polinome čiji su koeficijenti iz polja možemo prikazati u obliku produkta ireducibilnih polinoma, pri čemu su faktori jedinstveni do na poredak i asociranost.

Sada ćemo otići korak dalje te vidjeti što se može reći za polinome čiji su koeficijenti iz faktorijalnog prstena, tj. proučit ćemo svojstva prstena polinoma $R[x]$ u slučaju da je R faktorijalan prsten.

Pri tome će nam pomoći i polje koje je najbliže faktorijalnom prstenu R (koji je i integralna domena), a to je polje kvocijenata od R. Prisjetimo se kako pomoću ulaganja $a \mapsto \frac{a}{1}$ možemo R identificirati s potprstenom polja kvocijenata od R. Također, primijetimo da za integralnu domenu R vrijedi $R[x]^\times = R^\times$, jer u ovom slučaju jed1ino polinomi stupnja 0, tj. konstante, mogu biti invertibilni (ako je $f \in R[x]$ polinom stupnja barem 1, tada je za svaki $g \in R[x]$, $g \neq 0$, fg polinom stupnja barem 1, jer je R integralna domena, a za $g = 0$ je $fg = 0$, te ne postoji polinom $g \in R[x]$ takav da je $fg = 1$ te f nije invertibilan).

Od sada nadalje u ovom poglavlju će R označavati faktorijalan prsten.

Definicija.
Neka su $a_1, a_2, \ldots, a_n \in R$ takvi da je $a_i \neq 0$ barem za jedan $i \in \{1, 2, \ldots, n\}$. *Najveća zajednička mjera elemenata* $a_1, a_2, \ldots, a_n$ je element $c \in R$ koji ima sljedeća dva svojstva:

1. c dijeli a_i, za sve $i \in \{1, 2, \ldots, n\}$,
2. ako je $d \in R$ takav da d dijeli a_i, za sve $i \in \{1, 2, \ldots, n\}$, tada d dijeli c.

Primjer.
U prstenu $\mathbb{Z}$ su 2 i -2 najveće zajedničke mjere elemenata $2, 4, 8$.

Najveća zajednička mjera elemenata koji nisu svi jednaki nuli postoji i ne mora biti jedinstvena. Ako su $a_1, a_2, \ldots, a_n \in R$ takvi da je $a_i \neq 0$ barem za jedan $i \in \{1, 2, \ldots, n\}$, primijetimo da su svake dvije najveće zajedničke mjere elemenata $a_1, a_2, \ldots, a_n \in R$ asocirane.

Zaista, označimo li dvije najveće zajedničke mjere ovih elemenata s c_1 i c_2, tada iz prethodne definicije slijedi da c_1 dijeli c_2 i c_2 dijeli c_1 pa su c_1 i c_2 asocirani te postoji invertibilan element $u \in R$ takav da je $c_1 = uc_2$.

Neka je sada c najveća zajednička mjera elemenata $a_1, a_2, \ldots, a_n$ koji nisu svi jednaki nuli te neka je u invertibilan element iz R. Pokažimo da je tada i $u \cdot c$ također najveća zajednička mjera elemenata $a_1, a_2, \ldots, a_n$: kako c dijeli a_i, za $i \in \{1, 2, \ldots, n\}$, postoji $b_i \in R$ takav da je $a_i = cb_i$. Tada je i $a_i = (uc)u^{-1}b_i$ pa i uc dijeli a_i, za $i \in \{1, 2, \ldots, n\}$. Također, ako je $d \in R$ takav da d dijeli a_i, za sve $i \in \{1, 2, \ldots, n\}$, tada postoji $b \in R$ takav da je $c = db$ pa je $uc = d(ub)$ pa d dijeli i uc.

Dakle, najveća zajednička mjera elemenata $a_1, a_2, \ldots, a_n$ koji nisu svi jednaki nuli je jedinstvena do na množenje invertibilnim elementima, tj. najveća zajednička mjera je klasa asociranosti (klasu asociranosti elementa c čine svi elementi koji su asocirani s c te je klasa asociranosti od c jednaka $\{uc : u \in R^\times\}$). U daljnjem ćemo

klasu asociranosti nekog elementa označavati samo tim elementom, tj. odabirom jednog predstavnika.

Definicija.

Neka je $f \in R[x]$, $f = \sum_{i=0}^{n} a_i x^i$. *Sadržaj polinoma* f je najveća zajednička mjera koeficijenata $a_0, a_1, \ldots, a_n$. Sadržaj polinoma f označavamo s $C(f)$ (od content of f).

Primjer.

Neka je $f = 2x^3 + 4x - 2 \in \mathbb{Z}[x]$. Tada je $C(f) = 2$. Najveća zajednička mjera koeficijenata $2, 0, 4, -2$ polinoma f je klasa asociranosti $2, -2$ elementa 2. Analogno smo mogli uzeti i da je $C(f) = -2$.

Definicija.

Kažemo da je polinom $f \in R[x]$ *primitivan* ako je $C(f)$ invertibilan, odnosno ako ne postoji neinvertibilan element iz R koji dijeli sve koeficijente polinoma f.

Ako je polinom f primitivan, tada možemo uzeti da je $C(f) = 1$, jer je u tom slučaju skup najvećih zajedničkiih mjera koeficijenata polinoma f jednak $R^\times$, a $1 \in R^\times$.

Primjer.

Polinom $f = 2x^3 + 4x - 2 \in \mathbb{Z}[x]$ nije primitivan. Polinom $g = x^3 + 2x - 1 \in \mathbb{Z}[x]$ je primitivan, jer je $C(f) = 1$. Također, primijetimo da je $f = 2g = C(f)g$.

Lema (Gaussova lema).

Ako su $f, g \in R[x]$, tada je $C(f \cdot g) = C(f) \cdot C(g)$. Posebno, produkt primitivnih polinoma je primitivan.

Dokaz:

Primijetimo da za $a \in R$ vrijedi $C(a \cdot f) = aC(f)$, jer u produktu $a \cdot f$ sve koeficijente polinoma f množimo s a. Polinome f i g možemo zapisati u obliku $f = C(f)f_1$, $g = C(g)g_1$, pri čemu su $f_1, g_1 \in R[x]$ primitivni polinomi (kada iz polinoma izlučimo njegov sadržaj, dobiveni polinom je primitivan). Tada vrijedi

$$C(f \cdot g) = C\big(C(f)C(g)f_1g_1\big) = C(f)C(g)C(f_1g_1)$$

pa je za dokaz ove leme dovoljno dokazati da je $C(f_1g_1) = 1$, tj. da je polinom f_1g_1 primitivan.

Neka je $f_1 = \sum_{i=0}^{n} a_i x^i$, $g_1 = \sum_{j=0}^{m} b_j x^j$. Tada je $f_1g_1 = \sum_{k=0}^{m+n} c_k x^k$, pri čemu je $c_k = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0$. Pretpostavimo da polinom f_1g_1 nije primitivan. Tada $C(f_1g_1)$ nije invertibilan te se u faktorijalnoj domeni R može prikazati u obliku produkta ireducibilnih elemenata (koji su u faktorijalnoj domeni također i prosti). Ovdje za sadržaj od f_1g_1 uzimamo jednog predstavnika klase asociranosti najveće zajedničke mjere koeficijenata od f_1g_1. Dakle, postoji ireducibilan element $p \in R$ takav da p dijeli c_k za sve $k = 0, 2, \ldots, m + n$. Kako je f_1 primitivan, p ne dijeli $C(f_1)$ te postoji $i \in \{0, 1, \ldots, n\}$ takav da p ne dijeli a_i te neka je s najmanji takav. Prema tome, p dijeli $a_0, a_1, \ldots, a_{s-1}$, ali p ne dijeli a_s. Na isti način možemo zaključiti da postoji $t \in \{0, 1, \ldots, m\}$ takav da p dijeli $b_0, b_1, \ldots, b_{t-1}$, ali p ne dijeli b_t. Primijetimo da je

$$c_{s+t} = a_0b_{s+t} + \cdots + a_{s-1}b_{t+1} + a_sb_t + a_{s+1}b_{t-1} + \cdots + a_{s+t}b_0.$$

Kako p dijeli $a_0, \ldots, a_{s-1}$, slijedi da p dijeli $a_0b_{s+t}, \ldots, a_{s-1}b_{t+1}$. Kako p dijeli $b_0, \ldots, b_{t-1}$, slijedi da p dijeli $a_{s+1}b_{t-1}, \ldots, a_{s+t}b_0$. Također, p dijeli i c_{s+t} pa p

mora dijeliti i $a_s b_t$. No, p je prost pa slijedi da p dijeli a_s ili p dijeli b_t, što nije moguće. Prema tome, polinom $f_1 g_1$ je primitivan te je $C(f \cdot g) = C(f) \cdot C(g)$.

U nastavku ovog poglavlja ćemo s K označavati polje kvocijenata faktorijalnog prstena R. Prema ranijoj konvenciji, izjednačavajući element $a \in R$ s elementom $\frac{a}{1} \in K$, prsten R ćemo smatrati potprstenom polja K te zato možemo prsten $R[x]$ smatrati potprstenom faktorijalne domene $K[x]$. U iduća dva rezultata ćemo vidjeti odnos svojstava primitivnih polinoma u $R[x]$ i u $K[x]$.

Lema.
Neka je K polje kvocijenata faktorijalnog prstena $R[x]$ te neka su $f, g \in R[x]$ primitivni polinomi. Tada su f i g asocirani u $R[x]$ ako i samo ako su asocirani u $K[x]$.
`Dokaz:`
Kako su i $R[x]$ i $K[x]$ integralne domene, polinomi f i g su asocirani u $R[x]$ ako i samo ako postoji invertibilan element u iz $R[x]$ takav da je $f = ug$ te su polinomi f i g asocirani u $K[x]$ ako i samo ako postoji invertibilan element v iz $K[x]$ takav da je $f = vg$. Uočimo da je $R[x]^\times = R^\times$, dok je $K[x]^\times = K \setminus \{0\}$, jer je K polje. Zato je $R[x]^\times \subseteq K[x]^\times$.
Prema tome, ako su f i g asocirani u $R[x]$, tada postoji $u \in R[x]^\times$ takav da je $f = ug$, no zbog $R[x]^\times \subseteq K[x]^\times$ je $u \in K[x]^\times$ pa su f i g asocirani i u $K[x]$. Primijetimo da u dokazu ovog smjera nismo koristiti činjenicu da su f i g primitivni.
Obratno, neka su f i g primitivni polinomi koji su asocirani u $K[x]$ te neka je $v \in K[x]^\times = K \setminus \{0\}$ takav da je $f = vg$. Kako je $v \in K \setminus \{0\}$, postoje $a, b \in R$, $b \neq 0$, takvi da je $v = \frac{a}{b}$. Sada je $f = \frac{a}{b} g$, odakle je $bf = ag$. Kako su f i g primitivni polinomi, možemo uzeti da je $C(f) = C(g) = 1$ pa imamo iduće jednakosti klasa asociranosti:

$$b = b \cdot 1 = bC(f) = C(bf) = C(ag) = aC(g) = a \cdot 1 = a.$$

Slijedi da a i b pripadaju istoj klasi asociranosti pa je $a = bu$ za neki invertibilan element $u \in R$. Sada je

$$f = \frac{a}{b} g = \frac{bu}{b} g = ug,$$

za $u \in R^\times = R[x]^\times$ te su f i g asocirani i u $R[x]$.

Primjer.
Općenito, polinomi mogu biti asocirani u $K[x]$, ali ne i u $R[x]$. Ukoliko je $R = \mathbb{Z}$, tada je $K = \mathbb{Q}$ te su polinomi $f = 2x^2 + 2$ i $g = 3x^2 + 3$ asocirani u $\mathbb{Q}[x]$, jer je $f = \frac{2}{3} g$ i $g = \frac{3}{2} f$, ali f i g nisu asocirani u $\mathbb{Z}[x]$, jer u prsteni $\mathbb{Z}[x]$ niti f ne dijeli g niti g ne dijeli f.

Lema.
Neka je K polje kvocijenata faktorijalnog prstena $R[x]$ te neka $f \in R[x]$ primitivan polinom pozitivnog stupnja. Tada je f ireducibilan u $R[x]$ ako i samo ako je f ireducibilan u $K[x]$.
`Dokaz:`
Neka je najprije f ireducibilan u $R[x]$ te pretpostavimo da f nije ireducibilan u $K[x]$. Prema definiciji ireducibilnog elementa, postoje neinvertibilnih elementi $g, h \in K[x]$

takvi da je $f = gh$. Očito je $g \neq 0$ i $h \neq 0$. Kako je $K[x]^\times = K \setminus \{0\}$, slijedi $g, h \notin K$ pa su g i h polinomi stupnja barem 1. Zapišimo ih u obliku

$$g = \sum_{i=0}^{n} \frac{a_i}{b_i} x^i, h = \sum_{j=0}^{m} \frac{c_j}{d_j} x^j,$$

za neke $a_i, b_i, c_j, d_j \in R$, $b_i \neq 0$, $d_j \neq 0$ za sve i, j. Neka je $b = b_0 b_1 \cdots b_n$ i $b_i^* = b_0 \cdots b_{i-1} b_{i+1} \cdots b_n$ za $i = 0, 1, \ldots, n$. Neka je g_1 polinom definiran s $g = \frac{1}{b} g_1$. Tada je $g_1 = \sum_{i=0}^{n} a_i b_i^* x^i$ pa je $g_1 \in R[x]$ (kao da smo izlučili zajednički nazivnik). Nadalje, neka je $a = C(g_1)$ i neka je polinom $g_2 \in R[x]$ definiran s $g_1 = a g_2$. Sada je polinom g_2 primitivan polinom stupnja jednakog stupnju polinoma g te vrijedi

$$g = \frac{a}{b} g_2.$$

Na isti način vidimo da postoje $c, d \in R$, $d \neq 0$, i primitivan polinom $h_2 \in R[x]$ stupnja jednakog stupnju polinoma h, takav da je

$$h = \frac{c}{d} h_2.$$

Odatle je

$$f = gh = \frac{ac}{bd} g_2 h_2$$

te $bdf = ac g_2 h_2$. Po pretpostavci leme je polinom f primitivan, a iz Gaussove leme slijedi da je i polinom $g_2 h_2$ primitivan kao produkt primitivnih polinoma. Zato vrijedi iduća jednakost klasa asociranosti:

$$bd = bd \cdot 1 = bdC(f) = C(bdf) = C(acg_2h_2) = acC(g_2h_2) = ac.$$

Dakle, postoji invertibilan element $u \in R$ takav da je $ac = ubd$, odakle je

$$f = \frac{ac}{bd} g_2 h_2 = \frac{bdu}{bd} g_2 h_2 = u g_2 h_2 = (u g_2) h_2.$$

Polinomi ug_2 i h_2 su polinomi stupnja barem 1 pa nisu invertibilni u $R[x]$ te, kako smo prikazali f u obliku produkta neinvertibilnih elemenata, slijedi da f nije ireducibilan u $R[x]$, što nije moguće. Prema tome, f mora ireducibilan u $K[x]$.
Obratno, pretpostavimo da je f ireducibilan u $K[x]$ te neka je $f = gh$, za polinome $g, h \in R[x]$. Da pokažemo da je f ireducibilan u $R[x]$, treba pokazati da je ili g invertibilan ili h invertibilan u $R[x]$. Iz $R[x] \subseteq K[x]$ slijedi $g, h \in K[x]$. Ako bi oba polinoma g i h bili stupnja barem 1, tada niti jedan od njih ne bi bio invertibilan u $K[x]$, jer je skup svih invertibilnih elemenata u $K[x]$ jednak $K \setminus \{0\}$, pa polinom f ne bi bio ireducibilan u $K[x]$. Prema tome, jedan od polinoma g i h mora biti stupnja 0, te možemo uzeti da je $g \in R$, $g \neq 0$. Tada je $C(f) = C(gh) = gC(h)$, a kako je f primitivan je $C(f) = 1$ te iz $gC(h) = 1$ slijedi da je g invertibilan, tj. $g \in R^\times = R[x]^\times$ pa je f ireducibilan i u $R[x]$.

Primjer.
Neka je $f = 2x + 2$ polinom iz $\mathbb{Z}[x]$, koji očito nije primitivan i $C(f) = 2$. Tada je

$f = 2(x+1)$ pa f nije ireducibilan u $\mathbb{Z}[x]$ jer niti 2 niti $x+1$ nisu invertibilni u $\mathbb{Z}[x]$. S druge strane, polinom f je ireducibilan u $\mathbb{Q}[x]$, jer je jedini način za prikazati f u obliku produkta dvaju polinoma $f = c(\frac{2}{c}x + \frac{2}{c})$, $c \neq 0$, a nenul element c je invertibilan u $\mathbb{Q}[x]$.

Teorem.
Ako je R faktorijalan prsten, tada je i $R[x]$ faktorijalan prsten.
Dokaz:
Najprije pokažimo da se svaki element iz $R[x]$ može prikazati u obliku produkta ireducibilnih elemenata. Neka je $f \in R[x]$. Ako je f polinom stupnja 0 (tj. ako je $f \in R$), tada ova tvrdnja odmah slijedi jer je R faktorijalan prsten.
Neka je f polinom pozitivnog stupnja. Polinom f možemo prikazati u obliku $f = C(f)f_1$, pri čemu je $f_1 \in R[x]$ primitivan polinom. Kako je R faktorijalan prsten, tada je ili $C(f)$ invertibilan ili je $C(f) = c_1c_2\cdots c_m$, pri čemu su svi elementi $c_1, c_2, \ldots, c_m$ ireducibilni u R. No, tada su svi $c_1, c_2, \ldots, c_m$ ireducibilni i u $R[x]$, jer ako prikažemo c_i u obliku $a \cdot b$, za $a, b \in R[x]$, tada a i b moraju biti polinomi stupnja 0, dakle $a, b \in R$ pa je jedan od njih invertibilan.
Neka je K polje kvocijenata od R. Tada je $K[x]$ faktorijalan prsten te postoje ireducibilni elementi $p_1^*, p_2^*, \ldots, p_n^* \in K[x]$ takvi da je $f_1 = p_1^* \cdot p_2^* \cdots p_n^*$. Kao u dokazu prethodne leme, svaki p_i^*, za $i = 1, 2, \ldots, n$, možemo prikazati u obliku

$$p_i^* = \frac{a_i}{b_i} p_i,$$

pri čemu su $a_i, b_i \in R$, $b_i \neq 0$, te je p_i primitivan polinom iz $R[x]$.
Pokažimo da je polinom p_i ireducibilan u $K[x]$. Pretpostavimo suprotno, neka p_i nije ireducibilan. Tada postoje $g, h \in K[x]$, koji nisu invertibilni, takvi da je $p_i = g \cdot h$ za $g, h \in R[x]$. Kako je $K[x]^\times = K \setminus \{0\}$, oba su polinoma g i h stupnja barem 1 te dobivamo $p_i^* = \frac{a_i}{b_i} gh$, što nije moguće jer je p_i^* ireducibilan, a $\frac{a_i}{b_i} g$ i h su polinomi pozitivnog stupnja iz $K[x]$, koji nisu invertibilni. Prema tome, p_i je primitivan polinom koji je ireducibilan u $K[x]$ pa je ireducibilan i u $R[x]$, prema prethodnoj lemi.
Za $a = a_1a_2\cdots a_n$, $b = b_1b_2\cdots b_n$ je $f_1 = \frac{a}{b} p_1p_2\cdots p_n$, odakle je $bf_1 = ap_1p_2\cdots p_n$. Polinom $p_1p_2\cdots p_n$ je primitivan kao produkut primitivnih polinoma, prema Gaussovoj lemi. Kako je polinom f_1 također primitivan, na isti način kao u dokazu prethodne leme dobivamo da su a i b asocirani u R te postoji $u \in R^\times$ takav da je $\frac{a}{b} = u$ i $f_1 = up_1p_2\cdots p_n$.
Zato je $f = C(f)f_1 = C(f)up_1p_2\cdots p_n$ te se f može prikazati kao produkt ireducibilnih elemenata u $R[x]$.
Preostaje dokazati jedinstvenost takvog prikaza. Neka je

$$f = c_1c_2\cdots c_mp_1p_2\cdots p_n = d_1d_2\cdots d_rq_1q_2\cdots q_s,$$

gdje su $c_1, c_2, \ldots, c_m, d_1, d_2, \ldots, d_r$ ireducibilni elementi iz R te $p_1, p_2, \ldots, p_n$, $q_1, q_2, \ldots, q_s$ ireducibilni primitivni elementi u $R[x]$. Kako je $C(f) = c_1c_2\cdots c_m = d_1d_2\cdots d_r$, jedinstvenost faktorizacije u R povlači $m = r$ te postoji permutacija $\sigma_1 \in S_m$ takva da su c_i i $d_{\sigma_1(i)}$ asocirani za sve $i = 1, 2, \ldots, m$. Slijedi da su i $c_1c_2\cdots c_m$ i $d_1d_2\cdots d_r$ asocirani, jer sada $d_1d_2\cdots d_r$ možemo zapisati u obliku $c_1c_2\cdots c_mu$, za neki invertibilni element $u \in R$. Prema tome, dobivamo

$p_1p_2\cdots p_n = uq_1q_2\cdots q_s$ pa su polinomi $p_1p_2\cdots p_n$ i $q_1q_2\cdots q_s$ asocirani u $R[x]$. Kako su, prema Gaussovoj lemi, polinomi $p_1p_2\cdots p_n$ i $q_1q_2\cdots q_s$ primitivni, iz ranije leme slijedi da su $p_1p_2\cdots p_n$ i $q_1q_2\cdots q_s$ asocirani i u $K[x]$. Kako je $K[x]$ domena jedinstvene faktorizacije, jedinstvenost faktorizacije u $K[x]$ povlači da je $n = s$ te postoji permutacija $\sigma_2 \in S_n$ takva da su p_i i $q_{\sigma_2(i)}$ asocirani u $K[x]$ za sve $i = 1, 2, \ldots, n$. Kako su p_i i $q_{\sigma_2(i)}$ primitivni, iz ranije leme slijedi da su asocirani i u $R[x]$, čime je pokazana i jedinstvenost faktorizacije u $R[x]$ pa je $R[x]$ faktorijalna domena.

Korolar.
Kako je $\mathbb{Z}$, i $\mathbb{Z}[x]$ je faktorijalan prsten. Ako je R faktorijalan prsten, tada je i $R[x_1, x_2] = (R[x_1])[x_2]$ faktorijalan prsten, jer je $R[x_1]$ faktorijalan prsten. Induktivno slijedi da je i $R[x_1, x_2, \ldots, x_n]$ faktorijalan prsten za sve $n \in \mathbb{N}$.

Teorem (Eisensteinov kriterij).
Neka je R faktorijalan prsten s poljem kvocijenata K. Ako je $f \in R[x]$ polinom pozitivnog stupnja, $f = \sum_{i=0}^{n} a_i x^i$ i p ireducibilan element iz R takav da p ne dijeli a_n, p dijeli a_i za sve $i = 0, 1, \ldots, n-1$ te p^2 ne dijeli a_0, tada je f ireducibilan u $K[x]$. Ako je f primitivan, tada je f ireducibilan i u $R[x]$.
Dokaz:
Neka je $f = C(f)f_1$, gdje je $f_1 \in R[x]$ primitivan i $C(f) \in R$. Ako je f primitivan, tada je $f = f_1$. Očito je $C(f)$ invertibilan u K. Ako f nije ireducibilan u $K[x]$, tada možemo f prikazati u obliku produkta dva polinoma pozitivnog stupnja u $K[x]$, no tada i f_1 možemo f prikazati u obliku produkta dva polinoma pozitivnog stupnja u $K[x]$ pa niti f_1 nije ireducibilan. Prema tome, da bi pokazali da je f ireducibilan u $K[x]$ je dovoljno dokazati da je f_1 ireducibilan u $K[x]$. Kako je f_1 primitivan, iz ranije leme slijedi da je dovoljno dokazati da je f_1 ireducibilan u $R[x]$.
Pretpostavimo suprotno, neka f_1 nije ireducibilan u $R[x]$. Tada postoje $g, h \in R[x]$, koji nisu invertibilni, takvi da je $f_1 = gh$. Kako je f_1 primitivan, oba polinoma g i h moraju biti stupnja barem 1, jer ako je na primjer $g \in R$ tada slijedi $f_1 = gh$ te $C(f_1) = 1 = gC(h)$, što nije moguće jer g nije invertibilan.
Neka je $g = \sum_{i=0}^{r} b_i x_i \in R[x]$, $r \geq 0$ i $g = \sum_{j=0}^{s} c_j x_j \in R[x]$, $s \geq 0$. Također, neka je $a_i = C(f)a_i^*$, za $i = 0, 1, \ldots, n$. Tada je $f_1 = \sum_{i=0}^{n} a_i^* x^i$. Kako p ne dijeli a_n, p ne dijeli $C(f)$, p ne dijeli a_n^*, p dijeli a_i^* za sve $i = 0, 1, \ldots, n-1$ te p^2 ne dijeli a_0^*.
Kako je $f_1 = gh$, slijedi $a_i^* = b_0c_i + b_1c_{i-1} + \cdots + b_ic_0$, za sve $i = 0, 1, \ldots, n$. Kako p dijeli a_0 i $a_0 = b_0c_0$, slijedi da p dijeli b_0 ili p dijeli c_0, jer je svaki ireducibilan element uz faktorijalnoj domeni prost.
Možemo uzeti da p dijeli b_0. Kako p^2 ne dijeli a_0, slijedi da p ne dijeli c_0. Također, kako p ne dijeli a_n, slijedi da postoji $k \in \mathbb{N}$ takav da p dijeli b_i za sve $i = 0, 1, \ldots, k-1$ te p ne dijeli b_k. Kako je $r \geq 1$ i $s \geq 1$, koristeći $r + s = n$ dobivamo $k \leq r < n$. Tada p dijeli a_k^* te iz $a_k^* = b_0c_k + b_1c_{k-1} + \cdots + b_{k-1}c_1 + b_kc_0$ slijedi da p dijeli b_kc_0, jer p dijeli sve preostale sumande s desne strane prethodne jednakosti. Kako je p prost, slijedi da p dijeli b_k ili p dijeli c_0, što nije moguće. Zato je f_1 ireducibilan u $R[x]$.

Primjer.
Neka je $f = 2x^5 - 6x^3 + 9x^2 - 15 \in \mathbb{Z}[x]$. Eisensteinov kriterij, uz $p = 3$, povlači

da je f ireducibilan i u $\mathbb{Q}[x]$ i u $\mathbb{Z}[x]$ (primijetimo da je f primitivan polinom).

Proširenja polja
Osnovni pojmovi

Definicija.
Neka su K i L polja, $K \subseteq L$, uz iste operacije. Tada kažemo da je L **proširenje polja** K te da je K **potpolje od** L**.** Ukoliko su K, L i M polja, $K \subseteq L \subseteq M$, uz iste operacije, tada kažemo da je L **međupolje**.

Ako je L proširenje polja K, tada L možemo promatrati i kao vektorski prostor nad poljem K. Zaista, znamo da je L obzirom na zbrajanje Abelova grupa te da za $k \in K$ i $l \in L$ vrijedi $k \cdot l \in L$, jer je $K \subseteq L$. Preostala svojstva vektorskog prostora slijede direktno iz svojstava polja L, jer je L ujedno i prsten, a sve se operacije odvijaju unutar L.

Definicija.
Neka je L proširenje polja K. Ako je L konačnodimenzionalan vektorski prostor nad K, tada kažemo da je L **konačno proširenje polja** K, a dimenziju tog vektorskog prostora nazivamo **stupanj proširenja** i označavamo s $[L : K]$. Ukoliko L nije konačno proširenje polja K, tada pišemo $[L : K] = \infty$.

Primjer.
Polje kompleksnih brojeva $\mathbb{C}$ je konačno proširenje polja realnih brojeva $\mathbb{R}$ te vrijedi $[\mathbb{C} : \mathbb{R}] = 2$ (prisjetimo se, jedna baza ovog vektorskog prostora je $\{1, i\}$). Polje realnih brojeva $\mathbb{R}$ nije konačno proširenje polja racionalnih brojeva $\mathbb{Q}$, $[\mathbb{R} : \mathbb{Q}] = \infty$.

Lema.
Neka su K i L polja te neka je $\varphi : K \to L$ netrivijalni homomorfizam prstena, tj. neka postoji $a \in K$ takav da je $\varphi(a) \neq 0$ te za $a, b \in K$ vrijedi $\varphi(a + b) = \varphi(a) + \varphi(b), \varphi(ab) = \varphi(a)\varphi(b)$. Tada je φ unitalni monomorfizam.
Dokaz:
Jezgra od φ je ideal u K, a jedini ideali u polju K su (0) i K. Kako postoji $a \in K$ koji nije u jezgri od φ, slijedi da je jezgra od φ jednaka (0) pa je φ monomorfizam. Prema tome, za $a \in K$, $a \neq 0$, vrijedi $\varphi(a) \neq 0$. Sada je, za $a \in K$, $a \neq 0$, $\varphi(a) = \varphi(a \cdot 1_K) = \varphi(a)\varphi(1_K)$, odakle množenjem s $\varphi(a)^{-1}$ slijedi $\varphi(1_K) = 1_L$.

Teorem.
Neka je K polje i $P \in K[x]$ nekonstantni polinom. Tada postoji proširenje L polja K takvo da za neki $\alpha \in L$ vrijedi $P(\alpha) = 0$. Drugim riječima, za svaki nekonstantni polinom s koeficijentima iz polja, postoji proširenje tog polja u kojem taj polinom ima nultočku.

Primjer.
Polinom $P = x^2 + 1 \in \mathbb{Q}[x]$ ima nultočku i u polju kompleksnih brojeva $\mathbb{C}$.

Neka je L proširenje polja K. Za $\alpha \in L$ s $K[\alpha]$ označavamo najmanji potprsten od L koji sadrži i K i α, tj. ako je M potprsten od L takav da je $K \subseteq M$ i $\alpha \in M$, tada je $K[\alpha] \subseteq M$.

Kako je $K[\alpha]$ prsten, iz $\alpha \in K[\alpha]$ slijedi $\alpha^2 \in K[\alpha], \alpha^3 \in [\alpha]$ te općenito i $\alpha^n \in [\alpha]$ za svaki prirodan broj n. Nadalje, iz $K \subseteq K[\alpha]$, sada slijedi da za prirodan broj n te $a_0, a_1, \ldots, a_n \in K$ vrijedi i $a_n\alpha^n + \ldots + a_1\alpha + a_0 \in K[\alpha]$,

tj. za svaki $P \in K[x]$ je $P(\alpha) \in K[\alpha]$ te $\{P(\alpha) : P \in K[x]\} \subseteq K[\alpha]$. Očito je $\alpha \in \{P(\alpha) : P \in K[x]\}$ te $K \subseteq \{P(\alpha) : P \in K[x]\}$. Također, za $P, Q \in K[x]$ je $P - Q \in K[x]$ i $P \cdot Q \in K[x]$ pa je i $P(\alpha) - Q(\alpha) \in K[\alpha]$ i $P(\alpha)Q(\alpha) \in K[\alpha]$. Zato je $\{P(\alpha) : P \in K[x]\}$ potprsten od K pa je $K[\alpha] \subseteq \{P(\alpha) : P \in K[x]\}$. Slijedi

$$K[\alpha] = \{P(\alpha) : P \in K[x]\}.$$

S $K(\alpha)$ označavamo najmanje potpolje od L koji sadrži i K i α, tj. ako je M potpolje od L takvo da je $K \subseteq M$ i $\alpha \in M$, tada je $K(\alpha) \subseteq M$. Vrijedi $K \subseteq K(\alpha) \subseteq L$ i $K[\alpha] \subseteq K(\alpha)$. Prema tome, za $Q \in K[x]$ je $Q(\alpha) \in K(\alpha)$ pa ukoliko je $Q(\alpha) \neq 0$ vrijedi i $Q(\alpha)^{-1} \in K(\alpha)$, jer je $K(\alpha)$ polje. Zato za $P, Q \in K[x]$, pri čemu je $Q(\alpha) \neq 0$, vrijedi $P(\alpha)Q(\alpha)^{-1} \in K(\alpha)$ te je $\{P(\alpha)Q(\alpha)^{-1} : P, Q \in K[x], Q(\alpha) \neq 0\} \subseteq K(\alpha)$. Očito je $\alpha \in \{P(\alpha)Q(\alpha)^{-1} : P, Q \in K[x], Q(\alpha) \neq 0\}$ te $K \subseteq \{P(\alpha)Q(\alpha)^{-1} : P, Q \in K[x], Q(\alpha) \neq 0\}$. Nadalje, neka su $P_1, P_2, Q_1, Q_2 \in K[x]$ takvi da je $Q_1(\alpha) \neq 0$ i $Q_2(\alpha) \neq 0$. Tada je

$$P_1(\alpha)Q_1(\alpha)^{-1} - P_2(\alpha)Q_2(\alpha)^{-1} = (P_1(\alpha)Q_2(\alpha) - P_2(\alpha)Q_1(\alpha))(Q_1(\alpha)Q_2(\alpha))^{-1}$$

pa je i $P_1(\alpha)Q_1(\alpha)^{-1} - P_2(\alpha)Q_2(\alpha)^{-1} \in \{P(\alpha)Q(\alpha)^{-1} : P, Q \in K[x], Q(\alpha) \neq 0\}$. Također,

$$P_1(\alpha)Q_1(\alpha)^{-1} \cdot P_2(\alpha)Q_2(\alpha)^{-1} = (P_1(\alpha)P_2(\alpha))(Q_1(\alpha)Q_2(\alpha))^{-1}$$

te je i $P_1(\alpha)Q_1(\alpha)^{-1} \cdot P_2(\alpha)Q_2(\alpha)^{-1} \in \{P(\alpha)Q(\alpha)^{-1} : P, Q \in K[x], Q(\alpha) \neq 0\}$, čime smo pokazali da je $\{P(\alpha)Q(\alpha)^{-1} : P, Q \in K[x], Q(\alpha) \neq 0\}$ prsten. Neka je $P_1(\alpha)Q_1(\alpha)^{-1} \in \{P(\alpha)Q(\alpha)^{-1} : P, Q \in K[x], Q(\alpha) \neq 0\}$, $P_1(\alpha)Q_1(\alpha)^{-1} \neq 0$. Tada je $P_1(\alpha) \neq 0$ pa je $Q_1(\alpha)P_1(\alpha)^{-1} \in \{P(\alpha)Q(\alpha)^{-1} : P, Q \in K[x], Q(\alpha) \neq 0\}$ te iz

$$P_1(\alpha)Q_1(\alpha)^{-1} \cdot Q_1(\alpha)P_1(\alpha)^{-1} = 1$$

slijedi da je $\{P(\alpha)Q(\alpha)^{-1} : P, Q \in K[x], Q(\alpha) \neq 0\}$ polje. Zato je $K(\alpha) \subseteq \{P(\alpha)Q(\alpha)^{-1} : P, Q \in K[x], Q(\alpha) \neq 0\}$.

Time smo pokazali

$$K(\alpha) = \{P(\alpha)Q(\alpha)^{-1} : P, Q \in K[x], Q(\alpha) \neq 0\}.$$

Definicija.
Neka je L proširenje polja K. Za element $\alpha \in L$ kažemo da je **algebarski nad** K ako postoji nekonstantan polinom $P \in K[x]$ takav da je $P(\alpha) = 0$. Ako α nije algebarski nad K, kažemo da je α **transcedentan nad** K. Ako je svaki $\alpha \in L$ algebarski nad K, kažemo da je L **algebarsko proširenje** polja K.

Primijetimo kako je u prethodnoj definiciji ključno zahtijevati da je P nekonstantan polinom, jer za polinom $P = 0$ vrijedi $P(\alpha) = 0$ za svaki $\alpha \in L$. Također, polje K je algebarsko proširenje samog sebe, tj. K je algebarsko proširenje od K, jer je, za $\alpha \in K$, polinom $P = x - \alpha \in K[x]$ te $P(\alpha) = 0$.

Ako je $\alpha \in L$ algebarski nad K i M međupolje, $K \subseteq M \subseteq L$, tada je α algebarski i nad M, jer postoji polinom $P \in K[x] \subseteq M[x]$, $P \neq 0$, takav da je $P(\alpha) = 0$.

Primjer.
Realan broj $\sqrt{2}$ je algebarski nad poljem $\mathbb{Q}$, jer za polinom $P_1 = x^2 - 2 \in \mathbb{Q}[x]$ vrijedi $P_1(\sqrt{2}) = 0$. Slično, i $\sqrt[3]{5}$ je algebarski nad $\mathbb{Q}$ jer za polinom $P_2 = x^3 - 5 \in \mathbb{Q}[x]$ vrijedi $P_2(\sqrt[3]{5}) = 0$. Ali, polje realnih brojeva $\mathbb{R}$ nije algebarsko proširenje polja racionalnih brojeva, jer su npr. π i e transcedentni nad $\mathbb{Q}$.
Polje kompleksnih brojeva $\mathbb{C}$ je algebarsko proširenje polja realnih brojeva $\mathbb{R}$. Za $z = a + bi \in \mathbb{C}$, $a, b \in \mathbb{R}$, možemo uzeti polinom $P = (x-a)^2 + b^2 = x^2 - 2ax + a^2 + b^2 \in \mathbb{R}[x]$, za koji vrijedi $P(z) = P(a + bi) = 0$.

Neka je L proširenje polja K i neka je $\alpha \in L$. Definiramo preslikavanje $\Phi_\alpha : K[x] \to L$ s $\Phi_\alpha(P) = P(\alpha)$, za $P \in K[x]$. Drugim riječima, ovo preslikavanje je evaluacija polinoma u α. Kako za $P, Q \in K[x]$ vrijedi $(P+Q)(\alpha) = P(\alpha) + Q(\alpha)$ i $(P \cdot Q)(\alpha) = P(\alpha)Q(\alpha)$, preslikavanje Φ_α je homomorfizam prstena. Tada je jezgra preslikavanja Φ_α ideal u $K[x]$. Jezgra ovog preslikavanja je trivijalna ako i samo ako ne postoji nenul polinom $P \in K[x]$ takav da je $P(\alpha) = 0$, tj. ako je α transcedentan nad K. Drugim riječima, preslikavanje Φ_α je monomorfizam ako i samo ako je α transcedentan nad K.

Neka je sada $\alpha \in L$ algebarski nad K. (Ponekad se to kratko zapisuje u obliku $\alpha \in L$, α alg./K). Tada je jezgra preslikavanja Φ_α ideal u $K[x]$ koji je različit od nul-ideala, jer postoji $P \in K[x]$, $P \neq 0$, takav da je $P(\alpha) = 0$ te $P \in Ker\Phi_\alpha$. Kako je $K[x]$ domena glavnih ideala, postoji normiran polinom $\mu_\alpha \in K[x]$ takav da je $Ker\Phi_\alpha = (\mu_\alpha)$.

Podsjetimo, polinom je normiran kada mu je vodeći koeficijent jednak 1. Neka je $P \in K[x]$ takav da je $Ker\Phi_\alpha = (P)$. Kako je $(P) \neq (0)$, polinom P ima vodeći koeficijent različit od nule, te označimo vodeći koeficijent od P s a. Tada je $\mu_\alpha = a^{-1}P$.

Polinom μ_α nazivamo **minimalni polinom elementa** $\alpha \in L$. Svojstva minimalnog polinoma elementa α navodimo u idućoj propoziciji. Stupanj polinoma P ćemo označavati s $degP$.

Propozicija.
Neka je L proširenje polja K i $\alpha \in L$ algebarski nad K. Tada vrijedi

1. Za $P \in K[x]$ vrijedi $P(\alpha) = 0$ ako i samo ako μ_α dijeli P.
2. Ako je $P \in K[x]$, $P \neq 0$, takav da je $P(\alpha) = 0$, tada je $deg\mu_\alpha \leq degP$. (Minimalni polinom od α je netrivijalni polinom najmanjeg stupnja kojem je α nultočka - odatle i naziv minimalni.)
3. Polinom μ_α je ireducibilan u prstenu $K[x]$.
4. Polinom μ_α je jedinstven ireducibilan normiran polinom u $K[x]$ kome je α nultočka.

`Dokaz:`
Primijetimo da je $P(\alpha) = 0$ ako i samo ako je $P \in Ker\Phi_\alpha$, tj. ako i samo ako je

$P \in (\mu_\alpha)$. Od ranije znamo da je $P \in (\mu_\alpha)$ ako i samo ako μ_α dijeli P.
Ako je $P \in K[x]$, $P \neq 0$, takav da je $P(\alpha) = 0$, tada je $P \in (\mu_\alpha)$ te postoji $Q \in K[x]$ takav da je $P = Q \cdot \mu_\alpha$. Kako je $P \neq 0$, slijedi da je i $Q \neq 0$ pa je $deg\mu_\alpha \leq degP$.
Pretpostavimo da μ_α nije ireducibilan. Tada postoje neinvertibilni $P, Q \in K[x]$ takvi da je $\mu_\alpha = P \cdot Q$. Očito je $P \neq 0$ i $Q \neq 0$. Kako su P i Q neinvertibilni, moraju biti stupnja barem 1 pa je $degP < deg\mu_\alpha$ i $degQ < deg\mu_\alpha$. Iz $\mu_\alpha(\alpha) = 0$ slijedi $P(\alpha)Q(\alpha) = 0$ pa je ili $P(\alpha) = 0$ ili $Q(\alpha) = 0$, što nije moguće prema dijelu $2.$, jer su polinomi P i Q manjeg stupnja od polinoma μ_α.
Neka je $P \in K[x]$ ireducibilan normiran polinom kome je α nultočka. Tada je $P \in (\mu_\alpha)$ te postoji $Q \in K[x]$ takav da je $P = Q \cdot \mu_\alpha$. Kako je P ireducibilan, jedan od polinoma Q i μ_α mora biti invertibilan u $K[x]$. No, polinom μ_α je stupnja barem 1 pa nije invertibilan, jer je $K[x]^\times = K \setminus \{0\}$. Zato je Q invertibilan, tj. $Q \in K$, $Q \neq 0$. Polinom μ_α je normiran, pa je vodeći koeficijent polinoma P jednak Q. Kako je i polinom P normiran, slijedi $Q = 1$ pa je $P = \mu_\alpha$.

U idućem teoremu ćemo detaljno opisati jedan specifičan oblik proširenja polja.

Teorem.
Neka je L proširenje polja K te $\alpha \in L$ algebarski nad K. Neka je μ_α minimalni polinom od α nad K i neka je $m = deg\mu_\alpha$. Tada je

$$K(\alpha) = K[\alpha] = \{P(\alpha) : P \in K[x], degP \leq m - 1\}.$$

Preciznije, skup $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$ je baza vektorskog prostora $K(\alpha)$ nad poljem K i $[K(\alpha) : K] = m$.
Dokaz:
Označimo $K_{m-1}[\alpha] = \{P(\alpha) : P \in K[x], degP \leq m - 1\}$. Očito je $K_{m-1}[\alpha] \subseteq K[\alpha]$. Vidjeli smo da je svaki element iz $K[\alpha]$ oblika $P(\alpha)$ za neki $P \in K[x]$. Neka je sada $P \in K[x]$. Prema Teoremu o dijeljenju s ostatkom za polinome, postoje $Q, R \in K[x]$ takvi da je $P = Q \cdot \mu_\alpha + R$ te $degR < deg\mu_\alpha = m$. Odatle je $P(\alpha) = Q(\alpha) \cdot \mu_\alpha(\alpha) + R(\alpha) = R(\alpha) \in K_{m-1}[\alpha]$. Prema tome, $K[\alpha] \subseteq K_{m-1}[\alpha]$ te slijedi $K[\alpha] = K_{m-1}[\alpha]$.
Pokažimo sada da je $K[\alpha]$ polje, tada će direktno slijediti da je $K[\alpha] = K(\alpha)$. Neka je $\beta = P(\alpha) \in K[\alpha]$, $\beta \neq 0$, za $P \in K[x]$, $degP \leq m - 1$ (pokazali smo da je $K[\alpha] = K_{m-1}[\alpha]$). Kako je μ_α ireducibilan i $degP < deg\mu_\alpha$, najveća zajednička mjera polinoma P i μ_α jednaka je 1 (jer je jedini polinom koji dijeli ireducibilni polinom μ_α i stupnja je manjeg od m upravo konstantni polinom stupnja 0). Zato postoje $A, B \in K[x]$ takvi da je $A \cdot P + B \cdot \mu_\alpha = 1$. Ovaj identitet slijedi direktnom primjenom Teorema o dijeljenju s ostatkom za polinome, na isti način kao i analogna posljedica Euklidova algoritma, u kojem se koristi Teorem o dijeljenju s ostatkom, u slučaju cijelih brojeva. Sada je $A(\alpha) \cdot P(\alpha) + B(\alpha) \cdot \mu_\alpha(\alpha) = 1$, odakle je $A(\alpha) \cdot P(\alpha) = 1$ te $A(\alpha) \cdot \beta = 1$ pa je β invertibilan i $\beta^{-1} = A(\alpha)$. Prema tome, svaki nenul element u $K[\alpha]$ je invertibilan te je $K[\alpha]$ polje.
Svaki element iz $K(\alpha) = K[\alpha] = K_{m-1}[\alpha]$ je oblika $a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0 \cdot 1$, za neke $a_0, a_1, \ldots, a_{m-1} \in K$, jer je dobiven uvrštavanjem α u polinom stupnja najviše $m-1$ s koeficijentima iz K. Zato skup $\{1, \alpha, \ldots, \alpha^{m-1}\}$ razapinje vektorski

prostor $K(\alpha)$ nad K. Pokažimo da je taj skup i linearno nezavisan.
Kada bi postojali $a_0, a_1, \ldots, a_{m-1} \in K$, koji nisu svi jednaki nuli, takvi da je

$$a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} = 0,$$

tada bi za polinom $P = a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0 \in K[x]$ vrijedilo $P \neq 0$ i $P(\alpha) = 0$, što nije moguće jer je stupanj polinoma P manji od stupnja minimalnog polinoma od α. Zato je skup $\{1, \alpha, \ldots, \alpha^{m-1}\}$ linearno nezavisan pa je i baza vektorskog prostora $K(\alpha)$ nad K.

Korolar.
Neka je L proširenje polja K te $\alpha \in L$ algebarski nad K. Tada je $K(\alpha)$ konačno proširenje polja K.

Primjer.
Vidjeli smo da je $\sqrt[3]{5}$ je algebarski nad $\mathbb{Q}$ te da je $\sqrt[3]{5}$ nultočka polinoma $P = x^3 - 5$. Ovaj je polinom očito normiran. Također, prost element 5 dijeli sve koeficijente ovog polinoma izuzev vodećeg koeficijenta, a 5^2 ne dijeli slobodni koeficijent. Prema Eisensteineovu je kriteriju polinom $x^3 - 5$ ireducibilan u $\mathbb{Q}[x]$. Kako je polinom $x^3 - 5$ ireducibilan normiran i $\sqrt[3]{5}$ mu je nultočka, slijedi $\mu_{\sqrt[3]{5}} = x^3 - 5$. Prema prethodnom teoremu slijedi $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$ te je skup $\{1, \sqrt[3]{5}, (\sqrt[3]{5})^2\} = \{1, \sqrt[3]{5}, \sqrt[3]{25}\}$ baza vektorskog prostora $\mathbb{Q}(\sqrt[3]{5})$ nad $\mathbb{Q}$. Kao skup, $\mathbb{Q}(\sqrt[3]{5})$ jednak je

$$\{q_1 + q_2\sqrt[3]{5} + q_3\sqrt[3]{25} : q_1, q_2, q_3 \in \mathbb{Q}\}.$$

Teorem.
Neka je L proširenje polja K i $\alpha \in L$ transcedentan nad K. Tada se monomorfizam $\Phi_\alpha : K[x] \to L$ na jedinstven način proširuje do monomorfizma polja $K(x)$ (polja racionalnih funkcija od $K[x]$) u polje L i to proširenje je izomorfizam polja $K(x)$ na potpolja $K(\alpha)$ polja L.

Teorem.
Neka su $K \subseteq L \subseteq M$ polja. Tada je $[M : K] = [M : L] \cdot [L : K]$, pri čemu smatramo da je $\infty \cdot n = n \cdot \infty = \infty \cdot \infty = \infty$, za $n \in \mathbb{N}$. Nadalje, ako je $\{\alpha_i : i \in I\}$ baza vektorskog prostora L nad poljem K te $\{\beta_j : j \in J\}$ baza vektorskog prostora M nad poljem L, tada je $\{\alpha_i \cdot \beta_j : i \in I, j \in J\}$ baza vektorskog prostora M nad poljem K.

Ako je L proširenje polja K i $S \subseteq L$, tada s $K(S)$ označavamo najmanje potpolje od L koje sadrži K i S, tj. ako je M potpolje od L takvo da je $K \subseteq M$ i $S \subseteq M$, tada je i $K(S) \subseteq M$.

Ako je $S = \{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq L$, tada umjesto $K(S)$ pišemo $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Vrijedi $K(\alpha_1, \alpha_2, \ldots, \alpha_n) = K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})(\alpha_n)$.

Definicija.
Za polje L kažemo da je **konačno generirano proširenje** polja K ako postoji $n \in \mathbb{N}$ te $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$ takvi da je $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Primjer.
Polje kompleksnih brojeva je konačno generirano proširenje polja realnih brojeva, jer je $\mathbb{C} = \mathbb{R}(i) = \mathbb{R}(i, -i)$.

Teorem.
Proširenje L polja K je konačno ako i samo ako je to proširenje algebarsko i konačno generirano.
Dokaz:
Neka je najprije L konačno proširenje polja K. Neka je $\alpha \in L$. Kako je vektorski prostor L nad poljem K konačnodimenzionalan, skup $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ ne može biti linearno nezavisan za svaki prirodan broj n. Zato postoji prirodan broj n takav da je skup $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ linearno nezavisan, te postoje $a_0, a_1, \ldots, a_n \in K$, koji nisu svi jednaki nuli, takvi da je

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0.$$

Prema tome, za polinom $P = a_nx^n + \cdots + a_2x^2 + a_1x + a_0 \in K[x]$ vrijedi $P \neq 0$ i $P(\alpha) = 0$ pa je α algebarski nad K i L je algebarsko proširenje polja K. Nadalje, neka je $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ baza vektorskog prostora L nad K. očito je $K(\alpha_1, \alpha_2, \ldots, \alpha_m) \subseteq L$, jer je $K \cup \{\alpha_1, \alpha_2, \ldots, \alpha_m\} \subseteq L$. S druge strane, kako je $L = \{a_1\alpha_1 + a_2\alpha_2 + \cdots + a_m\alpha_m : a_1, a_2, \ldots, a_m \in K\}$ te $\{a_1\alpha_1 + a_2\alpha_2 + \cdots + a_m\alpha_m : a_1, a_2, \ldots, a_m \in K\} \subseteq K(\alpha_1, \alpha_2, \ldots, \alpha_m)$, slijedi $L = K(\alpha_1, \alpha_2, \ldots, \alpha_m)$ pa je L konačno generirano proširenje polja K.
Neka je sada L algebarsko i konačno generirano proširenje polja K. Neka su $\alpha_1, \alpha_2 \ldots, \alpha_m \in L$ takvi da je $L = K(\alpha_1, \alpha_2, \ldots, \alpha_m)$. Definiramo $K_0 = K$, $K_1 = K(\alpha_1)$ te $K_j = K(\alpha_1, \ldots, \alpha_j)$ za $j = 2, \ldots, m$. Tada je $K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_{m-1} \subseteq K_m = L$ te

$$[L : K] = [K_m : K_{m-1}] \cdot [K_{m-1} : K_{m-2}] \cdots [K_2 : K_1] \cdot [K_1 : K_0].$$

Primijetimo da za svaki $j \in \{1, 2, \ldots, m\}$ vrijedi $K_j = K_{j-1}(\alpha_j)$, a kako je α_j algebarski nad K i $K \subseteq K_{j-1}$, slijedi da je α_j algebarski i nad K_{j-1} pa je K_j konačno proširenje od K_{j-1}, tj. $[K_j : K_{j-1}] < \infty$. Prema tome, i $[L : K] < \infty$ te je L konačno proširenje polja K.

Primjer.
Kako $\mathbb{R}$ nije algebarsko proširenje od $\mathbb{Q}$, $\mathbb{R}$ nije niti konačno proširenje od $\mathbb{Q}$.

Općenito proširenje polja ne mora biti algebarsko, ali elementi koji su algebarski u proširenju čine posebno zanimljivu strukturu.

Teorem.
Neka je L proširenje polja K. Tada je skup M svih elemenata iz L koji su algebarski nad K polje. Drugim riječima, skup algebarskih elemenata u proširenju čini međupolje.
Dokaz:
Neka su $x, y \in M$. Treba dokazati da su tada i $x + y, x - y, xy \in M$ te $x^{-1}, y^{-1} \in M$, za $x \neq 0$, $y \neq 0$. Primijetimo da je $K \subseteq K(x) \subseteq K(x, y)$, te

$$[K(x, y) : K] = [K(x, y) : K(x)] \cdot [K(x) : K].$$

Na isti način kao u dokazu prethodnog teorema možemo zaključiti da je $[K(x, y) : K(x)] < \infty$ i $[K(x) : K] < \infty$. Iz prethodne jednakosti slijedi da je i $K(x, y)$

konačno proširenje polja K. Prema prethodnom je teoremu svako konačno proširenje ujedno i algebarsko, pa je $K(x, y)$ algebarsko proširenje polja K te je svaki element iz $K(x, y)$ algebarski nad K, tj. $K(x, y) \subseteq M$. Prema tome, dobivamo $x + y, x - y, xy \in M$ te $x^{-1}, y^{-1} \in M$ (za $x \neq 0$, $y \neq 0$) te je M polje, $K \subseteq M \subseteq L$.

Polja cijepanja

Definicija.
Neka je K polje i $P \in K[x]$ nekonstantni polinom. Kažemo da se polinom P **cijepa nad proširenjem** L **polja** K ako postoje $a \in K$ i $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$ takvi da je

$$P = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Ako je pri tome $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, kažemo da je L **polje cijepanja polinoma** P **nad poljem** K.

Primijetimo da je a u prethodnoj definiciji samo vodeći koeficijent polinoma P. Polinom se cijepa nad proširenjem ukoliko u tom proširenju ima onoliko nultočaka koliki mu je stupanj, brojeći njihovu kratnost (elementi $\alpha_1, \alpha_2, \ldots, \alpha_n$ nisu nužno međusobno različiti).

Primjer.
Polje $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2}, -\sqrt{2})$ je polje cijepanja polinoma $x^2 - 2$ nad $\mathbb{Q}$.
Polje kompleksnih brojeva $\mathbb{C}$ je polje cijepanja polinoma $x^2 + 1$ nad poljem realnih brojeva $\mathbb{R}$, jer je $\mathbb{C} = \mathbb{R}(i)$. Isti polinom možemo promatrati i kao element iz $\mathbb{Q}[x]$, odnosno kao polinom nad poljem racionalnih brojeva. U tom je slučaju polje cijepanja $\mathbb{Q}(i)$.
Polje $\mathbb{Q}(\sqrt[3]{2})$ je potpolje od $\mathbb{R}$ i nije polje cijepanja polinoma $x^3 - 2$ nad poljem racionalnih brojeva $\mathbb{Q}$. Jedina realna nultočka ovog polinoma je $\sqrt[3]{2}$ pa polje $\mathbb{Q}(\sqrt[3]{2})$ ne sadrži preostale dvije nultočke polinoma $x^3 - 2$, koji se zato ne cijepa nad tim poljem.

Teorem.
Neka je K polje i $P \in K[x]$ nekonstantni polinom. Tada postoji polje cijepanja polinoma P nad poljem K.
Dokaz:
Neka je $a \in K$ vodeći koeficijent polinoma P i neka je $P_1 \in K[x]$ polinom za koji vrijedi $P = aP_1$. Tada je polinom P_1 normiran. Najprije ćemo pokazati da postoji proširenje M polja K nad kojim se polinom P_1 cijepa, tada će se nad istim proširenjem cijepati i polinom P.
Ovu tvrdnju ćemo pokazati indukcijom po stupnju polinoma P. Ako je P polinom stupnja 1, tada je $P_1 = x - \alpha_1$, za neki $\alpha_1 \in K$, pa tvrdnja trivijalno vrijedi jer je $P = a(x - \alpha_1)$ te se P i P_1 cijepaju nad poljem K.
Pretpostavimo da za polinom stupnja n postoji proširenje polja M nad kojim se taj polinom cijepa te neka je stupanj od P jednak $n + 1$.
U prethodnom poglavlju smo vidjeli da postoji proširenje K_1 polja K i $\alpha_1 \in K_1$ tako da je $P_1(\alpha_1) = 0$. Tada je $P_1 = (x - \alpha_1)Q$, pri čemu je $Q \in K_1[x]$ normiran polinom stupnja n. Po pretpostavci indukcije, postoji proširenje M polja K_1 i $\alpha_2, \ldots, \alpha_{n+1} \in M$ takvi da je

$$Q = (x - \alpha_2) \cdots (x - \alpha_{n+1}).$$

Kako je M proširenje od K_1, slijedi $\alpha_1 \in M$ pa se P cijepa nad poljem M, jer iz $P = aP_1 = a(x - \alpha_1)Q$ slijedi

$$P = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_{n+1}).$$

Sada je potpolje $L(\alpha_1, \alpha_2, \ldots, \alpha_{n+1})$ od M polje cijepanja polinoma P nad poljem K.

Napomena: Neka je $P \in K[x]$ nekonstantan polinom te neka su L_1 i L_2 proširenja polja K koja su polja cijepanja polinoma P nad poljem K. Tada postoji izomorfizam polja $\varphi : L_1 \to L_2$ takav da je $\varphi(a) = a$, za sve $a \in K$.

Algebarski zatvarač

Definicija.
Kažemo da je polje M **algebarski zatvoreno** ako svaki nekonstantni polinom u $M[x]$ ima nultočku u M.

Neka je $P \in M[x]$ nekonstantni polinom te neka je polja M algebarski zatvoreno. Tada postoji $\alpha \in M$ takav da je $P(\alpha) = 0$ te postoji i polinom $Q \in M[x]$ takav da je $P = (x - \alpha)Q$. Ukoliko je P polinom stupnja većeg od 1, tada i polinom Q ima nultočku u polju M. Nastavimo li na isti način, možemo zaključiti da nekonstantni polinom nad algebarski zatvorenim poljem ima onoliko nultočaka koliki mu je stupanj, računajući njihovu kratnost. Prema tome, nekonstantni polinom $P \in M[x]$, pri čemu je polje M algebarski zatvoreno, se cijepa nad M.
Primjer.
Polje kompleksnih brojeva je algebarski zatvoreno, do polja racionalnih i realnih brojeva nisu.

Definicija.
Kažemo da je proširenje L polja K **algebarski zatvarač polja** K ako je L algebarsko proširenje polja K i polje L je algebarski zatvoreno.

Primjer.
Polje kompleksnih brojeva je algebarski zatvarač polja realnih brojeva.

Teorem (Steinitz).
Svako polja K ima algebarski zatvarač. Ako su L_1 i L_2 algebarski zatvarači polja K, tada postoji izomorfizam polja $\psi : L_1 \to L_2$ takav da je $\psi(x) = x$, za sve $x \in K$.

Propozicija.
Polje K je algebarski zatvoreno ako i samo ako ne postoji algebarsko proširenje L polja K koje je različito od K.
`Dokaz:`
Neka je najprije K algebarski zatvoreno polje. Neka je L algebarsko proširenje od K te neka je $\alpha \in L$. Tada je α algebarski nad K pa postoji nekonstantan polinom $P \in K[x]$ takav da je $P(\alpha) = 0$. Kako je polje K algebarski zatvoreno, polinom P se cijepa nad K te postoje $a, a_1, \ldots, a_n \in K$ takvi da je $P = a(x-a_1)\cdots(x-a_n)$. Prema tome, $\alpha \in \{a_1, \ldots, a_n\}$ te je $\alpha \in K$ i $K = L$.
Obratno, pretpostavimo da ne postoji algebarsko proširenje polja K koje je različito od K. Neka je $P \in K[x]$ nekonstantni polinom. Znamo da postoji proširenje L polja K u kojem polinom P ima nultočku, tj. za neki $\alpha \in L$ je $P(\alpha) = 0$. Prema tome, α je algebarski nad K pa je proširenje $K(\alpha)$ konačno proširenje polja K, a svako konačno proširenje je i algebarsko. Dakle, $K(\alpha)$ je algebarsko proširenje polja K pa je $K(\alpha) = K$ te je i $\alpha \in K$. Pokazali smo da nekonstantni polinom $P \in K[x]$ ima nultočku u K pa je polje K algebarski zatvoreno.

Konačna polja

U ovoj ćemo se temi najprije upoznati s pojmom *karakteristike polja*. Neka je K polje te označimo s 0_K nulu u polju K i s 1_K jedinicu u polju K. Za prirodan broj n i $x \in K$ definiramo

$$n \cdot x = \underbrace{x + x + \cdots + x}_{n \text{ puta}}.$$

Sada možemo definirati preslikavanje $\varphi : \mathbb{Z} \to K$:

- $\varphi(0) = 0_K$,
- $\varphi(n) = n \cdot 1_K$, za prirodan broj n,
- $\varphi(n) = -\varphi(-n)$, za negativan cijeli broj n.

Primijetimo da je $\varphi(1) = 1_K$. Također, za cijele brojeve m, n očito vrijedi $\varphi(m + n) = (m+n) \cdot 1_K = m \cdot 1_K + n \cdot 1_K$ i $\varphi(m \cdot n) = (m \cdot n) \cdot 1_K = (m \cdot 1_K) \cdot (n \cdot 1_K)$ pa je φ homomorfizam prstena. Znamo da je jezgra tog homomorfizma ideal u $\mathbb{Z}$. Označimo sliku homomorfizma φ s $\varphi(\mathbb{Z})$.

Razlikujemo dva slučaja:

1. $Ker\varphi = \{0\}$, tj. φ je monomorfizam. Tada je, prema Prvom teoremu o izomorfizmu za prstene, $\mathbb{Z} \cong \varphi(\mathbb{Z})$ te $\mathbb{Z}$ možemo identificirati s potprstenom $\varphi(\mathbb{Z})$ od K, a $\mathbb{Q}$ možemo identificirati s potpoljem od K. Tada kažemo da je K **polje karakteristike** 0, a $\mathbb{Q}$ je najmanje potpolje od K i nazivamo ga **prosto potpolje od** K.
   Kako je jezgra preslikavanja φ trivijalna, znači da za svaki cijeli broj n, $n \neq 0$, vrijedi $n \cdot 1_K \neq 0$. Posljedično, za svaki $x \in K$, $x \neq 0_K$, i cijeli broj n, $n \neq 0$, vrijedi $n \cdot x = n \cdot (x \cdot 1_K) = x \cdot (n \cdot 1_K) \neq 0$.

2. $Ker\varphi \neq \{0\}$, tj. φ nije monomorfizam. Kako je $\mathbb{Z}$ domena glavnih ideala i $Ker\varphi \neq (0)$, postoji prirodan broj p takav da je $Ker\varphi = (p)$. Kako je $\varphi(1) = 1_K \neq 0_K$, slijedi $1 \notin Ker\varphi$ pa je $Ker\varphi \neq \mathbb{Z}$. Zato je $p \neq 1$, tj. $p \geq 2$.
   Prema Prvom teoremu o izomorfizmu za prstene sada slijedi

   $$\mathbb{Z}/(p) \cong \varphi(\mathbb{Z}).$$

   Kako je K polje, a $\varphi(\mathbb{Z})$ potprsten s jedinicom od K, jer je $1_K = \varphi(1) in \varphi(\mathbb{Z})$, slijedi da je $\varphi(\mathbb{Z})$ integralna domena. Zato i kvocijentni prsten $\mathbb{Z}/(p)$ mora biti integralna domena. Vidjeli smo da tada ideal (p) mora biti prost, pa je i p prost element, tj. p je prost broj. Primijetimo da je ideal (p) ujedno i maksimalan te je kvocijentni prsten $\mathbb{Z}/(p)$ polje. Prisjetimo se kako je $\mathbb{Z}/(p) \cong \mathbb{Z}_p$. Tada kažemo da je K **polje karakteristike** p, a $\mathbb{Z}_p$ je najmanje potpolje od K i nazivamo ga **prosto potpolje od** K.
   Sada za svaki $x \in K$ vrijedi $p \cdot x = x \cdot (p \cdot 1_K) = 0$. Također, za $x \in K$ i prirodan broj n koji je djeljiv s p vrijedi $n \cdot x = 0$.

Karakteristiku polja K ponekad označavamo s $charK$. Karakteristika polja je ili 0 ili prost broj.

Primjer.
Polja racionalnih, realnih i kompleksnih brojeva su polja karakteristike 0. Zaista, za svaki kompleksan broj z, $z \neq 0$, i prirodan broj n vrijedi $n \cdot z \neq 0$. Polje racionalnih funkcija s koeficijentima iz polja $\mathbb{Z}_p$, $\mathbb{Z}_p(x)$, je beskonačno polje proste karakteristike. Podsjetimo,

$$\mathbb{Z}_p(x) = \left\{ \frac{P}{Q} : P, Q \in \mathbb{Z}_p[x], Q \neq 0 \right\}.$$

Kako ovo polje sadrži sve polinome iz $\mathbb{Z}_p[x]$, ne može biti konačno. S druge strane, kako ovo polje sadrži polje $\mathbb{Z}_p$, i ono mora biti karakteristike p, tj. $char\mathbb{Z}_p(x) = p$.

Ako je K konačno polje, tada ne može postojati injekcija sa $\mathbb{Z}$ u K, pa je svako konačno polje proste karakteristike.

Neka je K konačno polje i neka je karakteristika polja K jednaka p. Sada znamo da je p prost broj te da K sadrži polje Z_p. Kako je K konačno polje, tada je K konačnodimenzionalan vektorski prostor nad poljem $\mathbb{Z}_p$. Označimo s n stupanj proširenja $[K : \mathbb{Z}_p]$ te neka je $\{e_1, e_2, \ldots, e_n\}$ baza vektorskog prostora K nad poljem $\mathbb{Z}_p$. Tada je, kao skup,

$$K = \{a_1e_1 + a_2e_2 + \cdots + a_ne_n : a_i \in \mathbb{Z}_p\},$$

jer vektorski prostor čine sve linearne kombinacije vektora baze s koeficijentima iz polja. Kako polje $\mathbb{Z}_p$ ima p elemenata, svaki od koeficijenata (skalara) a_i možemo odabrati na p načina pa prema pravilu produkta slijedi $|K| = p^n$.

Korolar.
Ako je K konačno polje, tada je $|K| = p^n$, za neki prost broj p i prirodan broj n. Također, $charK = p$.

Primjer.
Ne postoji polje s 15 elemenata niti polje sa 100 elemenata, jer niti 15 niti 100 nisu potencije prostih brojeva (imaju više od jednog prostog djelitelja).

Definicija.
Neka je K polje i $P \in K[x]$, $P = \sum_{i=0}^{n} a_i x^i$, $P \neq 0$. Derivaciju $P' \in K[x]$ definiramo kao

$$P' = \sum_{i=1}^{n} i \cdot a_i x^{i-1}.$$

Ako je $P = 0$, stavljamo $P' = 0$.

Za prirodan broj i smo $i \cdot a_i$ definirali na početku ovog potpoglavlja. Za polinome $P, Q \in K[x]$ se može direktno vidjeti da vrijedi $(P \cdot Q)' = P' \cdot Q + P \cdot Q'$.

Propozicija.
Neka je $a \in K$. Ako $(x - a)^2$ dijeli polinom $P \in K[x]$, tada je $P(a) = P'(a) = 0$. Drugim riječima, pomoću derivacije polinoma možemo ispitati kratnost njegove nultočke.

`Dokaz:`
Kako $(x-a)^2$ dijeli P, postoji polinom $Q \in K[x]$ takav da je $P = (x-a)^2 Q$. Očito je $P(a) = 0$. Iz $P' = ((x-a)^2 Q)' = 2(x-a)Q + (x-a)^2 Q'$ slijedi i $P'(a) = 0$.

Propozicija.
Neka je p prost broj i K polje karakteristike p. Tada je **Frobeniusovo preslikavanje** $\varphi : K \to K$ definirano s $\varphi(x) = x^p$, $x \in K$, monomorfizam polja K u samog sebe. Ako je K konačno polje, tada je φ **automorfizam od** K, tj. izomorfizam polja K u samog sebe.
`Dokaz:`
Neka su $x, y \in K$. Direktno iz komutativnosti množenja u polju slijedi

$$\varphi(xy) = (xy)^p = x^p y^p = \varphi(x)\varphi(y).$$

Također, primjenom distributivnosti i komutativnosti množenja u polju dobivamo

$$\varphi(x+y) = (x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}. \tag{1}$$

Prethodna je jednakost varijanta Binomnog teorema za polja. Zbog distributivnosti i komutativnosti množenja je u svaki sumand koji se dobiva u produktu

$$(x+y)^p = \underbrace{(x+y)(x+y)\cdots(x+y)}_{p \text{ puta}}$$

oblika $x^i y^{p-i}$, za neki $i \in \{0, 1, \ldots, p\}$. Broj pojavljivanja izraza $x^i y^{p-i}$ jednak je broju načina da od p faktora odaberemo njih i koji će u umnošku sudjelovati s x, a to je $\binom{p}{i}$.
Neka je $i \in \{1, 2, \ldots, p-1\}$. Tada je $\binom{p}{i}$ prirodan broj veći od 1. Iz jednakosti

$$\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{i!}$$

slijedi

$$i!\binom{p}{i} = p(p-1)\cdots(p-i+1).$$

Kako je desna strana prethodne jednakosti djeljiva prostim brojem p, i neki od faktora s lijeve strane mora biti djeljiv s p, jer ako prost broj dijeli produkt tada dijeli i neki od faktora. Kako je $i < p$, slijedi da je $\binom{p}{i}$ djeljivo s p. Karakteristika polja K jednaka je p pa za sve $x, y \in K$ te $i \in \{1, 2, \ldots, p-1\}$ vrijedi

$$\binom{p}{i} x^i y^{p-i} = 0.$$

Za $i \in \{0, p\}$ je $\binom{p}{i} = 1$ pa iz (1) dobivamo

$$\varphi(x+y) = x^p + y^p = \varphi(x) + \varphi(y).$$

Pokazali smo da je φ homomorfizam polja. Označimo li jedinicu u polju K s 1_K, dobivamo $\varphi(1_K) = 1_K^p = 1_K$ pa je $\varphi \neq 0$. Kako je φ netrivijalni homomorfizam polja, φ je i monomorfizam. Ako je K konačno polje, tada je φ injekcija s konačnog skupa u samog sebe pa je φ i bijekcija, tj. izomorfizam.

Dio prethodnog teorema u kojem se navodi da za x, y iz polja K karakteristike p vrijedi $(x+y)^p = x^p + y^p$ se često u literaturi naziva ,,Brucoški san" (,,The Freshman's Dream"). Navodno na pojedinim studijima neki brucoši smatraju da ovaj identitet vrijedi općenito, no za $p > 1$ je p-ta potencija sume jednaka sumi p-tih potencija jedino u polju karakteristike p.

Do sad smo vidjeli da je svako konačno polje proste karakteristike te da je broj elemenata konačnog polja potencija prostog broja. Idući teorem daje potpunu karakterizaciju konačnih polja, te pokazuje da za svaki odabir prostog broja p i prirodnog broja n postoji polja s p^n elemenata.

Teorem.
Za svaki prost broj p i prirodan broj n postoji do na izomorfizam jedinstveno polje s p^n elemenata. To je polje cijepanja polinoma $x^{p^n} - x \in \mathbb{Z}_p[x]$ nad poljem $\mathbb{Z}_p$.
Dokaz:
Pojasnit ćemo samo pojavljivanje polinoma $x^{p^n} - x$. Ako je K polje s p^n elemenata, tada je broj elemenata u $K^\times$ jednak $p^n - 1$ i $K^\times$ je konačna grupa. Kako, prema Lagrangeovu teoremu, red elementa dijeli red grupe, za svaki $a \in K$, $a \neq 0$, vrijedi $a^{p^n-1} = 1$, odnosno $a^{p^n-1} - 1 = 0$. Drugim riječima, svaki nenul element polja K je nultočka polinoma $x^{p^n-1} - 1$. Množenjem ovog polinoma s x dobivamo polinom $x^{p^n} - x$ kojem su tada nultočke i 0 i svi nenul elementi iz K, odnosno nultočke polinoma $x^{p^n} - x$ su svi elementi polja K.

Galoisova grupa proširenja

Neka je K polje. Podsjetimo, *automorfizam polja* K je izomorfizam polja K na samog sebe. Kada kažemo izomorfizam polja, smatramo da se radi o homomorfizmu prstena koji je i bijekcija. Skup svih automorfizama polja K označavamo s $Aut(K)$.

Propozicija.
$Aut(K)$ je grupa obzirom na kompoziciju, podgrupa grupe permutacija skupa K.
Dokaz:
Kako je identiteta automorfizam polja K, slijedi $Aut(K)qneq\emptyset$. Neka se $\sigma_1, \sigma_2 \in Aut(K)$. Kako su σ_1 i σ_2 bijekcije, također su i elementi grupe permutacija skupa K. Osim toga, i σ_2^{-1} je element grupe permutacija skupa K. Neka su $x, y \in K$. Kako je σ_2 bijekcija, postoje $x', y' \in K$ takvi da je $\sigma_2(x') = x$ i $\sigma_2(y') = y$. Tada je i $\sigma_2^{-1}(x) = x'$ i $\sigma_2^{-1}(y) = y'$. Sada je

$$\sigma_2^{-1}(x+y) = \sigma_2^{-1}(\sigma_2(x') + \sigma_2(y')) = \sigma_2^{-1}(\sigma_2(x'+y')) = x'+y' = \sigma_2^{-1}(x) + \sigma_2^{-1}(y),$$
$$\sigma_2^{-1}(xy) = \sigma_2^{-1}(\sigma_2(x')\sigma_2(y')) = \sigma_2^{-1}(\sigma_2(x'y')) = x'y' = \sigma_2^{-1}(x)\sigma_2^{-1}(y)$$

pa je σ_2^{-1} homomorfizam prstena te $\sigma_2^{-1} \in Aut(K)$. Kako je kompozicija homomorfizama također homomorfizam te je i kompozicija bijekcija također bijekcija, slijedi $\sigma_1\sigma_2^{-1} \in Aut(K)$ pa je $Aut(K)$ podgrupa grupe permutacija skupa K.

Definicija.
Neka je L proširenje polja K. Automorfizam $\sigma \in Aut(L)$ za koji vrijedi $\sigma(x) = x$, za sve $x \in K$, nazivamo K-**automorfizam polja** L. Skup svih K-automorfizama polja L označavamo s $Aut_K(L)$.

Propozicija.
$Aut_K(L)$ je podgrupa grupe $Aut(L)$.
Dokaz:
Očito je $Aut_K(L) \subseteq Aut(L)$ te je identiteta element iz $Aut_K(L)$ pa je $Aut_K(L) \neq \emptyset$. Neka su $\sigma_1, \sigma_2 \in Aut_K(L)$. Iz $\sigma_2(x) = x$, za $x \in K$, slijedi $\sigma_2^{-1}(x) = x$, za $x \in K$, pa je i $\sigma_2^{-1} \in Aut_K(L)$. Iz definicije kompozicije funkcije slijedi $\sigma_1\sigma_2^{-1} \in Aut_K(L)$ pa je $Aut_K(L) \leq Aut(L)$.

Definicija.
Grupu $Aut_K(L)$ nazivamo **Galoisova grupa proširenja** L **polja** K. Galoisova grupa se još označava i s $Gal(L, K)$ te $Gal(L/K)$. (Evariste Galois - čita se Galoa, Galoaova grupa).

Primjer.
Pogledajmo slučaj $L = \mathbb{C}$ i $K = \mathbb{R}$. Očito je $id \in Aut_{\mathbb{R}}(\mathbb{C})$. Označimo funkciju kompleksnog konjugiranja sa σ: $\sigma(z) = \overline{z}$. Iz osnovnih svojstava kompleksnog konjugiranja slijedi da je σ automorfizam polja $\mathbb{C}$, koji je identiteta na $\mathbb{R}$. Prema tome, $\{id, \sigma\} \subseteq Aut_{\mathbb{R}}(\mathbb{C})$. Nešto kasnije ćemo pokazati da vrijedi i jednakost.

Definicija.
Neka je G podgrupa grupe $Aut(L)$. Definiramo

$$L^G = \{x \in L : \sigma(x) = x, \forall \sigma \in G\}.$$

Dakle, skup L^G je skup svih elemenata iz polja L na kojem svi elementi grupe G djeluju kao identiteta, odnosno L^G je skup elemenata iz L koji su zajedničke fiksne točke svih elemenata iz G.

Propozicija.
L^G je potpolje polja L.
Dokaz:
Očito je $L^G \subseteq L$ te $1 \in L^G$ jer za svaki $\sigma \in Aut(L)$ vrijedi $\sigma(1) = 1$. Neka su $x, y \in L^G$. Tada je $\sigma(x) = x$ i $\sigma(y) = y$ za sve $\sigma \in L^G$. Također je i $\sigma(x - y) = \sigma(x) - \sigma(y) = x - y$, $\sigma(xy) = \sigma(xy) = \sigma(x)\sigma(y)$ te (za $x \neq 0$) $\sigma(x^{-1}) = \sigma(x)^{-1} = x^{-1}$ pa su $x - y, xy, x^{-1} \in L^G, x \neq 0$, te je L^G polje.

Neka je L proširenje polja K te neka je $G \subseteq Aut_K(L)$. Vidjeli smo da je $Aut_K(L) \subseteq Aut(L)$ Za svaki $\sigma \in G$ vrijedi $\sigma(x) = x, \forall x \in K$, pa za svaki $x \in K$ vrijedi $\sigma(x) = x, \forall \sigma \in G$, odakle slijedi i $K \subseteq L^G$. Dakle, ako je G podgrupa Galoisova grupe proširenja L polja K, tada je L^G međupolje, $K \subseteq L^G \subseteq L$.

S druge strane, ako je M međupolje, $K \subseteq M \subseteq L$, tada je $Aut_M(L) \leq Aut_K(L)$, jer je element σ iz $Aut_M(L)$ identiteta na M, pa je identiteta i na K, tj. $\sigma \in Aut_K(L)$.

Teorem.
Neka je L polje i G konačna podgrupa od $Aut(L)$. Tada je $[L : L^G] = |G|$. Posebno, L je konačno proširenje polja L^G.

Korolar.
Neka je L konačno proširenje polja K i neka je G konačna podgrupa Galoisove grupe $Aut_K(L)$. Tada je

$$[L^G : K] = \frac{[L : K]}{|G|}.$$

Dokaz:
Kako je L^G međupolje, tj. $K \subseteq L^G \subseteq L$, vrijedi

$$[L : K] = [L : L^G] \cdot [L^G : K] = |G| \cdot [L^G : K].$$

Napomena.
Neka je L proširenje polja K. Do sad smo vidjeli iduće: svakom međupolju M, $K \subseteq M \subseteq L$, možemo pridružiti odgovarajući Galoisovu grupu $Aut_M(L)$, koja je podgrupa Galoisove grupe $Aut_K(L)$. Obratno, svakoj podgrupi G Galoisove grupe $Aut_K(L)$ možemo pridružiti međupolje L^G. U nastavku ćemo detaljnije proučiti odnos između međupolja i podgrupa Galoisove grupe te odnos između navedenih pridruživanja. Zasad znamo iduće: možemo krenuti od međupolja M, pridružiti mu podgrupu $Aut_M(L)$ od $Aut_K(L)$ te zatim toj podgrupi pridružiti međupolje $L^{Aut_M(L)}$, za koje znamo da vrijedi $M \subseteq L^{Aut_M(L)}$.

Definicija.
Neka je K polje, $P \in K[x]$ nekonstantni polinom te L polje cijepanja polinoma P nad poljem K. Kažemo da je **polinom** P **separabilan** ako su sve nultočke od P u L jednostruke, tj. ako je

$$P = a(x - a_1)(x - a_2) \cdots (x - a_n), a \in K, a_1, \ldots, a_n \in L, a_i \neq a_j \text{ za } i \neq j.$$

Ranije smo vidjeli da se kratnost nultočaka može okarakterizirati pomoću derivacije polinoma:

Propozicija.
Nekonstantni polinom $P \in K[x]$ je separabilan ako i samo ako ne postoji polinom stupnja barem 1 koji dijeli i P i P'.

U slučaju ireducibilnih polinoma se prethodni kriterij može i dodatno pojednostavniti:

Propozicija.
Ireducibilan polinom $P \in K[x]$ je separabilan ako i samo ako je $P' \neq 0$.

Dokaz:
Možemo pretpostaviti da je polinom P normiran, jer vodeći koeficijent ne utječe na kratnost nultočke. Kako je P ireducibilan, jedini nekonstantni polinom koji dijeli P je oblika cP, za $c \in K$, $c \neq 0$. Ako je $P' = 0$, tada P dijeli P i P dijeli P' pa prema prethodnoj propoziciji polinom P nije separabilan. Time smo pokazali da ako iz separabilnosti polinoma P slijedi $P' \neq 0$.
Obratno, ako je $P' \neq 0$, tada polinom oblika cP, $c \neq 0$, ne dijeli P' jer je P većeg stupnja od polinoma P', pa ne postoji polinom stupnja barem 1 koji dijeli i P i P'. Prema prethodnoj propoziciji, P je separabilan.

Definicija.
Neka je L proširenje polja K. Kažemo da je element $\alpha \in L$ **separabilan nad** K ako je α 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.

Primijetimo da separabilno proširenje mora biti i algebarsko. Prema tome, proširenje koje nije algebarsko nije niti separabilno. Prema prethodnoj definiciji, separabilnost elementa ovisi o separabilnosti njegova minimalnog polinoma, koji je ireducibilan i normiran.

Napomena.
Ako je K polje karakteristike 0 i $P = \sum_{i=0}^{n} a_i x^i \in K[x]$ polinom stupnja n, uz $n \geq 1$, tada je $P' = \sum_{i=1}^{n} i \cdot a_i x^{i-1}$ polinom stupnja $n-1$, jer je $n \cdot a_n \neq 0$. Prema tome, nad poljem karakteristike 0 jedino konstantni polinomi (stupnja 0) imaju derivaciju jednaku nuli.
Ako je K polje karakteristike p, tada je $P = x^p \in K[x]$ vrijedi $P' = px^{p-1} = 0$, iako je P polinom pozitivnog stupnja.

Korolar.
Neka je K polje karakteristike 0. Tada je svako algebarsko proširenje polja K separabilno.

Dokaz:
Neka je $P \in K[x]$ ireducibilan nekonstantan polinom. Nad poljem karakteristike 0 vrijedi $deg P' = deg P - 1$ te je $P' \neq 0$. Prema prethodnoj propoziciji je polinom P separabilan, dakle svaki ireducibilan nekonstantan polinom u $K[x]$ je separabilan. Posebno, minimalni polinom svakog elementa iz algebarskog proširenja polja K je separabilan pa je i algebarsko proširenje polja K separabilno.

Korolar.
Neka je K konačno polje. Tada je svako algebarsko proširenje polja K separabilno.
Dokaz:
Neka je L algebarsko proširenje konačnog polja K te neka je $\alpha \in L$. Element α je algebarski nad K pa je $K(\alpha)$ konačno proširenje konačnog polja K. Prema tome, i polja $K(\alpha)$ je konačno i broj elemenata ovog polja je jednak p^n za neki prost broj p i prirodan broj n. Također, p je ujedno i karakteristika tog polja. U prethodnom poglavlju smo vidjeli kako je svaki element takvog polja nultočka polinoma $x^{p^n} - x$, pa je i α nultočka ovog polinoma. Zato minimalni polinom od α dijeli polinom $x^{p^n} - x$. Kako je derivacija ovog polinoma jednaka -1 (primijetimo da smo nad poljem karakteristike p pa vrijedi $(x^{p^n})' = p^n x^{p^n - 1} = 0$), sve nultočke polinoma $x^{p^n} - x$ su međusobno različite pa su mmeđusobno različite i sve nultočke polinoma svakog polinoma koji ga dijeli. Slijedi da su sve nultočke minimalnog polinoma od α međusobno različite te je ovaj polinom separabilan. Zato je i element α separabilan te je L separabilno proširenje polja K.

Korolar.
Jedino beskonačna polja proste karakteristike mogu imati neseparabilna algebarska proširenja.

U idućem rezultatu ćemo vidjeti kako se svojstvo separabilnosti prenosi na međupolja.

Propozicija.
Neka je L separabilno proširenje polja K i neka je M međupolje, $K \subseteq M \subseteq L$. Tada je L separabilno proširenje polja M i M separabilno proširenje polja K.

Sada ćemo opisati Galoisovg grupu posebne klase proširenja polja. U tome će nam trebati pomoćna lema:
Lema.
Neka je K polje te $P \in K[x]$ ireducibilan polinom. Neka su L_1 i L_2 proširenja polja K te $\alpha_1 \in L_1$ i $\alpha_2 \in L_2$ takvi da je $P(\alpha_1) = P(\alpha_2) = 0$, $L_1 = K(\alpha_1)$, $L_2 = K(\alpha_2)$. Tada postoji izomorfizam $\varphi : L_1 \to L_2$ takav da je $\varphi(\alpha_1) = \alpha_2$ i $\varphi(a) = a$, za sve $a \in K$.

Propozicija.
Neka je L algebarsko proširenje polja K tako da je $L = K(\alpha)$, za neki $\alpha \in L$. Tada je $|Aut_K(L)| \leq [L : K]$. Nadalje, $|Aut_K(L)| = [L : K]$ ako i samo ako je minimalni polinom $\mu_\alpha \in K[x]$ elementa α separabilan i L je polje cijepanja tog polinoma nad poljem K.
Dokaz:
Neka je stupanj polinoma μ_α jednak n te neka je $\mu_\alpha = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n, a_1, \ldots, a_n \in K$. Ranije smo pokazali da je $[L : K] = n$ te da je $\{1, \alpha, \ldots, \alpha^{n-1}\}$ baza vektorskog prostora L nad K. Prema tome, svaki element iz L je oblika $b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$, za neke $b_0, b_1, \ldots, b_{n-1} \in K$.

Neka je $\varphi \in Aut_K(L)$. Tada je

$$\varphi(b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}) = \varphi(b_0) + \varphi(b_1)\varphi(\alpha) + \cdots + \varphi(b_{n-1})\varphi(\alpha)^{n-1} = b_0 + b_1\varphi(\alpha) + \cdots + b_{n-1}\varphi(\alpha)^{n-1}$$

(primijetimo da je $\varphi(b_i) = b_i$ jer elementi iz $Aut_K(L)$ djeluje kao identiteta na K) pa je element iz Galoisove grupe $Aut_K(L)$ potpuno određen djelovanjem na α. Kako je $\mu_\alpha(\alpha) = 0$, slijedi $\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n = 0$. Zato je $\varphi(\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n) = 0$, odnosno

$$\varphi(\alpha)^n + a_1\varphi(\alpha)^{n-1} + \ldots + a_{n-1}\varphi(\alpha) + a_n = 0,$$

tj. $\mu_\alpha(\varphi(\alpha)) = 0$.
Dakle, svaki element $\varphi \in Aut_K(L)$ je potpuno određen s $\varphi(\alpha)$, a $\varphi(\alpha)$ je nultočka polinoma μ_α. Prema tome, Galoisova grupa $Aut_K(L)$ može imati najviše onoliko elemenata koliko polinom μ_α ima međusobno različitih nultočaka u polju L, što je manje ili jednako stupnju tog polinoma $n = [L : K]$. Slijedi $|Aut_K(L)| \leq [L : K]$.
Nadalje, neka je $\alpha' \in L$ proizvoljna nultočka polinoma μ_α u polju L. Kako je $L = K(\alpha)$ i $\alpha' \in L$ slijedi $K(\alpha') \subseteq K(\alpha)$. Kako je $\mu_\alpha(\alpha') = 0$, a polinom μ_α je ireducibilan i normiran, slijedi $\mu_\alpha = \mu_{\alpha'}$ (drugim riječima, polinom μ_α je minimalni polinom svake svoje nultočke u L). No, zato je i $[K(\alpha') : K] = [K(\alpha) : K]$ te je $L = K(\alpha') = K(\alpha)$. Prema prethodnoj lemi, uz $L_1 = L_2 = L$, postoji $\varphi \in Aut_K(L)$ takav da je $\varphi(\alpha) = \alpha'$. Time smo pokazali da za svaku nultočku α' od μ_α u L postoji $\varphi \in Aut_K(L)$ takav da je $\varphi(\alpha) = \alpha'$, odnosno broj elemenata Galoisove grupe $Aut_K(L)$ je jednak broju međusobno različiti nultočaka polinoma μ_α u polju L. Posebno, broj elemenata Galoisove grupe $Aut_K(L)$ je jednak $n = [L : K]$, stupnju polinoma μ_α, ako i samo ako polinom μ_α u polju L ima n međusobno različitih nultočaka. Ako polinom μ_α u polju L ima n nultočaka tada se μ_α cijepa nad L, a kako je $L = K(\alpha)$ tada je L ujedno i polje cijepanja tog polinoma. S druge strane, ako su sve nultočke od μ_α međusobno različite, tada je taj polinom separabilan.

Primjer.

1. Neka je $L = \mathbb{C}$ i $K = \mathbb{R}$. Kako je $\mathbb{C} = \mathbb{R}(i)$ i $[\mathbb{C} : \mathbb{R}] = 2$, slijedi $|Aut_{\mathbb{R}}(\mathbb{C})| \leq 2$. Već smo vidjeli da su identiteta i kompleksno konjugiranje elementi Galoisove grupe $Aut_{\mathbb{R}}(\mathbb{C})$ pa je to grupa reda 2.

2. Neka je $L = \mathbb{Q}(\sqrt[3]{2})$ i $K = \mathbb{Q}$. Vidjeli smo da je minimalni polinom $\mu_{\sqrt[3]{2}} = x^3 - 2$ te da u skupu $\mathbb{Q}(\sqrt[3]{2})$ ovaj polinom ima samo jednu nultočku. Zato je $|Aut_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))| = 1$.

Situacija koja je opisana prethodnom propozicijom nije posebno ograničavajuća:
Teorem o primitivnom elementu.
Neka je L konačno separabilno proširenje polja K. Tada postoji $\alpha \in L$ takav da je $L = K(\alpha)$.

Drugim riječima, prethodnim rezultatom su pokrivena konačna separabilna proširenja.

Definicija.
Konačno separabilno proširenje L polja K zovemo **normalno proširenje polja** K ako je L polje cijepanja nekog polinoma $P \in K[x]$ nad K.

Prema Teoremu o primitivnom elementu je normalno proširenje L polja K upravo oblika $L = K(\alpha)$ za neki $\alpha \in L$.

Često se pojedine algebarske strukture mogu definirati na više ekvivalentnih načina. To je i ovdje slučaj:

Propozicija.
Neka je L konačno separabilno proširenje polja K. Sljedeće tvrdnje su ekvivalentne:

1. L je normalno proširenje polja K.
2. Ako je $Q \in K[x]$ ireducibilan polinom koji ima nultočku u polju L, tada se Q cijepa nad L.
3. $|Aut_K(L)| = [L : K]$.
4. $K = L^{Aut_K(L)} = \{x \in L : \sigma(x) = x, \forall \sigma \in Aut_K(L)\}$.

Ranije smo vidjeli da je uvijek $K \subseteq L^{Aut_K(L)}$. Sada znamo i da jednakost, u slučaju da je L konačno separabilno proširenje, vrijedi ako i samo ako je proširenje normalno.

Korolar.
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:
Kako je L konačno separabilno proširenje od K, slijedi da je L i konačno separabilno proširenje od M. Polje L je polje cijepanja nekog polinoma $P \in K[x]$, a kako je $K \subseteq M$ slijedi da je $P \in M[x]$ te je L i polje cijepanja polinoma iz $M[x]$ pa je L normalno proširenje od M.
Prema prethodnoj propoziciji (dio 3.) je $|Aut_K(L)| = [L : K]$ i $|Aut_M(L)| = [L : M]$ pa je

$$|Aut_M(L)| \cdot [M : K] = [L : M] \cdot [M : K] = [L : K] = |Aut_K(L)|.$$

Korolar.
Neka je L separabilno proširenje polja K i neka je H konačna podgrupa od $Aut_K(L)$. Tada je L normalno proširenje polja L^H i vrijedi

$$H = Aut_{L^H}(L).$$

Dokaz:
Već smo vidjeli da je L^H međupolje i $[L : L^H] = |H|$, te je L konačno separabilno proširenje od L^H. Za $\alpha \in L$ definiramo polinom $P \in L[x]$:

$$P = \prod_{\varphi \in H} (x - \varphi(\alpha)).$$

Za $\psi \in H$ je preslikavanje $\varphi \mapsto \psi \circ \varphi$ bijekcija s H na H (lijeva translacija), dobivamo iduću jednakost skupova:

$$\{\varphi(\alpha) : \varphi \in H\} = \{(\psi \circ \varphi)(\alpha) : \varphi \in H\}.$$

Djelovanjem s ψ na koeficijente polinoma P dobivamo polinom

$$\prod_{\varphi \in H} (x - (\psi \circ \varphi)(\alpha)) = \prod_{\varphi \in H} (x - \varphi(\alpha)) = P.$$

Prema tome, $P \in L^H[x]$, jer svaki $\psi \in H$ djeluje kao identiteta na koeficijentima polinoma P.
Kako je H grupa, H sadrži i neutralni element, tj. postoji $\varphi \in H$ takav da je $\varphi(\alpha) = \alpha$. Zato je α nultočka polinoma P te minimalni polinom μ_α od α dijeli P. Polinom P se, po definiciji, cijepa nad L, pa se i minimalni polinom od α cijepa nad L.
Neka je sada $Q \in L^H[x]$ ireducibilan polinom koji ima nultočku u L. Označimo li tu nultočku s α, polinom Q je oblika $a\mu_\alpha$, jer je ireducibilan i α mu je nultočka. Vidjeli smo da se minimalni polinom svakog elementa iz L cijepa nad L pa se i polinom Q cijepa. Slijedi da proširenje L polja L^H ima svojstvo 2. iz prethodnog teorema pa je normalno.
Prema dijelu 3. prethodnog teorema je sada $|Aut_{L^H}(L)| = [L : L^H] = |H|$.
Kako je $L^H = \{x \in L : \sigma(x) = x, \forall \sigma \in H\}$, za $\sigma \in H$ i $x \in L^H$ vrijedi $\sigma(x) = x$ pa je $\sigma \in Aut_{L^H}(L)$ odnosno $H \subseteq Aut_{L^H}(L)$. Sada iz jednakosti $|Aut_{L^H}(L)| = |H|$ slijedi $H = Aut_{L^H}(L)$.

Neka je L konačno proširenje polja K. Označimo s $\mathcal{F}$ skup svih međupolja M, $K \subseteq M \subseteq L$. Nadalje, označimo s $\mathcal{G}$ skup svih podgrupa Galoisove grupe $Aut_K(L)$.

Za $H \in \mathcal{G}$ definiramo $\Psi(H) = L^H = \{x \in L : \sigma(x) = x, \forall \sigma \in H\}$. Dobivamo preslikavanje $\Psi : \mathcal{G} \to \mathcal{F}$, jer je $K \subseteq L^H \subseteq L$.

Za $M \in \mathcal{F}$ definiramo $\Phi(M) = Aut_M(L) = \{\sigma \in Aut_K(L) : \sigma(x) = x, \forall x \in M\}$. Time dobivamo preslikavanje $\Phi : \mathcal{F} \to \mathcal{G}$, jer je $Aut_M(L) \leq Aut_K(L)$.

Teorem (Fundamentalni teorem Galoisove teorije).
Neka je L normalno proširenje polja K. Tada su funkcije Ψ i Φ međusobno inverzne bijekcije.
Dokaz:
Neka je $M \in \mathcal{F}$. Prema ranijem korolaru je L normalno proširenje polja M pa je, prema prethodnom teoremu, dijelu 4., $M = L^{Aut_M(L)}$.

Pokažimo da je Φ injekcija. Neka su $M_1, M_2 \in \mathcal{F}$ takvi da je $\Phi(M_1) = \Phi(M_2)$, tj. $Aut_{M_1}(L) = Aut_{M_2}(L)$. Tada je i

$$M_1 = L^{Aut_{M_1}(L)} = L^{Aut_{M_2}(L)} = M_2$$

pa je Φ injekcija.
Pokažimo sada da je Φ i surjekcija. Neka je $H \in \mathcal{G}$. Tada je $L^H \in \mathcal{F}$ te prema prethodnom korolaru vrijedi

$$\Phi(L^H) = Aut_{L^H}(L) = H$$

pa je Φ i surjekcija. Dakle, Φ je bijekcija, analogno se može vidjeti da je i Ψ bijekcija. Neka je $H \in \mathcal{G}$. Koristeći prethodni korolar još jednom, dobivamo

$$\Phi(\Psi(H)) = \Phi(L^H) = Aut_{L^H}(L) = H$$

te su bijekcije Ψ i Φ međusobno inverzne.

Napomena.
Prema Fundamentalnom teoremu Galoisove teorije, u slučaju da je L normalno proširenje polja K, broj međupolja je jednak broju podgrupa Galoisove grupe $Aut_K(L)$. Za $M_1, M_2 \in \mathcal{F}$ je $M_1 \subseteq M_2$ ako i samo ako je $\Phi(M_1) \supseteq \Phi(M_2)$, dok za $H_1, H_2 \in \mathcal{G}$ imamo $H_1 \subseteq H_2$ ako i samo ako je $\Psi(H_1) \supseteq \Psi(H_2)$ (kako preslikavanja koja su identiteta na većem skupu M_2 moraju biti identiteta i na manjem skupu M_1, iz $M_1 \subseteq M_2$ slijedi $\Phi(M_1) \supseteq \Phi(M_2)$; analogno iz $H_1 \subseteq H_2$ slijedi $\Psi(H_1) \supseteq \Psi(H_2)$, a kako su Ψ i Φ međusobno inverzni slijede i obrati).

Upoznali smo pojam normalne podgrupe i pojam normalnog proširenja. Sada ćemo povezati ova dva pojma.

Teorem.
Neka je L normalno proširenje polja K i neka je M 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 $Aut_K(L)/Aut_M(L)$.