Konačna polja

Ivan Novak

28.3.2025.

Za položiti ovu zadaću potrebno je skupiti barem 11 bodova. Svaki zadatak osim 16. i 17. nosi po 1 bod, a u 16. i 17. zadatku svaki podzadatak nosi po 1 bod.

Cilj ovog predavanja je objasniti kako izgledaju konačna polja. Konkretno, dokazat ćemo da svako konačno polje ima p^n elemenata za neki prost broj p i prirodan broj n, da polja s p^n elemenata postoje, te da su svaka dva konačna polja s p^n elemenata izomorfna.

Kratki uvod u algebarske strukture

Grupa je uređeni par $(G, \cdot)$, gdje je $\cdot : G \times G \to G$ operacija sa sljedećim svojstvima:

- asocijativnost, tj. $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$, za sve $g_1, g_2, g_3 \in G$;
- postoji neutralni element $e \in G$, za njega vrijedi $g \cdot e = e \cdot g = g$, za svaki $g \in G$;
- svaki $g \in G$ ima inverz g^{-1}, za njega vrijedi $g \cdot g^{-1} = g^{-1} \cdot g = e$.

Ako je operacija $\cdot$ komutativna, tada kažemo da je G komutativna ili Abelova. U tom slučaju operaciju množenja najčešće označavamo s $+$ umjesto $\cdot$, a neutralni element s 0.
Podgrupa H je podskup grupe G koji je grupa s obzirom na istu operaciju $\cdot$, to označavamo s $H \leq G$.
Prsten je uređena trojka $(R, +, \cdot)$, gdje su $+$ i $\cdot$ operacije na skupu R sa sljedećim svojstvima:

- $(R, +)$ je komutativna grupa,
- operacija $\cdot$ je asocijativna i postoji neutralni element 1,
- operacija $\cdot$ je distributivna u odnosu na $+$.

Prsten je komutativan ako je i operacija množenja $\cdot$ komutativna.
Integralna domena je komutativni prsten u kojem vrijedi

$$ab = 0 \implies a = 0 \text{ ili } b = 0.$$

Polje F je komutativni prsten u kojem svaki element $a \neq 0$ ima multiplikativni inverz, odnosno b takav da je $ab = 1_F$, gdje je 1_F neutralni element za mmnoženje od F (koji zovemo jedinica i često pišemo samo 1 umjesto 1_F).
Možemo kraće reći da je $(F \setminus \{0\}, \cdot)$ komutativna grupa, koju zovemo multiplikativna grupa polja i često označavamo s $F^\times$.
Karakteristika polja je najmanji prirodan broj n takav da je $\underbrace{1 + 1 + \ldots + 1}_{n \text{ puta}} = 0$, a ako taj broj ne postoji kažemo da je polje karakteristike 0.

Primjer 1. Vrijedi da su $\mathbb{Q}, \mathbb{R}$ i $\mathbb{C}$ polja, te $\mathbb{Z}$ nije polje, jer 2 nema multiplikativni inverz. Ta polja su karakteristike 0.

Nama zanimljiviji primjer je sljedeći.

Primjer 2. Za prost broj p, cijeli brojevi modulo p sa zbrajanjem i množenjem modulo p čine konačno polje s p elemenata karakteristike p, koje označavamo sa $\mathbb{F}_p$.

Zadatak 1. Dokažite da je karakteristika polja uvijek prost broj ili 0.

Homomorfizmi

Kad god pričamo o nekim algebarskim strukturama, moramo reći što će biti preslikavanja između njih koja su nam zanimljiva, te što znači da su dvije strukture izomorfne.

Definicija 3. Neka su R i S prstenovi. Homomorfizam prstenova $f : R \to S$ je funkcija sa sljedećim svojstvima:

- $f(a+b) = f(a) + f(b)$ za sve $a, b \in R$,
- $f(ab) = f(a)f(b)$ za sve $a, b \in R$.
- $f(1_R) = 1_S$.

Ako je f bijekcija, kažemo da je f izomorfizam i da su R i S izomorfni. Ako je f bijekcija i $R = S$, kažemo da je f automorfizam od R. Skup svih automorfizama s operacijom komponiranja čini grupu koju označavamo s $\mathrm{Aut}(R)$. Skup nultočaka homomorfizma zovemo jezgra i označavamo s $\ker f$. Vrijedi da je f injekcija ako i samo ako je $\ker f = \{0\}$.

Napomena 4. Svako polje je prsten, pa svi gore navedeni pojmovi imaju smisla i za polja.

Zadatak 2. Dokažite da skup svih automorfizama prstena s operacijom komponiranja čini grupu. Dokažite da je homomorfizam prstenova f injekcija ako i samo ako je $\ker f = \{0\}$.

Prosto potpolje

Definicija 5. Ako su L i K polja takva da je K sadržano u L (te su naravno računske operacije u L i K iste), kažemo da je L proširenje od K i pišemo L/K.

Primjer 6. Promotrimo skup $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Taj skup je polje, jer svaki element ima multiplikativni inverz (samo "racionaliziramo" razlomke). Dakle, $\mathbb{Q}[\sqrt{2}]$ je proširenje od $\mathbb{Q}$.

Lema 7. *Neka je F polje.*

a) *Ako je F karakteristike 0, onda sadrži potpolje izomorfno s $\mathbb{Q}$.*

b) *Ako je F karakteristike $p > 0$, onda sadrži potpolje izomorfno s $\mathbb{F}_p$.*

Dokaz. Neka je F polje. Označimo sa 1_F neutralni element u F. Za prirodan broj n, definiramo $n_F = \underbrace{1_F + 1_F + \ldots + 1_F}_{n \text{ puta}}$, te za negativne cijele brojeve $(-n)_F = -n_F$. Preslikavanje ϕ koje broju $n \in \mathbb{Z}$ pridružuje $n_F \in F$ je homomorfizam prstenova $\mathbb{Z} \to F$. Prema zadatku 1, jezgra tog homomorfizma je ili $\{0\}$ ili skup oblika $\{pm : m \in \mathbb{Z}\}$ za prost broj p.
Ako je jezgra $\{0\}$, onda možemo proširiti ϕ do preslikavanja iz $\mathbb{Q}$ u F, tako što definiramo $\phi(m/n) := \phi(m)/\phi(n) = m_F \cdot n_F^{-1}$. Preslikavanje $\phi : \mathbb{Q} \to F$ je injektivno, pa je $\phi(\mathbb{Q})$ potpolje od F izomorfno s $\mathbb{Q}$.
Ako je jezgra $\{pm : m \in \mathbb{Z}\}$, onda je $n_F = (n+p)_F$ za svaki $n \in \mathbb{Z}$, pa ϕ možemo shvatiti kao preslikavanje iz $\mathbb{F}_p$ u F. To preslikavanje je također injektivno. □

Polje iz prethodne leme zovemo prosto potpolje od F.
Naravno, ako je F konačno, nužno ima pozitivnu karakteristiku, pa mu je $\mathbb{F}_p$ prosto potpolje za neki prost broj p.

Broj elemenata konačnog polja

Napomena 8. Izrazito važna činjenica je sljedeća: ako je L/K proširenje polja, onda L ima strukturu vektorskog prostora nad K, gdje je množenje skalara $\lambda \in K$ i vektora $v \in L$ dano množenjem u polju L. To omogućava da primjenjujemo linearnu algebru na ta proširenja, što daje puno alata.

Lema 9. *Svako konačno polje karakteristike p ima p^n elemenata za neki prirodan broj n.*

Dokaz. Neka je F konačno polje karakteristike p. Tada F ima strukturu vektorskog prostora nad $\mathbb{F}_p$.
Kako je F konačno, dimenzija tog vektorskog prostora je konačna. Označimo ju s n.
Neka je $f_1, f_2, \ldots, f_n$ baza za F. Tada se svaki element polja F može zapisati kao

$$\alpha_1 f_1 + \ldots + \alpha_n f_n, \quad \alpha_1, \ldots, \alpha_n \in \mathbb{F}_p$$

na jedinstven način. Izbora za skalare $\alpha_1, \ldots, \alpha_n$ ima p^n, pa tvrdnja slijedi. □

Kako konstruirati proširenja polja, vol. 1

Za sad znamo da je broj elemenata konačnog polja uvijek potencija prostog broja, ali jedina konačna polja za koja znamo da postoje su ona s prostim brojem elemenata.

Zadatak 3. Neka je $n > 1$ i p prost broj. Dokažite da $\mathbb{Z}/p^n\mathbb{Z}$ (cijeli brojevi modulo p^n sa zbrajanjem i množenjem modulo p^n) nije polje.

Također, znamo da svako polje s p^n elemenata mora biti proširenje od $\mathbb{F}_p$.
U primjeru s $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$, poslužili smo se činjenicom da $\sqrt{2}$ leži u većem polju $\mathbb{R}$ koje nam je dobro poznato, pa smo iz njega izrezali manje međupolje. Međutim, nemamo puno primjera većih polja koja sadrže $\mathbb{F}_p$.

Primjer 10. Sad ćemo konstruirati polje s 4 elementa.
Neka je $F = \{0, 1, \omega, 1+\omega\}$, tako da je $1+1=0$, $\omega+\omega=0$ i $\omega^2 = \omega + 1$.
Drugim riječima,

$$F = \{a + b\omega \mid a, b \in \mathbb{F}_2,\ \omega^2 = \omega + 1\}.$$

Tada je F polje s 4 elementa.

Primjer 11. Slično možemo konstruirati polje s 9 elemenata. Stavimo

$$F = \{a + b\epsilon \mid a, b \in \mathbb{F}_3,\ \epsilon^2 = 2\}.$$

U oba slučaja smo konstruirali polje na sljedeći način: krenuli smo od polja koje znamo, dodali smo u njega formalni simbol (ω odnosno ϵ) i dodali relaciju koju taj formalni simbol zadovoljava. Pomoću te relacije svaki izraz $f(\omega)$ za polinom f koji se pojavi u računanju možemo svesti na $g(\omega)$ za neki drugi polinom g stupnja ≤ 1.
Međutim, nismo zadovoljni ovom razinom formalnosti, gdje smo samo izmislili simbol i rekli mu kako se treba ponašati: što ako smo npr. u uputama kako da se simbol ponaša bili kontradiktorni? Znači da moramo eksplicitno provjeravati da smo ovom konstrukcijom dobili polje.

Zadatak 4. Neka je

$$F = \{a + b\epsilon \mid a, b \in \mathbb{F}_7,\ \epsilon^2 = 2\}.$$

Dokažite da F nije polje.

Kako konstruirati proširenja polja, vol. 2

Definicija 12. Neka je R prsten. Ideal u R je podskup $I \subseteq R$ zatvoren na zbrajanje i oduzimanje takav da je $f \cdot g \in I$ za svaki $f \in R$ i svaki $g \in I$.

Ideja iza definicije ideala je sljedeća. Recimo da imamo veliki prsten R u kojem želimo na silu dodati neku novu relaciju (npr. $\epsilon^2 = 2$). Tada neće samo vrijediti $\epsilon^2 = 2$ već i niz drugih relacija, npr. $\epsilon^3 = 2\epsilon$, $\epsilon^2 + 3 = 5$ itd. Ako želimo odjednom uzeti u obzir sve relacije koje slijede iz $\epsilon^2 = 2$, dobit ćemo da je skup stvari koje postanu jednake 0 zatvoren na zbrajanje i oduzimanje, te zatvoren na množenje elementima iz R.
Ako imamo ideal I u prstenu R, onda možemo na R definirati relaciju ekvivalencije na sljedeći način:

$$a \equiv b \pmod{I} \iff a - b \in I.$$

Skup klasa označavamo s R/I. Na klasama ekvivalencije definiramo operacije zbrajanja i množenja tako da je $[a] \cdot [b] = [ab]$, $[a] + [b] = [a + b]$, gdje $[a] \in R/I$ označava klasu od $a \in R$. Uz potpuno istu argumentaciju kao kod definicije kongruencija, ovo su dobro definirane operacije uz koje R/I čini prsten, koji zovemo *kvocijentni prsten*.
U prstenu R/I računamo kao i u R, samo što kad god sretnemo nešto iz I u računu, možemo to nešto zamijeniti s 0.

Zadatak 5. Dokažite da su operacije dobro definirane (morat ćete koristiti oba svojstva ideala iz definicije).

Ovo je zapravo direktna generalizacija konstrukcije cijelih brojeva modulo n, čak i oznake odgovaraju ($\mathbb{Z}/n\mathbb{Z}$ jer je ideal iz definicije kongruencija upravo $n\mathbb{Z}$).
Uz ovaj novi alat, možemo na čišći način definirati polja s 4 odnosno 9 elemenata:

Primjer 13. Polje s 4 elemenata je $F = \mathbb{F}_2[x]/I$, gdje je $I = \{a \cdot (x^2 + x + 1) \mid a \in \mathbb{F}_2[x]\}$.
Polje s 9 elemenata je $F = \mathbb{F}_3[x]/I$, gdje je $I = \{a \cdot (x^2 - 2) \mid a \in \mathbb{F}_3[x]\}$.
Međutim, skup $F = \mathbb{F}_7[x]/I$, gdje je $I = \{a \cdot (x^2 - 2) \mid a \in \mathbb{F}_7[x]\}$ nije polje.

Općenito, ako želimo proširiti dano polje K, postupak je sljedeći: prvo pređemo u prsten polinoma $K[x]$, onda zadamo koju relaciju želimo da x zadovoljava. Ako je ta relacija ispravnog tipa, dobit ćemo polje, i to polje će u pravilu sadržavati početno polje K. Idući cilj je opisati ideale u prstenu $K[x]$ (vidjet ćemo da su jednostavniji nego što se čine), a onda vidjeti za koje ideale I će $K[x]/I$ biti polje (odgovor je jako elegantan).

Ideali od $K[x]$

Ideal je po definiciji skup koji je zatvoren na zbrajanje i oduzimanje, te množenje elementima prstena.

Definicija 14. Neka je R prsten i $a \in R$. Glavni ideal $(a) = aR$ je skup $\{ra \mid r \in R\}$.

Drugim riječima, (a) je skup svih višekratnika od a. Ovo su najjednostavniji ideali, a u dovoljno lijepim prstenovima su svi ideali ovog oblika. Takav je i $K[x]$ za polje K.

Primjer 15. Dokažimo prvo da su svi ideali u $\mathbb{Z}$ glavni.
Neka je $I \subset \mathbb{Z}$ ideal. Neka je m najmanji pozitivan element od I. Tvrdimo da je $I = (m)$. Naime, ako je $n \in I$ i $m \nmid n$, onda možemo prema teoremu o dijeljenju s ostatkom n zapisati kao $qm + r$, za $0 < r < m$. Međutim, kako je $m \in I$, slijedi $qm \in I$, pa je i $qm - n = r \in I$. Međutim, to je kontradikcija s time da je m minimalan.

Primijetimo da je jedina činjenica o $\mathbb{Z}$ koju smo koristili teorem o dijeljenju s ostatkom. Analogon tog teorema postoji u $K[x]$.

Teorem 16. *Neka je K polje, i neka su f i g ne-nul polinomi iz $K[x]$. Tada postoje polinomi q i r iz $K[x]$ takvi da je*

$$f = q \cdot g + r, \ \deg r < \deg f \quad \textit{ili } r = 0.$$

Stoga su svi ideali u $K[x]$ također glavni.

Zadatak 6. Dokažite da ideal $(2, x) := \{a \cdot 2 + b \cdot x \mid a, b \in \mathbb{Z}[x]\} \subset \mathbb{Z}[x]$ nije glavni. (Naime, u dokazu teorema o dijeljenju s ostatkom je bitno da su vodeći koeficijenti polinoma invertibilni, a u $\mathbb{Z}[x]$ to ne mora biti slučaj.)

Sad kad znamo kako izgledaju ideali u $K[x]$, vrijeme je da odredimo kad će kvocijent biti polje.
Prisjetimo se, za nekonstantan polinom $f \in K[x]$ kažemo da je *ireducibilan* ako se ne može zapisati kao $g \cdot h$ za nekonstantne polinome $g, h \in K[x]$.

Propozicija 17. *Neka je K polje i $f \in K[x]$ nekonstantan. Tada je $K[x]/(f)$ polje ako i samo ako je f ireducibilan.*

Dokaz. Pretpostavimo da se f može zapisati kao $g \cdot h$ za nekonstantne g i h. Onda je $g \cdot f \equiv 0 \pmod{(f)}$, pa ili $[g]$ ili $[h]$ nema multiplikativni inverz u $K[x]/(f)$. Kako je $\deg g < \deg f$, ne može vrijediti $g \equiv 0 \pmod{(f)}$, pa $[g]$ nije ni invertibilan ni 0, pa $K[x]/(f)$ nije polje.
Pretpostavimo sada da f jest ireducibilan. Uzmimo sada $g \in K[x]$ takav da je $g \not\equiv 0 \pmod{(f)}$. Tada po Bezoutovoj lemi za polinome postoje polinomi $a, b \in K[x]$ za koje je $af + bg = 1$. Promatranjem jednadžbe modulo f dobivamo

$$bg \equiv 1 \pmod{f},$$

odnosno $[b]$ je multiplikativni inverz od $[g]$ u $K[x]/(f)$. Zaključujemo da za svaki $g \in K[x]$ vrijedi ili $[g] = [0]$ ili je $[g]$ invertibilan, pa je traženi skup stvarno polje. □

Dakle, konačno imamo recept za konstruirati veća polja: samo nađi ireducibilni polinom i promotri kvocijent prstena polinoma! Ne samo da dobivamo polje, nego odmah znamo i koja su pravila zbrajanja i množenja u njemu.

Polja kardinalnosti p^2

Zadatak 7. Neka je f ireducibilan polinom iz $K[x]$, gdje je K polje. Dokažite da $K[x]/(f)$ ima strukturu vektorskog prostora nad K dimenzije $\deg(f)$, te da $1, x, x^2, \ldots, x^{\deg(f)-1}$ čine bazu.

Dakle, da bismo konstruirali polja kardinalnosti p^2, samo trebamo za svaki prost broj p naći ireducibilan polinom stupnja 2 u $\mathbb{F}_p[x]$.
To je lako: polinom stupnja 2 je ireducibilan ako i samo ako nema nultočku.

Zadatak 8. Dokažite da za svaki prost broj p postoji polinom stupnja 2 u $\mathbb{F}_p[x]$ koji nema nultočku u $\mathbb{F}_p$.

Međutim, već za stupanj 3 je teško pronaći konkretne polinome stupnja 3 koji su ireducibilni u $\mathbb{F}_p[x]$ (ok, za neke p je lagano). Tako da nas naša prva metoda ipak nije odvela predaleko i trebamo drugačiji pristup (vratit ćemo se kasnije na ovaj pristup).

Zadatak 9. Neka je d prirodan broj. Dokažite da za beskonačno mnogo prostih brojeva p postoji $\alpha \in \mathbb{F}_p$ takav da je polinom $x^d - \alpha$ ireducibilan.

Polje cijepanja

Recimo da imamo ireducibilan polinom $f \in K[x]$. Tada on nema nultočaka u K (osim ako je stupnja 1). Pitanje koje se postavlja je možemo li uvijek povećati K tako da f ima nultočku u K.
Naravno, ako imamo polinom s racionalnim koeficijentima, to možemo učiniti, jer po osnovnom teoremu algebre svaki polinom s kompleksnim koeficijentima ima nultočku nad $\mathbb{C}$. Međutim, tu koristimo veliku crnu kutiju, te smo također previše povećali naše polje.
Možemo i manje povećati polje - u idućoj propoziciji se javlja poznati akter.

Propozicija 18. *Neka je f ireducibilan polinom iz $K[x]$. Tada f ima nultočku u proširenju $K[x]/(f)$.*

Dokaz. Promotrimo $[x] \in K[x]/(f)$. Tada je $f([x]) = [f(x)] = 0$ u $K[x]/(f)$. □

Ovo je možda izrazito zbunjujuće (možda bi i notacija mogla biti bolja). Ali zapravo je izrazito logično: $K[x]/(f)$ smo konstruirali tako što smo u K dodali element α za koji smo htjeli da vrijedi $f(\alpha) = 0$. Dobro, nismo baš tako, nego smo drugačije formalizirali, ali $f(\alpha) = 0$ i dalje vrijedi.
Uglavnom, ako imamo polinom f, možemo povećati polje da ima nultočku α. Onda napišimo $f = (x-\alpha)\cdot g$, pa možemo isto ponoviti za neki ireducibilni faktor od g i za ovo veće proširenje. Nakon najviše $\deg(f)$ koraka, dobivamo polje u kojem f ima sve nultočke.

Definicija 19. Neka je $f \in K[x]$ nekonstantan. Proširenje L/K takvo da je f umnožak linearnih polinoma iz $L[x]$ i takvo da ne postoji manje proširenje M/K s takvim svojstvom zovemo *polje cijepanja* od f.

Teorem 20. *Sva polja cijepanja polinoma $f \in K[x]$ su izomorfna.*

Ovaj teorem nije težak za dokazati, ali nemamo vremena i trebali bi razviti još malo teorije za njega, pa ćemo ga uzeti kao crnu kutiju.

Konačno sva konačna polja

Lema 21. *Neka je K polje. Nenul polinom $f \in K[x]$ ima najviše* $\deg(f)$ *nultočaka.*

Dokaz. Ako je α nultočka, podijelimo f s $x - \alpha$ i primijenimo indukciju. □

Lema 22. *Neka je $\varphi(n)$ broj brojeva manjih ili jednakih n koji su relativno prosti s n. Tada je*

$$\sum_{d|n} \varphi(d) = n.$$

Zadatak 10. Dokažite ovu lemu.

Sad mrvicu teorije grupa.

Definicija 23. Neka je G grupa i H podgrupa. Kažemo da je H ciklička podgrupa ako je $H = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ za neki $a \in H$, koji zovemo generator od H.

Teorem 24 (Lagrange)**.** *Neka je G konačna grupa i $H \subseteq G$ podgrupa. Tada $|H|$ dijeli $|G|$.*

Zadatak 11. Dokažite ovu tvrdnju (ili potražite dokaz na internetu i zapišite ga svojim riječima, ovo je obično prvi teorem iz teorije grupa koji se dokaže).

Posebno, ako je G konačna grupa i $a \in G$, tada $|\langle a \rangle|$ dijeli $|G|$, odnosno najmanji $n \in \mathbb{N}$ takav da je $a^n = 1$ dijeli $|G|$. Kraće rečeno, red elementa dijeli red grupe.
Sada konačno možemo konstruirati konačna polja svih redova p^n.

Zadatak 12. Neka je F polje karakteristike $p > 0$. Dokažite da je $x^p + y^p = (x + y)^p$ za sve $x, y \in F$.

Propozicija 25. *Polje cijepanja polinoma $x^{p^n} - x \in \mathbb{F}_p[x]$ ima p^n elemenata.*

Dokaz. Neka je F polje cijepanja od $x^{p^n} - x$. Neka je $H \subset F$ skup svih nultočaka tog polinoma. Tada H ima p^n elemenata te sadrži 0 i 1. Nadalje, H je zatvoren na zbrajanje, jer ako je $x^{p^n} = x$ i $y^{p^n} = y$, onda je $(x + y)^{p^n} = x^{p^n} + y^{p^n}$ po prethodnom zadatku. Također, H je zatvoren na dijeljenje, jer ako je $x^{p^n} = x$ i $y^{p^n} = y$, onda je $(x/y)^{p^n} = x/y$.
Dakle, H je polje. Sada imamo potpolje polja cijepanja polinoma koje sadrži sve nultočke tog polinoma. Dakle, onda je H polje cijepanja polinoma, odnosno $H = F$.

□

Sad smo konačno konstruirali polje s p^n elemenata. Preostaje dokazati da su sva polja s p^n elemenata izomorfna. Međutim, to je jednostavno. Ako je F neko polje s p^n elemenata, onda po Lagrangeovom teoremu za svaki $x \in F^\times$ vrijedi $x^{p^n - 1} = 1$, pa je F također polje cijepanja od $x^{p^n} - x \in \mathbb{F}_p[x]$. Kako su sva polja cijepanja polinoma međusobno izomorfna, zaključujemo da su sva polja s p^n elemenata izomorfna.
To znači da sada možemo uvesti po jednu oznaku za svaku potenciju prostog broja. Od sada nadalje, polje s $q = p^n$ elemenata ćemo označavati s $\mathbb{F}_q$.

Multiplikativna struktura konačnih polja

Za sad znamo da u polju $\mathbb{F}_q$ vrijedi $x^q = x$ za svaki $x \in \mathbb{F}_q$. Ono što je sada cilj dokazati je analogon teorema o primitivnom korijenu za $\mathbb{F}_p$, koji kaže da postoji $g \in \mathbb{F}_p$ takav da je svaki $n \in \mathbb{F}_p^\times$ jednak nekoj potenciji od g.
Prvo trebamo jedan općenitiji rezultat.

Propozicija 26. *Neka je $G \subset K^\times$ konačna podgrupa multiplikativne grupe polja. Tada je G ciklička.*

Dokaz. Neka je n red od G i neka je $\psi(d)$ broj elemenata od G koji su reda d. Tada je $\psi(d) = 0$ za $d \nmid n$ zbog Lagrangeovog teorema.
Neka je d djelitelj od n i $y \in G$ reda d. Tada je y nultočka polinoma $x^d - 1$, te su sve potencije od y također nultočke, i ima ih točno d, pa su to sve nultočke.
U skupu $\{1, y, y^2, \ldots, y^{d-1}\}$ ima točno $\varphi(d)$ elemenata reda d (to su oni čiji su eksponenti relativno prosti s d), pa je $\psi(d) = \varphi(d)$ ili je $\psi(d) = 0$. U svakom slučaju, $\psi(d) \leq \varphi(d)$.
Međutim, imamo

$$\sum_{d|n} \psi(d) = n = \sum_{d|n} \varphi(d),$$

pa je $\psi(d) = \varphi(d)$ za svaki d. Posebno, $\psi(n) = \varphi(n) > 0$ pa u G postoji element reda n. □

Ako ovo primijenimo na $\mathbb{F}_q^\times$, dobijemo da postoji $g \in \mathbb{F}_q^\times$ takav da je $\mathbb{F}_q^\times = \{1, g, g^2, \ldots\}$. Taj g zovemo generator ili primitivni korijen.

Zadatak 13. Neka je g generator za $\mathbb{F}_{p^n}$, gdje je $n \geq 2$. Neka je $g + g^2 = g^m$ za $m \in \{1, 2, \ldots, p^n - 1\}$. Dokažite da je $m \geq n + 1$.

Potpolja od $\mathbb{F}_q$

Neka je F potpolje od $\mathbb{F}_q$, gdje je $q = p^n$. Onda imamo toranj proširenja $\mathbb{F}_q/F/\mathbb{F}_p$, pa je $F = \mathbb{F}_{p^m}$ za $1 \leq m \leq n$.
Općenito, ako je L/K proširenje polja, s $[L : K]$ označavamo dimenziju L kao vektorskog prostora nad K, i to zovemo stupanj proširenja.

Lema 27. *Ako je $L/M/K$ toranj proširenja polja, onda je $[L : K] = [L : M][M : K]$.*

Skica dokaza. Ako je $\{\alpha_1, \ldots, \alpha_k\}$ baza za L/M i $\{\beta_1, \ldots, \beta_\ell\}$ baza za M/K, onda umnošci

$$\{\alpha_i \beta_j \mid 1 \leq i \leq k, 1 \leq j \leq \ell\}$$

čine bazu za L/K. □

Zadatak 14. Dopunite prethodni dokaz argumentom da je ovaj skup stvarno baza za L/K.

Vratimo se na naš toranj. Imamo $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}][F_{p^m} : \mathbb{F}_p]$, pa nužno vrijedi $m \mid n$.

Zadatak 15. Dokažite da u polju $\mathbb{F}_{p^n}$ postoji potpolje reda p^m za svaki m koji dijeli n.

Dakle, potpolja od $\mathbb{F}_{p^n}$ su točno sva polja $\mathbb{F}_{p^m}$, gdje je m djelitelj od n.

Ireducibilni polinomi stupnja n

Vratimo se sada ideji drugačije konstrukcije konačnog polja: preko ireducibilnih polinoma. Tamo nam je bio problem što nismo znali općenito naći ireducibilne polinome stupnja n u $\mathbb{F}_p[x]$ za svaki n.
Međutim, sada ćemo dokazati da takvi polinomi postoje, tako što ćemo ih prebrojati.

Zadatak 16.

a) Neka su f i g dva različita normirana ireducibilna polinoma iz $\mathbb{F}_p[x]$. Dokažite da f i g nemaju zajedničkih nultočaka ni u kojem proširenju od $\mathbb{F}_p$.

b) Dokažite da ako je f ireducibilan polinom iz $\mathbb{F}_p[x]$, onda f i f' nemaju zajedničkih nultočaka ni u kojem proširenju od $\mathbb{F}_p$. Zaključite da ireducibilni polinomi iz $\mathbb{F}_p[x]$ nemaju dvostrukih nultočaka.

Zadatak 17.

a) Promatranjem nultočaka na obje strane, dokažite da za svaki prost broj p i prirodan broj n vrijedi (ova jednakost je u $\mathbb{F}_p[x]$)

$$x^{p^n} - x = \prod_{d \mid n} \prod_{\substack{f \in \mathbb{F}_p[x] \\ \text{normiran,} \\ \text{ireducibilan,} \\ \deg(f) = d}} f(x).$$

b) Neka je $M_k(p)$ broj ireducibilnih normiranih polinoma stupnja k u $\mathbb{F}_p[x]$. Dokažite $\sum_{d|n} dM_d(p) = p^n$.

c) Pomoću Mobiusove inverzije dokažite da je

$$M_n(p) = \frac{1}{n} \sum_{d|n} \mu(d) p^{n/d},$$

gdje je μ Mobiusova funkcija. Konačno, zaključite da je $M_n(p) > 0$ za sve p i n.