UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Matematika – 1. stopnja

Andraž Naglič

Konstruktibilna števila

Delo diplomskega seminarja

Mentor: prof. dr. Matej Brešar

Ljubljana, 2017

Kazalo

Konstruktibilna števila

Povzetek

V nalogi je predstavljen pojem konstruktibilnih števil. Najprej se izpeljejo sredstva abstraktne algebre, ki so nujno potrebna za dokaz izreka, ki pove, katera realna števila so konstruktibilna. Temu sledi definicija konstruktibilnih števil in izpeljava prej omenjenega izreka. S pomočjo tega izreka na koncu odgovorimo na tri vprašanja povezana s konstruktibilnimi števili.

Constructible numbers

Abstract

In this work we present constructible numbers. First, we develop tools of abstract algebra needed in the proof of the theorem that tells us which real numbers are constructible. Then follows the definition of constructible numbers and formulation of the theorem mentioned above. With that theorem we provide answer for three questions connected with constructible numbers.

Math. Subj. Class. (2010): 12F05

Ključne besede: konstruktibilno število, kolobar polinomov, razširitev obsega, nerazcepen polinom

Keywords: constructible number, ring of polynomials, field extention, irreducible polynomial

1. Uvod

Že v antični Grčiji so se matematiki in filozofi ukvarjali z geometrijskimi problemi. Dva od najbolj znanih geometrijskih izrekov, ki so ju dokazali starogrški matematiki, sta Pitagorov izrek in Talesov izrek. Obstajajo pa tudi problemi, ki jih starogrški matematiki niso znali rešiti. V tej nalogi bo govora o treh takih problemih. To so podvojitev kocke, trisekcija kota in kvadratura kroga. Omejitev pri reševanju teh problemov je, da smemo uporabiti le šestilo in ravnilo brez oznak dolžin. Podvojitev kocke zahteva, da s pomočjo dane kocke s prostornino ena konstruiramo kocko s prostornino dva. Problem trisekcije kota nas sprašuje, če lahko kot poljubne velikosti razdelimo na tri enake dele (seveda le z uporabo šestila in ravnila). Kvadratura kroga pa sprašuje, če lahko iz danega enotskega kroga konstruiramo kvadrat, ki ima enako ploščino kot krog. Pokazali bomo, da prvi dve konstrukciji nista mogoči. Tudi tretja konstrukcija je nemogoča, toda tega ne bomo dokazali. Glavni izrek naloge reši splošnejši problem. Pove namreč, katera števila lahko konstruiramo s šestilom in ravnilom ter katerih ne moremo.

Razlog, da starogrški matematiki niso znali rešiti teh problemov, je, da so iskali geometrijsko rešitev, saj niso imeli na voljo sodobnejših abstraktnih teorij. Prvi, ki je objavil rešitev teh treh problemov, je bil francoski matematik Pierre Laurent Wantzel. Tako kot on bomo v tej nalogi izpeljali vse izreke abstraktne algebre, ki jih bomo potrebovali za dokaz izreka, ki pove, katera realna števila so konstruktibilna.

2. Grupe, kolobarji, obsegi in vektorski prostori

V tem poglavju bomo definirali nekatere od algebraičnih struktur in izpeljali tiste njihove lastnosti, ki jih bomo potrebovali v glavnem delu naloge. Ker se bodo definicije in izreki vrstili en za drugim, si bomo nekatere rezultate ogledali na primeru celih števil. Glavnina snovi tega poglavja je povzeta po viru [2].

2.1. **Osnovne definicije.**

Definicija 2.1. *Binarna operacija* na množici M je preslikava iz $M \times M$ v M.

Opomba 2.2. Pravimo, da je množica M zaprta za binarno operacijo, saj parom elementov iz M priredi nov element v tej isti množici.

Definicija 2.3. *Grupa* je neprazna množica G skupaj z binarno operacijo množenja (produkt elementov a in b označimo z $a \cdot b$ oziroma na kratko z ab), ki ima naslednje lastnosti:

(1) Za vse elemente $a, b, c \in G$ velja $a(bc) = (ab)c$. Tej lastnosti pravimo *asociativnost*.
(2) Obstaja element $e \in G$, za katerega velja $ea = ae = a$ za vse elemente $a \in G$. Elementu e pravimo *enota* grupe G.
(3) Za vsak element $a \in G$ obstaja $b \in G$, da velja: $ab = ba = e$. Elementu b pravimo *inverz* elementa a in ga označimo z a^{-1}. Pravimo tudi, da so elementi grupe obrnljivi.

Grupa je *komutativna/Abelova*, če ima operacija še lastnost:

(4) Za vse elemente $a, b \in G$ je $ab = ba$.

Grupo G opremljeno z binarno operacijo množenja označimo z $(G, \cdot)$.

Opomba 2.4. Enoto grupe največkrat označimo z 1. Če je grupa G Abelova, njeno binarno operacijo običajno označimo s $+$ in jo imenujemo seštevanje. V tem primeru spremenimo tudi ostale oznake. Enoto označimo z 0, inverz elementa a pa z $-a$.

Definicija 2.5. Množica H je *podgrupa* grupe G, če je $H \subseteq G$ in je že sama grupa za isto operacijo (operacijo zožimo na $H \times H$).

Lema 2.6. *Naj bo G grupa in H njena neprazna podmnožica. Množica H je podgrupa G natanko tedaj, ko velja: če sta $a, b \in H$, potem je tudi $ab^{-1} \in H$.*

Dokaz. ($\Leftarrow$) Množica H je neprazna. Torej obstaja $a \in H$ in je zato $e = aa^{-1} \in H$. Če je $b \in H$, je tudi $b^{-1} = eb^{-1} \in H$. Če sta $a, b \in H$, je tudi $b^{-1} \in H$ in zato je $a(b^{-1})^{-1} = ab \in H$. Asociativnost sledi iz asociativnosti G. Množica H je torej grupa oziroma podgrupa G.

($\Rightarrow$) Množica H je grupa. Torej je za vsak $b \in H$ tudi $b^{-1} \in H$. Sledi: če sta $a, b \in H$, je tudi $ab^{-1} \in H$, saj je množica H zaprta za grupno operacijo. □

Primer 2.7. Oglejmo si množico celih števil $\mathbb{Z}$ in običajno operacijo seštevanja. Seštevanje celih števil je binarna operacija, saj dvema celima številoma priredi njuno vsoto, ki je spet celo število. Prepričamo se lahko, da so izpolnjene vse štiri lastnosti iz definicije 2.3. Asociativnost bi sicer morali preveriti po definiciji seštevanja naravnih števil, a iz prakse vemo, da lahko pri seštevanju celih števil oklepaje izpustimo

$$a + (b + c) = a + b + c = (a + b) + c.$$

Enoto za seštevanje lahko uganemo. Iščemo celo število x, za katerega bo

$$a + x = x + a = a$$

za vsako celo število a. To je seveda število 0. Tudi inverz celega števila lahko uganemo. Inverz števila a bo tako celo število y, da velja

$$a + y = y + a = 0.$$

To enakost izpolni število $y = -a$, ki je tudi celo število. Preprosto je še preveriti, da je seštevanje celih števil komutativno. S tem smo pokazali, da je $(\mathbb{Z}, +)$ Abelova grupa.

Podobno kot za seštevanje celih števil, se lahko lotimo dokazovanja lastnosti za množenje celih števil. Asociativnost in komutativnost zlahka preverimo in število 1 je enota za množenje. Problem nastane pri obrnljivosti. Inverz celega števila a je število $\frac{1}{a}$, ki je racionalno, ne pa celo število. Množica $\mathbb{Z}$ torej ni grupa za množenje. Ker cela števila lahko seštevamo in množimo, je to zgled, iz katerega izhaja definicija kolobarja. ♢

Definicija 2.8. *Kolobar* je neprazna množica R skupaj z dvema binarnima operacijama. Vsoto elementov a in b označimo s $+$, produkt pa na kratko označimo z ab. Za binarni operaciji mora veljati

(1) $(R, +)$ je Abelova grupa
(2) Za vse $a, b, c \in R$ velja $a(bc) = (ab)c$ (asociativnost množenja).
(3) Obstaja enota za množenje $e \in R$, za katero je $ea = ae = a$ za vse elemente $a \in R$.
(4) Za vse $a, b, c \in R$ je $a(b + c) = ab + ac$ in $(a + b)c = ac + bc$. To sta zakona *distributivnosti*.

Kolobar je komutativen, če ima množenje še lastnost:

(5) Za vse $a, b \in R$ je $ab = ba$ (komutativnost množenja).

Opomba 2.9. Velja dogovor, da v kolobarju seštevanje označujemo s $+$ in znak za produkt opuščamo (produkt elementov a in b označimo z ab). V nadaljevanju zato ne bomo vedno pisali, kako označujemo operaciji v kolobarju.

V tej nalogi bo govora le o komutativnih kolobarjih, zato bomo v nadaljevanju uporabljali kar izraz kolobar namesto komutativni kolobar. Vse definicije in izreke v nadaljevanju bi lahko (z nekaj spremembami) formulirali tudi za nekomutativne kolobarje. Kadar govorimo o obrnljivih elementih kolobarja R, s tem mislimo na obrnljive elemente za operacijo množenja (za seštevanje so vsi obrnljivi). Podobno kot pri grupah lahko za kolobarje definiramo *podkolobarje*. To so podgrupe aditivne grupe $(R, +)$, ki so zaprte za množenje.

Na splošno v kolobarjih ne velja, da iz enakosti $ab = ac$ sledi $b = c$. To je posledica dejstva, da se v kolobarju dva neničelna elementa lahko zmnožita v 0. Kolobar, v katerem je produkt neničelnih elementov vedno različen od 0, imenujemo *cel kolobar*. Povedano drugače, če je v celem kolobarju $ab = 0$, potem je $a = 0$ ali $b = 0$. To pomeni, da v celih kolobarjih velja pravilo krajšanja. Recimo, da je $a \neq 0$ in $ab = ac$. Enakost lahko preoblikujemo v $a(b-c) = 0$. Ker vemo, da $a \neq 0$, mora biti $b-c = 0$ oziroma $b = c$.

Kolobar F, v katerem $1 \neq 0$, se imenuje *obseg*, če je vsak neničelni element v F obrnljiv. Hitro lahko vidimo, da je vsak obseg cel. Naj bosta a in b neničelna elementa obsega F. Recimo, da je $ab = 0$. Enakost pomnožimo z a^{-1} in b^{-1} in dobimo

$$1 = a^{-1}abb^{-1} = 0,$$

kar pa je v nasprotju z definicijo obsega.

Obsegu, v katerem je množenje komutativno, običajno pravimo komutativni obseg. A ker bo v nadaljevanju govora le o komutativnih obsegih, bomo z besedo obseg označevali komutativne obsege. Podmnožici K obsega F, ki je že sama zase obseg za isti operaciji kot F (zoženi na K), pravimo *podobseg*.

Pri študiju algebraičnih struktur imajo pomembno vlogo preslikave, ki ohranjajo strukturo množic. Takim preslikavam pravimo homomorfizmi.

Definicija 2.10. Naj bosta R in S kolobarja. Funkcija $f : R \longrightarrow S$ je *homomorfizem kolobarjev*, če ima naslednji lastnosti:

$$f(a + b) = f(a) + f(b) \quad \text{in} \quad f(ab) = f(a)f(b)$$

za vse elemente $a, b \in R$.

Še posebej nas zanimajo homomorfizmi, ki bijektivno preslikajo en kolobar v drugega. Takim homomorfizmom pravimo *izomorfizmi*. Če med kolobarjema R in S obstaja izomorfizem, pravimo, da sta kolobarja izomorfna in to označimo z $R \cong S$.

Pomembni množici, povezani s homomorfizmom kolobarja, sta jedro in slika homomorfizma. *Jedro* homomorfizma je

$$\operatorname{Ker} f = \{x; f(x) = 0\} \subseteq R.$$

Če je f injektiven, je $\operatorname{Ker} f = \{0\}$. *Slika* homomorfizma je

$$\operatorname{Im} f = \{f(x); x \in R\} \subseteq S.$$

Preverimo lahko, da sta jedro in slika podkolobarja v R oziroma v S, a opazimo, da jedro zadošča tudi strožjemu pogoju:

$$x \in \operatorname{Ker} f, r \in R \Rightarrow f(rx) = f(r)f(x) = f(r)\cdot 0 = 0.$$

Torej jedro homomorfizma ni zaprto le za množenje znotraj jedra, ampak za množenje z vsemi elementi kolobarja R. Zato pravimo, da je jedro homomorfizma ideal kolobarja R.

Definicija 2.11. Podmnožica I kolobarja R je *ideal*, če je

(1) $(I, +)$ podgrupa $(R, +)$ in
(2) $rx \in I$ za vse $r \in R$, $x \in I$.

Opomba 2.12. V nekomutativnih kolobarjih lahko govorimo o levih, desnih in dvostranskih idealih (glede na to, s katere strani množimo z elementi iz R), v komutativnih kolobarjih pa med njimi ni razlike.

Opazimo naslednjo lastnost idealov. Naj bo a obrnljiv element kolobarja R in I neki ideal tega kolobarja. Če je $a \in I$, je tudi $1 = a^{-1}a \in I$. To pa pomeni, da so v idealu I tudi vsi elementi oblike $r\cdot 1$, kjer je $r \in R$ in zato je $I = R$. *Pravi ideali* (tisti, ki niso enaki celotnemu kolobarju in niso enaki $\{0\}$) torej ne vsebujejo obrnljivih elementov.

Izrek 2.13. *Naj bo R kolobar. Potem je R obseg natanko tedaj, ko sta $\{0\}$ in R njegova edina ideala.*

Dokaz. ($\Rightarrow$) Zgoraj smo pokazali, da pravi ideali ne vsebujejo obrnljivih elementov. Ker so v obsegu vsi neničelni elementi obrnljivi, sta $\{0\}$ in R edina ideala v R.

($\Leftarrow$) Naj bo a neničelni element R. Pokazali bomo, da je a obrnljiv. Množica $Ra = \{ra;\ r \in R\}$ je ideal kolobarja R, saj je

$$r_1a - r_2a = (r_1 - r_2)a \in Ra \quad \text{in} \quad \underbrace{r_1r}_{\in R}\, a \in Ra$$

za vse $r_1, r_2, r \in R$. Ker ima R enoto, je $a = 1\cdot a \in Ra$ in zato $Ra \neq \{0\}$. Po predpostavki sledi, da je $Ra = R$. Torej mora obstajati tak $b \in R$, da je $ba = 1$. Od tod sledi, da je $b = a^{-1}$. Pokazali smo, da je poljuben neničeln element kolobarja R obrnljiv. Torej je R obseg. □

Poskusimo sedaj opisati ideal, ki ga generira element $a \in R$. Zanima nas torej, kateri je najmanjši ideal, ki vsebuje a. Vsak ideal, ki vsebuje a, mora vsebovati tudi množico $Ra = \{ra;\ r \in R\}$. V zgornjem dokazu smo videli, da je Ra ideal. Zato je to ideal, generiran z elementom a. Označimo ga z (a). Ideal, ki je generiran z enim elementom imenujemo *glavni ideal*. Kolobar, ki je cel in v katerem so vsi ideali glavni, imenujemo *glavni kolobar*.

Primer 2.14. V kolobarju celih števil $\mathbb{Z}$, opremljenim z običajnim seštevanjem in množenjem, so množice $n\mathbb{Z} = \{nk; k \in Z\}$ podgrupe aditivne grupe $(\mathbb{Z}, +)$. Preverimo, da je to res. Naj bosta $x, y \in n\mathbb{Z}$. Zapišemo ju lahko kot

$$x = nk \quad \text{in} \quad y = nl$$

za neka $k, l \in \mathbb{Z}$. Potem je

$$x - y = nk - nl = n(k - l) \in n\mathbb{Z}.$$

Po lemi 2.6 je množica $n\mathbb{Z}$ res podgrupa v $(\mathbb{Z}, +)$. Množice $n\mathbb{Z}$ so torej kandidati za ideale v kolobarju celih števil. Naj bo $z \in \mathbb{Z}$ in $x = nk \in n\mathbb{Z}$. Potem je

$$zx = znk = nzk \in n\mathbb{Z}.$$

Sledi, da je množica $n\mathbb{Z}$ ideal kolobarja $\mathbb{Z}$. Zlahka preverimo, da je $n\mathbb{Z} = (n)$. Ker so to edini ideali v $\mathbb{Z}$, je $\mathbb{Z}$ glavni kolobar. ♢

2.2. **Kvocientni kolobar.** Kolobar celih števil je osnovni zgled, na katerem temeljijo lastnosti kolobarjev, ki smo jih navedli. Sedaj bomo posplošili pojem kongruentnosti modulo m s kolobarja celih števil na splošen kolobar. Števili a in b sta kongruentni modulo m (imata enak ostanek pri deljenju z m) natanko tedaj, ko je $a - b = mk$ za neki $k \in \mathbb{Z}$ oziroma natanko tedaj, ko je $a - b \in m\mathbb{Z}$.

Definicija 2.15. Naj bo I ideal kolobarja R. Množico

$$r + I = \{r + i; i \in I\}$$

imenujemo *odsek* kolobarja R po idealu I.

Iz enakosti $a + I = b + I$ ne sledi nujno, da je $a = b$. Velja pa naslednja lema.

Lema 2.16. *Naj bo I ideal kolobarja R in $a, b \in R$. Potem je $a + I = b + I$ natanko tedaj, ko je $a - b \in I$.*

Dokaz. ($\Rightarrow$) Vemo, da je $a \in a + I$. Ker je $a + I = b + I$, je $a = b + i$ za neki $i \in I$. Zato je $a - b = i \in I$.

($\Leftarrow$) Predpostavimo, da je $a - b = i \in I$ oziroma $a = b + i$. Torej je

$$a + i_1 = b + \underbrace{i + i_1}_{\in I} \in b + I.$$

Od tod sledi, da je $a + I \subseteq b + I$. Pokazati moramo še, da je $b + I \subseteq a + I$. Naj bo $b + i_1 \in b + I$. Lahko ga preoblikujemo v

$$b + i_1 = \underbrace{b + i}_{=a} \underbrace{-i + i_1}_{\in I} \in a + I.$$

Pokazali smo, da je $b + I \subseteq a + I$. Ko upoštevamo še prejšnji rezultat, dobimo $b + I = a + I$. □

Izrek 2.17. *Naj bo I ideal kolobarja R.* Kvocientni *oziroma* faktorski kolobar *je množica*

$$R/I = \{r + I; r \in R\},$$

na kateri definiramo operacijo seštevanja

(1) $(a + I) + (b + I) := (a + b) + I$
in množenja
(2) $(a + I)(b + I) := ab + I$.

Dokaz. Dokazati moramo, da množica R/I res postane kolobar za tako definirani operaciji. Najprej moramo preveriti dobro definiranost operacij. Če je

$$a + I = a' + I \quad \text{in} \quad b + I = b' + I, \tag{1}$$

mora veljati, da je

$$(a + b) + I = (a' + b') + I \quad \text{in} \tag{2}$$

$$ab + I = a'b' + I. \tag{3}$$

Izraza v (1) lahko zapišemo kot

$$a - a' = x \in I \quad \text{in} \quad b - b' = y \in I.$$

Dokazali bomo, da je $(a + b) - (a' + b') \in I$, kar je ekvivalentno pogoju (2). Ker je seštevanje v kolobarju komutativno, je

$$(a + b) - (a' + b') = (a - a') + (b - b').$$

Ker sta oba sumanda v I, je tudi njuna vsota vsebovana v I. Sledi, da je seštevanje v R/I dobro definirano.

Dokazali bomo še, da je $ab - a'b' \in I$, kar je ekvivalentno pogoju (3). Torej

$$ab - a'b' = ab - (a - x)(b - y) = ab - ab + ay + bx - xy.$$

Sumandi ay, bx in $-xy$ so vsebovani v I, ker je I ideal. Zato je tudi njhova vsota vsebovana v I.

Preveriti moramo še, da operaciji izpolnjujeta lastnosti kolobarskih operacij. Asociativnost in komutativnost seštevanja v R/I sledita iz asociativnosti in komutativnosti v R. Namreč

$$\begin{aligned}((a + I) + (b + I)) + (c + I) &= ((a + b) + I) + (c + I) = ((a + b) + c) + I \\ &= (a + (b + c)) + I = (a + I) + ((b + c) + I) \\ &= (a + I) + ((b + I) + (c + I))\end{aligned}$$

in

$$\begin{aligned}(a + I) + (b + I) &= (a + b) + I = (b + a) + I \\ &= (b + I) + (a + I).\end{aligned}$$

Zlahka preverimo, da je $0 + I = I$ enota za seštevanje in da je odsek $-a + I$ inverz za seštevanje odseka $a + I$. Podobno kot zgoraj dokažemo asociativnost in komutativnost množenja v R/I. Preverimo še, da je odsek $1 + I$ enota za množenje. S tem je izrek dokazan. □

Naj bo $\varphi : R \longrightarrow R'$ homomorfizem kolobarjev. Povedali smo, da je $\operatorname{Ker}(\varphi)$ ideal kolobarja R. Torej lahko tvorimo kvocientni kolobar $R/\operatorname{Ker}(\varphi)$.

Izrek 2.18. *Naj bo $\varphi : R \longrightarrow R'$ homomorfizem kolobarjev. Potem je kolobar $R/\operatorname{Ker}\varphi$ izomorfen kolobarju $\operatorname{Im}\varphi$ ($R/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$).*

Dokaz. Definirajmo preslikavo $\overline{\varphi} : R/\operatorname{Ker}\varphi \longrightarrow \operatorname{Im}\varphi$ s predpisom

$$\overline{\varphi}(a + \operatorname{Ker}\varphi) = \varphi(a)$$

Pokazali bomo, da je preslikava $\overline{\varphi}$ izomorfizem kolobarjev. Najprej preverimo dobro definiranost preslikave. Če je

$$a + \operatorname{Ker}\varphi = a' + \operatorname{Ker}\varphi, \tag{4}$$

mora $\overline{\varphi}$ oba odseka preslikati v isti element. Vzemimo odseka iz enačbe (4). Ker sta enaka, pomeni, da je $a - a' \in \operatorname{Ker}\varphi$. To pa pomeni, da je

$$0 = \varphi(a - a') = \varphi(a) - \varphi(a') \quad \text{oziroma} \quad \varphi(a) = \varphi(a').$$

Pokazali smo, da za enaka odseka velja

$$\overline{\varphi}(a + \operatorname{Ker}\varphi) = \varphi(a) = \varphi(a') = \overline{\varphi}(a' + \operatorname{Ker}\varphi).$$

Preslikava $\overline{\varphi}$ je zato dobro definirana. Sedaj preverimo, da je $\overline{\varphi}$ homomorfizem kolobarjev. Naj bosta $a + \operatorname{Ker}\varphi, b + \operatorname{Ker}\varphi \in R/\operatorname{Ker}\varphi$. Oglejmo si, kam $\overline{\varphi}$ preslika njuno vsoto in produkt.

$$\begin{aligned}\overline{\varphi}((a + \operatorname{Ker}\varphi) + (b + \operatorname{Ker}\varphi)) &= \overline{\varphi}((a+b) + \operatorname{Ker}\varphi) \\ &= \varphi(a+b) = \varphi(a) + \varphi(b) \\ &= \overline{\varphi}(a + \operatorname{Ker}\varphi) + \overline{\varphi}(b + \operatorname{Ker}\varphi)\end{aligned}$$

$$\begin{aligned}\overline{\varphi}((a + \operatorname{Ker}\varphi)(b + \operatorname{Ker}\varphi)) &= \overline{\varphi}(ab + \operatorname{Ker}\varphi) \\ &= \varphi(ab) = \varphi(a)\varphi(b) \\ &= \overline{\varphi}(a + \operatorname{Ker}\varphi)\overline{\varphi}(b + \operatorname{Ker}\varphi)\end{aligned}$$

Preverimo še injektvnost in surjektivnost preslikave $\overline{\varphi}$. Naj bo $a + \operatorname{Ker}\varphi \in \operatorname{Ker}\overline{\varphi}$. To pomeni, da je $\varphi(a) = 0$ oziroma $a \in \operatorname{Ker}\varphi$. Torej je $a + \operatorname{Ker}\varphi = \operatorname{Ker}\varphi$, ki je ničelni elementi v $R/\operatorname{Ker}\varphi$. Pokazali smo, da je $\operatorname{Ker}\overline{\varphi} = \{0\}$, kar pomeni, da je $\overline{\varphi}$ injektivna preslikava.

Surjektivnost je dokaj očitna. Ko element $a \in R$ preteče kolobar R, odseki $a + \operatorname{Ker}\varphi$ pretečejo kvocientni kolobar $R/\operatorname{Ker}\varphi$ in elementi $\varphi(a)$ pretečejo $\operatorname{Im}\varphi$. Preslikava $\overline{\varphi}$ je torej izomorfizem kolobarjev. □

V praksi največkrat poiščemo surjektivni homomorfizem kolobarjev in poiščemo njegovo jedro. Zgornji izrek nam nato pove, da je dobljeni kvocientni kolobar izomorfen kodomeni tega homomorfizma.

Primer 2.19. Množica $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ je kolobar za binarni operaciji, definirani s predpisoma

$$\overline{k} + \overline{l} := \text{ ostanek pri deljenju } k + l \text{ z } n$$

in

$$\overline{k} \cdot \overline{l} := \text{ ostanek pri deljenju } k \cdot l \text{ z } n.$$

Dokaz tega dejstva prepuščamo bralcu. Oglejmo si preslikavo $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_2$ s predpisom

$$\varphi(n) = \begin{cases} \overline{0}; & n \text{ sodo število} \\ \overline{1}; & n \text{ liho število} \end{cases}$$

Zlahka preverimo, da je preslikava φ homomorfizem kolobarjev. Jedro homomorfizma φ je množica $2\mathbb{Z} = \{2n; n \in \mathbb{Z}\}$. Homomorfizem φ je surjektiven, saj je $\varphi(0) = \overline{0}$ in $\varphi(1) = \overline{1}$. Po izreku 2.18 sledi, da je $\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2$. ♢

2.3. **Maksimalni ideali in nerazcepnost.**

Definicija 2.20. Ideal M kolobarja R je *maksimalen*, če ni enak celotnemu kolobarju ($M \neq R$) in če ne obstaja tak ideal I, da bi veljalo $M \subsetneq I \subsetneq R$.

Izrek 2.21. *Naj bo R kolobar in M njegov ideal, ki ni enak celotnemu kolobarju ($M \neq R$). Potem je M maksimalen natanko tedaj, ko je množica R/M obseg.*

Dokaz. Po izreku 2.13 vemo, da je R/M obseg natanko tedaj, ko sta $\{0\} = M$ in R/M njegova edina ideala.

($\Rightarrow$) Naj bo I ideal kolobarja R/M. Definirajmo množico

$$J := \{x \in R; x + M \in I\}.$$

Množica J je ideal kolobarja R, saj velja

(1) Če sta $x, y \in J$, sta odseka $x + M$ in $y + M$ vsebovana v I. Zato je odsek

$$(x - y) + M = (x + M) + (-y + M)$$

element ideala I. Sledi, da je $x - y \in J$ in zato je J Abelova podgrupa kolobarja R.

(2) Naj bo $x + M \in I$ in $r \in R$. Ker je I ideal kolobarja R/M, je

$$rx + M = (r + M)(x + M) \in I.$$

Od tod sledi, da je $rx \in J$ in je množica J zaprta za množenje z elementi kolobarja R.

Naj bo $m \in M$. Potem je odsek $m + M = M$ in zato vsebovan v idealu I. Sledi, da je $m \in J$. Torej velja $M \subseteq J \subseteq R$. Ker je M maksimalen ideal, mora veljati bodisi $J = M$ bodisi $J = R$. Če je $J = M$, je $I = \{M\} = \{0\}$, saj je $m + M = M$ za vse $m \in M$. Če je $J = R$, je $I = R/M$. Pokazali smo, da kolobar R/M nima pravih idealov. Po izreku 2.13 sledi, da je R/M obseg.

($\Leftarrow$) Predpostavimo, da R/M nima pravih idealov in dokažimo, da mora biti M maksimalen ideal. Naj bo J ideal kolobarja R, ki vsebuje M ($M \subseteq J \subseteq R$). Dokažimo, da je J/M ideal kolobarja R/M.

(1) Naj bosta $a + M, b + M \in J/M$. Element $a - b$ je vsebovan v množici J, saj je J ideal kolobarja R. Torej je odsek $(a - b) + M$ vsebovan v J/M.

(2) Naj bo $r + M \in R/M$ in $a + M \in J/M$. Element ra je vsebovan v J, saj je J ideal. Sledi, da je odsek

$$ra + M = (r + M)(a + M)$$

vsebovan v J/M.

Ker smo predpostavili, da sta $\{0\}$ in R/M edina ideala kolobarja R/M, mora biti J/M enak enemu od njiju. Če je $J/M = \{0\}$, mora biti $J = M$, saj za vse elemente $m \in M$ velja $m + M = M$. Če je $J/M = R/M$, je vsak odsek $x + M \in R/M$ enak nekemu odseku $j + M \in J/M$. Torej je $x + M = j + M$, kar pomeni, da je $x - j = m \in M$. Ker je $M \subseteq J$, je $j + m = x \in J$. Vsak element kolobarja R je torej tudi element kolobarja J. Kar pomeni, da je $J = R$.

Ker med idealom M in kolobarjem R ni nobenega pravega ideala, je M maksimalen ideal kolobarja R. □

Primer 2.22. V kolobarju celih števil $\mathbb{Z}$ so maksimalni tisti ideali, ki jih generira število $\pm p$, kjer je p praštevilo, tj. ideali oblike $p\mathbb{Z} = (p)$. Preverimo to trditev. Naj bo $(p) \subseteq (n) \subseteq \mathbb{Z}$. Od tod sledi, da je $p \in (n)$. Torej je $p = kn$ za neki $k \in \mathbb{Z}$, kar pomeni, da n deli p. Ker je p praštevilo, je bodisi $n = 1$ bodisi je $n = p$. V prvem primeru je $(n) = (1) = \mathbb{Z}$, v drugem primeru pa je $(n) = (p)$. Torej je ideal (p) res maksimalen. ♢

Videli smo, da v kolobarju celih števil obstaja močna povezava med praštevili in maksimalnimi ideali. Zato pojem praštevila posplošimo in definiramo nerazcepne elemente poljubnega kolobarja.

Definicija 2.23. Naj bo p element kolobarja R. Pravimo, da je p *nerazcepen*, če izpolnjuje naslednja pogoja

(1) $p \neq 0$ in p ni obrnljiv,

(2) če je $p = ab$, je bodisi a obrnljiv bodisi b obrnljiv.

V kolobarju celih števil praštevila generirajo maksimalne ideale. Analogno lahko za glavne kolobarje dokažemo naslednji izrek.

Izrek 2.24. *Naj bo p element glavnega kolobarja R. Naj bo $p \neq 0$ in neobrnljiv. Pri teh predpostavkah so naslednje trditve ekvivalentne.*

(1) Element p je nerazcepen.
(2) Ideal (p) je maksimalen v kolobarju R.
(3) Množica $R/(p)$ je obseg.

Dokaz. Ekvivalenca točk (2) in (3) je že dokazana, saj je to natanko trditev izreka 2.21. Dokažimo še ekvivalenco točk (1) in (2).

(2) $\Rightarrow$ (1) Naj bo (p) maksimalen ideal kolobarja R. Pokazati moramo, da je element p nerazcepen. Ker je ideal (p) maksimalen, vemo, da p ni obrnljiv. Zato je bodisi nerazcepen bodisi razcepen in neobrnljiv. Recimo, da je $p = ab$ in sta oba elementa a in b neobrnljiva. Potem je ideal $(p) \subseteq (a)$. Ker je ideal (p) maksimalen, mora biti bodisi $(a) = (p)$ bodisi $(a) = R$. Videli bomo, da pri obeh možnostih pride do konflikta s predpostavko, da sta elementa a in b neobrnljiva. Od tod bo sledilo, da mora biti element p nerazcepen.

(1) Recimo, da je $(a) = (p)$. Potem je $a \in (p)$, kar pomeni, da je $a = kp$ za neki $k \in R$. A od tod sledi, da je

$$a = kp = kab \quad \text{oziroma} \quad kb = 1 \quad \text{oziroma} \quad k = b^{-1}.$$

To je v nasprotju s predpostavko, da b ni obrnljiv, zato ideala (p) in (a) ne moreta biti enaka.

(2) Recimo, da je $(a) = R$. To pomeni, da je $1 \in (a)$, kar pomeni, da je $1 = ra$ za neki $r \in R$. To pa pomeni, da je a obrnljiv in $k = a^{-1}$, kar nasprotuje predpostavki, da je a neobrnljiv.

Torej mora biti element p nerazcepen.

(1) $\Rightarrow$ (2) Pokazati moramo, da vsak nerazcepen element p generira maksimalni ideal (p). Ker element p ni obrnljiv, vemo, da $1 \notin (p)$ in zato $(p) \neq R$ (enak razmislek smo naredili v zgornjem delu dokaza). Naj bo torej ideal $(p) \subseteq (a)$. Potem je $p = ab$ za neki $b \in R$. Ker je p nerazcepen, mora biti bodisi a obrnljiv bodisi b obrnljiv. Če je element a obrnljiv, je ideal $(a) = R$. Če je element b obrnljiv, je ideal $(b) = Rb = R$ in velja

$$(p) = Rp = Rba = Ra = (a).$$

Sledi, da ideal $(p) \neq R$ in v kolobarju R ni ideala (a), za katerega bi veljalo $(p) \subsetneq (a)$. Torej je ideal (p) maksimalen. □

2.4. **Kolobarji polinomov.** V tem poglavju bomo definirali kolobar polinomov nad obsegom F. Izpeljali bomo še osnovni izrek o deljenju polinomov in pokazali, da je kolobar polinomov nad obsegom glavni kolobar. V naslednjem poglavju bomo videli, da sta ti dve lastnosti polinomov ključnega pomena pri študiju razširitev obsegov.

Izrek 2.25. *Označimo s $F[x]$ množico vseh zaporedij $(a_0, a_1, \ldots)$, kjer je $a_i \in F$ za vsak $i \in \mathbb{N}_0$ in je le končno mnogo elementov a_i različnih od 0. Množica $F[x]$ postane kolobar, če na njej definiramo binarni operaciji seštevanja in množenja na sledeč način*

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) := (a_0 + b_0, a_1 + b_1, \ldots) \tag{5}$$

in

$$(a_0, a_1, \ldots)\cdot(b_0, b_1, \ldots) := (c_0, c_1, \ldots) \tag{6}$$

kjer je

$$c_n = \sum_{i=0}^{n} a_{n-i}b_i = \sum_{i+j=n} a_i b_j = a_n b_0 + a_{n-1}b_1 + \cdots + a_1 b_{n-1} + a_0 b_n.$$

Kolobar $F[x]$ imenujemo kolobar polinomov *nad obsegom F, njegove elemente pa polinomi nad obsegom F.*

Dokaz. Ker je F obseg, so vse komponente zaporedja $(a_0 + b_0, a_1 + b_1, \ldots)$ elementi obsega F. Prav tako so vse komponente zaporedja $(c_0, c_1, \ldots)$ elementi obsega F. Sledi, da je množica $F[x]$ zaprta za operaciji seštevanja in množenja, definirani v izrazih (5) in (6). Ker smo seštevanje polinomov definirali po komponentah, asociativnost in komutativnost seštevanja sledita iz asociativnosti in komutativnosti seštevanja v obsegu F. Zlahka preverimo, da je polinom $(0, 0, \ldots)$ enota za seštevanje v $F[x]$ in da je $-(a_0, a_1, \ldots) = (-a_0, -a_1, \ldots)$. Sledi, da je množica $F[x]$ Abelova grupa za seštevanje, definirano v enačbi (5).

Dokažimo asociativnost množenja. Naj bodo $(a_0, a_1, \ldots), (b_0, b_1, \ldots)$ in $(c_0, c_1, \ldots)$ polinomi v $F[x]$. Označimo

$$((a_0, a_1, \ldots)(b_0, b_1, \ldots))(c_0, c_1, \ldots) = (d_0, d_1, \ldots)$$

in

$$(a_0, a_1, \ldots)((b_0, b_1, \ldots)(c_0, c_1, \ldots)) = (e_0, e_1, \ldots).$$

Dokažimo, da je $d_n = e_n$ za vsak $n \in \mathbb{N}_0$. Velja

$$d_n = \sum_{i=0}^{n}\left(\sum_{j=0}^{n-i} a_{n-i-j}b_j\right)c_i = \sum_{i=0}^{n}\sum_{j=0}^{n-i} a_{n-i-j}b_j c_i = \sum_{i+j+k=n} a_i b_j c_k$$

in

$$e_n = \sum_{i=0}^{n} a_{n-i}\left(\sum_{j=0}^{i} b_{i-j}c_j\right) = \sum_{i=0}^{n}\sum_{j=0}^{n-i} a_{n-i}b_{i-j}c_j = \sum_{i+j+k=n} a_i b_j c_k.$$

Sledi, da je res $d_n = e_n$ za vsak $n \in \mathbb{N}_0$. Torej je množenje na množici $F[x]$ definirano z enačbo (6) asociativno. Uganemo, da je enota za množenje polinom $(1, 0, \ldots)$, in to še preverimo. Označimo

$$(1, 0, \ldots) = (e_0, e_1, \ldots) \quad \text{in} \quad (a_0, a_1, \ldots)(e_0, e_1, \ldots) = (f_0, f_1, \ldots)$$

ter izračunajmo

$$f_n = \sum_{i=0}^{n} a_{n-i}e_i = a_n e_0 + a_{n-1}e_1 + \cdots + a_0 e_n = a_n\cdot 1 = a_n.$$

Dokazali smo, da je množica $F[x]$ res kolobar za binarni operaciji definirani z enačbama (5) in (6). □

Prevedimo zgornjo notacijo v bolj prepoznavno obliko. Polinome oblike $(a, 0, \ldots)$ označimo krajše z a. Označimo element $(0, 1, 0, \ldots)$ kolobarja $F[x]$ z x. Preverimo lahko, da za vsako število $n \in \mathbb{N}_0$ velja

$$x^n = \underbrace{x\cdot x\cdots x}_{n-krat} = (0, \ldots, 0, 1, 0, \ldots),$$

kjer je enica na komponenti $n+1$. Naj bo $f = (a_0, a_1, \ldots) \in F[x]$. Z zgornjima oznakama lahko f zapišemo kot

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

kjer je n največji indeks i, pri katerem je $a_i \neq 0$. Če želimo poudariti, da je f polinom v spremenljivki X, ga lahko označimo z $f(X)$. Navedimo še nekaj terminologije. Naj bo polinom f definiran kot zgoraj. Elemente a_i obsega F imenujemo *koeficienti* polinoma. Element a_n je *vodilni koeficient*, število n pa je *stopnja polinoma* f. Oznaka za stopnjo polinoma f je $\mathrm{st}(f)$. Polinomu $0 = (0, 0, \ldots)$ ne določimo stopnje. Če je vodilni koeficient enak 1, pravimo, da je f *moničen polinom*. Polinome oblike $(a, 0, \ldots)$ imenujemo *konstantni polinomi*.

Oglejmo si, kateri polinomi kolobarja $F[x]$ so obrnljivi. Če je polinom f konstanten, tj. $f = (a, 0 \ldots)$, je njegov inverz $f^{-1} = (a^{-1}, 0, \ldots)$, ki je polinom v $F[x]$, saj je F obseg. Naj bo sedaj $f = (a_0, a_1, \ldots)$ polinom stopnje $n \geq 1$ in recimo, da je polinom $g = (b_0, b_1, \ldots)$ stopnje $m \geq 0$ njegov inverz. Stopnja polinoma fg je vsaj 1, vodilni koeficient pa je $a_n b_m$. Predpostavili smo, da je $fg = 1$, od koder sledi, da mora biti $a_n b_m = 0$. Ker je F obseg, sledi, da je $b_m = 0$, saj je polinom f stopnje n in zato $a_n \neq 0$. To je v nasprotju s predpostavko o stopnji polinoma g in zato polinom f nima inverza. Pokazali smo, da nekonstantni polinomi niso obrnljivi.

Iz zgoraj dokazanega potegnemo še en sklep. Če lahko polinom $f \in F[x]$ zapišemo kot produkt dveh nekonstantnih polinomov iz $F[x]$, potem je polinom f razcepen. To dejstvo bomo kasneje večkrat potrebovali.

Dokažimo sedaj še, da je kolobar polinomov nad obsegom glavni kolobar in pa osnovni izrek o deljenju polinomov.

Lema 2.26. *Naj bo $F[x]$ kolobar polinomov nad obsegom F. Kolobar $F[x]$ je cel (nima deliteljev niča).*

Dokaz. Naj bosta $f = (a_0, a_1, \ldots)$ in $g = (b_0, b_1, \ldots)$ neničelna polinoma v kolobarju $F[x]$. Naj bo $\mathrm{st}(f) = n$ in $\mathrm{st}(g) = m$, torej $a_n \neq 0$ in $b_m \neq 0$. Vodilni koeficient polinoma fg je $a_n b_m$. Če bi bil produkt $fg = 0$, bi moral biti $a_n = 0$ ali $b_m = 0$, saj je F obseg in zato cel. To pa je v nasprotju s predpostavko o stopnjah polinomov f in g. Sledi, da je kolobar $F[x]$ cel. □

Izrek 2.27. *Za vsaka polinoma $f(x), g(x) \in F[x]$, pri čemer $g(x) \neq 0$, obstajata taka polinoma $q(x)$ in $r(x) \in F[x]$, da velja*

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

kjer je $\mathrm{st}(r) < \mathrm{st}(g)$ ali pa je $r(x) = 0$.

Dokaz. Naj bo

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m \quad \text{in} \quad a_m \neq 0$$

ter

$$g(x) = b_0 + b_1 x + \cdots + b_n x^n \quad \text{in} \quad b_n \neq 0.$$

Če je $m < n$, je $f(x) = 0 \cdot g(x) + f(x)$.

Z indukcijo dokažimo izrek za primere, ko je $m \geq n$. Če je $m = 0$, mora biti tudi $n = 0$. V tem primeru sta polinoma $f(x)$ in $g(x)$ konstantna in zato velja

$$f(x) = (f(x)g(x)^{-1})g(x) + 0 = (a_0 b_0^{-1})b_0 + 0.$$

Dokažimo še indukcijski korak. Predpostavimo, da izrek velja za vse polinome stopnje $m-1$ in dokažimo, da potem velja tudi za polinome stopnje m. Izračunamo lahko, da je

$$\frac{a_m}{b_n} x^{m-n} g(x) = \frac{a_m}{b_n} b_0 x^{m-n} + \cdots + a_m x^m.$$

Definirajmo polinom

$$h(x) := f(x) - \frac{a_m}{b_n} x^{m-n} g(x).$$

Opazimo, da je $\mathrm{st}(h) < m$. Zato je po indukcijski predpostavki

$$h(x) = q_1(x)g(x) + r(x),$$

kjer je $\mathrm{st}(r) < \mathrm{st}(g)$ ali pa je $r = 0$. Ta zapis polinoma h vstavimo v zgornjo enačbo in dobimo

$$\begin{aligned} f(x) &= h(x) + \frac{a_m}{b_n} x^{m-n} g(x) \\ &= q_1(x)g(x) + r(x) + \frac{a_m}{b_n} x^{m-n} g(x) \\ &= \underbrace{(q_1(x) + \frac{a_m}{b_n} x^{m-n})}_{:=q(x)} g(x) + r(x). \end{aligned}$$

□

Izrek 2.28. *Kolobar $F[x]$ je glavni.*

Dokaz. Z lemo 2.26 smo dokazali, da je kolobar $F[x]$ cel. Torej moramo dokazati le še, da je vsak ideal kolobarja $F[x]$ glavni. Naj bo I ideal kolobarja $F[x]$. Če je $I = \{0\}$, lahko rečemo, da je $I = (0)$. V nasprotnem primeru $I \neq \{0\}$, zato so v njem tudi neničelni polinomi. Izberimo neničelni polinom $g(x) \in I$, ki ima med vsemi polinomi v I najnižjo stopnjo. Pokazali bomo, da je $I = (g(x))$. Ker je I ideal in je $g(x) \in I$, je ideal $(g(x))$ tudi vsebovan v I.
Pokažimo še vsebovanost $I \subseteq (g(x))$. Naj bo polinom $f(x) \in I$. Iz osnovnega izreka o deljenju polinomov sledi, da lahko $f(x)$ zapišemo v obliki

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

kjer je $\mathrm{st}(r) < \mathrm{st}(g)$ ali pa je $r = 0$. Sledi, da je polinom $r(x) \in I$, saj je

$$r(x) = f(x) - q(x)g(x).$$

Ker smo polinom $g(x)$ izbrali tako, da ima najnižjo stopnjo izmed vseh polinomov v I, mora biti $r(x) = 0$. Torej je $f(x) = q(x)g(x) \in (g(x))$. Pokazali smo, da je $I \subseteq (g(x))$. □

2.5. **Vektorski prostori in razširitve obsegov.** V tem poglavju bomo definirali pojem vektorskega prostora nad obsegom in njegove lastnosti. Te bodo ključnega pomena pri dokazovanju najpomembnejšega izreka te naloge. Ta izrek bo glavno orodje, s katerim bomo lahko ugotavljali, katera števila so konstruktibilna in katera niso.

Definicija 2.29. Abelova grupa $(V, +)$ je *vektorski prostor* nad obsegom F, če obstaja preslikava $f : F \times V \longrightarrow V$ s predpisom $f(\lambda, v) = \lambda v$, za katero veljajo naslednje lastnosti:

(1) $(\lambda + \mu)v = \lambda v + \mu v$
(2) $\lambda(v + w) = \lambda v + \lambda w$
(3) $(\lambda\mu)v = \lambda(\mu v)$
(4) $1v = v$

za vse $\lambda, \mu \in F$ in vse $v, w \in V$. Preslikavo oziroma operacijo f imenujemo *množenje s skalarji*.

Vsoto oblike

$$\lambda_1 x_1 + \ldots + \lambda_n x_n$$

imenujemo *linearna kombinacija* elementov $x_1, x_2, \ldots, x_n$. Podmnožica X vektorskega prostora V nad F je *linearno neodvisna*, če velja: če so $x_1, x_2, \ldots, x_n \in X$, $\lambda_1, \lambda_2, \ldots, \lambda_n \in F$ in je

$$\lambda_1 x_1 + \ldots + \lambda_n x_n = 0,$$

potem je $\lambda_1 = \lambda_2 = \ldots = \lambda_n = 0$. Množica, ki ni linearno neodvisna, je *linearno odvisna*. Pravimo, da množica X *razpenja* (je ogrodje) vektorskega prostora V, če lahko vsak element prostora V zapišemo kot linearno kombinacijo elementov iz X. To pomeni, da je

$$V = \{\lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_n x_n;\ \lambda_i \in F,\ x_i \in X\}.$$

Množici X, ki hkrati razpenja vektorski prostor V in je linearno neodvisna, pravimo *baza* prostora V.

Izrek 2.30. *Naj bo V vektorski prostor nad obsegom F. Naj ima V bazo X, ki ima končno mnogo elementov ($|X| = n \in \mathbb{N}$). Potem ima vsaka baza prostora V enako število elementov kot X.*

Dokaz. Naj bosta X in Y bazi prostora V. Označimo

$$X = \{x_1, x_2, \ldots, x_n\}$$

in

$$Y = \{y_1, y_2, \ldots, y_m\}.$$

Ker sta to bazi, lahko zapišemo

$$0 \neq y_m = \lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_n x_n.$$

Ker $y_m \neq 0$, je vsaj eden od $\lambda_i \neq 0$. Recimo, da $\lambda_j \neq 0$. Sledi:

$$x_j = \lambda_j^{-1} y_m - \lambda_j^{-1}\lambda_1 x_1 - \lambda_j^{-1}\lambda_2 x_2 - \ldots - \lambda_j^{-1}\lambda_n x_n.$$

Torej množica $\{y_m, x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n\}$ razpenja V. Sedaj lahko zapišemo

$$y_{m-1} = s_m y_m + \mu_1 x_1 + \ldots + \mu_{j-1} x_{j-1} + \mu_{j+1} x_{j+1} + \ldots + \mu_n x_n.$$

Če bi bili vsi $\mu_i = 0$, bi bilo $y_{m-1} - s_m y_m = 0$, kar pa je v nasprotju s predpostavko, da je množica Y baza. Naj bo $\mu_k \neq 0$. Enak razmislek kot prej nas pripelje do sklepa, da množica $\{y_m, y_{m-1}\} \cup \{x_i;\ i \neq j, k\}$ razpenja V.
Recimo, da je $n < m$. Po n korakih tega procesa ugotovimo, da množica

$$\{y_m, y_{m-1}, \ldots, y_{m-n+1}\}$$

razpenja V. Ker je $n < m$, je $m - n + 1 \geq 2$. To pa je v nasprotju s predpostavko, da je množica Y linearno neodvisna. Torej mora biti $m \leq n$.

Če zamenjamo vlogi množic X in Y, lahko naredimo podoben sklep. Dobimo neenakost $n \leq m$. Sledi, da mora biti $n = m$. □

Pokazali smo, da imajo vse baze vektorskega prostora V nad obsegom F enako število elementov. Zato lahko *dimenzijo* vektorskega prostora definiramo kot moč neke baze tega prostora. Označimo jo z $\dim_F(V)$.

Oglejmo si naslednjo situacijo: naj bo K podobseg v obsegu F. Gledano obratno, pravimo, da je F *razširitev* obsega K. Ali lahko F gledamo kot vektorski prostor nad K? Če za množenje s skalarji vzamemo kar množenje v obsegu F, dobimo

$$f : K \times F \to F \quad \text{s predpisom} \quad f(\lambda, x) = \lambda x.$$

Element λx je v obsegu F, saj je obseg zaprt za množenje in je $\lambda \in K \subseteq F$. Lastnosti (1) in (2) iz definicije 2.29 sledita iz distributivnostnih zakonov, lastnost (3) pa je posledica asociativnosti množenja v obsegu. Lastnost (4) je izpolnjena, saj je enota v K ista kot enota v F.

Obseg F je torej vektorski prostor nad svojim podobsegom K. Zato lahko govorimo o dimenziji obsega F nad K. Kaj pa, če imamo zaporedje razširitev obsegov $K \subseteq H \subseteq F$? Ali lahko v tem primeru kaj povemo o povezavi med

$$\dim_H(F), \dim_K(F) \quad \text{in} \quad \dim_K(H)?$$

Izrek 2.31. *Naj bodo $K \subseteq H \subseteq F$ obsegi. Velja:* $\dim_K(F) = \dim_H(F) \dim_K(H)$.

Opomba 2.32. Kadar govorimo o razširitvah obsegov, je pogosteje uporabljena oznaka $[F : K] = \dim_K(F)$. Zgornji izrek torej pravi: $[F : K] = [F : H][H : K]$.

Dokaz. Naj bo X baza prostora H nad K in Y baza prostora F nad H. Pokazali bomo, da je $XY = \{xy; x \in X, y \in Y\}$ baza prostora F nad K.
Vzemimo $f \in F$.

$$f = \sum_j h_j y_j = \sum_j \left(\sum_i k_{ij} x_i \right) y_j = \sum_j \sum_i k_{ij} x_i y_j,$$

kjer so $h_j \in H$ in $k_{ij} \in K$. Torej množica XY razpenja vektorski prostor V nad K.
Dokažimo še linearno neodvisnost množice XY. Naj bo

$$0 = \sum_j \sum_i k_{ij} x_i y_j = \sum_j \left(\sum_i k_{ij} x_i \right) y_j.$$

Ker je množica Y linearno neodvisna, sledi, da je

$$\sum_i k_{ij} x_i = 0$$

za vse indekse j. Ker je množica X linearno neodvisna, sledi, da so vsi $k_{ij} = 0$. □

Recimo, da je F razširitev obsega K in $a \in F$. Zanima nas, kateri je najmanjši obseg, ki vsebuje a in K. Oglejmo si homomorfizem kolobarjev $\varphi_a : K[x] \to F$ s predpisom $\varphi_a(x) = a$. Ker je to homomorfizem kolobarjev, velja $\varphi_a(p) = p(a)$, kjer je $p \in K[x]$. Slika tega homomorfizma je

$$\mathrm{Im}(\varphi_a) = \{p(a);\ p \in K[x]\}.$$

Označimo jo s $K[a]$. Slika homomorfizma je vedno podkolobar kodomene, zato je $K[a]$ podkolobar F. Preverimo lahko tudi, da je to najmanjši podkolobar F, ki vsebuje K in a.

Res: $a \in K[a]$, saj je $p(x) = x \in K[x]$. Če je H kolobar, ki vsebuje K in a, mora vsebovati tudi vse potence a, saj je kolobar zaprt za množenje. Podobno lahko sklepamo, da so v H vsi elementi oblike ka^n za $k \in K$ in tudi vse končne vsote takih elementov. Sledi, da je $K[a] \subseteq H$. Torej je $K[a]$ najmanjši podkolobar F, ki vsebuje K in a. Kolobar $K[a]$ v splošnem ni obseg, saj niso vsi njegovi elementi obrnljivi. Podobno kot zgoraj, pa lahko pokažemo, da je množica racionalnih funkcij nad K, evaluiranih v a, najmanjši podobseg F, ki vsebuje K in a. To je

$$\left\{ p(a)q^{-1}(a) = \frac{p(a)}{q(a)};\ p, q \in K[x], q(a) \neq 0 \right\} =: K(a).$$

Vrnimo se sedaj k homomorfizmu φ_a. Oglejmo si, kaj se zgodi, če je a ničla kakega polinoma iz $K[x]$ (pravimo, da je tak *a algebraičen* nad K). To pomeni, da φ_a slika neničelni polinom v 0. Torej φ_a ni injektiven, zato ima netrivialno jedro. Jedro homomorfizma je vedno ideal v definicijskem območju, torej je $\mathrm{Ker}(\varphi_a)$ ideal kolobarja $K[x]$. Ker je $K[x]$ glavni kolobar, je vsak njegov ideal generiran z enim elementom. Torej obstaja $g \in K[x]$, da je $\mathrm{Ker}(\varphi_a) = (g)$. Vemo, da ima g med vsemi polinomi v $\mathrm{Ker}(\varphi_a)$ najnižjo stopnjo. Preverimo še, da je g nerazcepen polinom nad $K[x]$. Recimo, da je g razcepen. To pomeni, da ga lahko zapišemo kot $g(x) = p(x)q(x)$, kjer sta $p, q \in K[x]$ in imata nižjo stopnjo od g. Sledi:

$$g(a) = 0 = p(a)q(a).$$

Ker je K cel (nima deliteljev niča), mora biti $p(a) = 0$ ali $q(a) = 0$. To pomeni, da je eden od njiju v $Ker(\varphi_a)$, kar pa je v nasprotju z dejstvom, da ima g najnižjo stopnjo v $Ker(\varphi_a)$. Po izreku 2.24 vemo, da je $K[x]/(g)$ obseg. Po izreku 2.18 o izomorfizmih pa vemo tudi, da je $K[x]/(g) \cong K[a]$. Torej je tudi $K(a) \cong K[a]$.

Povzemimo zadnjih nekaj ugotovitev. Če je F razširitev obsega K in $a \in F$ ničla kakega polinoma iz $K[x]$, je $K[x]/(g)$ obseg, ki je izomorfen $K[a]$ (oba sta izomorfna tudi obsegu $K(a)$). Vemo, da je $K(a)$ vektorski prostor nad K. Ali lahko določimo bazo tega prostora?

Recimo, da je $\mathrm{st}(g) = n$. Trdimo, da je množica

$$X = \{1 + (g), x + (g), \ldots, x^{n-1} + (g)\}$$

baza $K[x]/(g)$ nad K. Dokažimo najprej linearno neodvisnost te množice. Vsaka linearna kombinacija elementov iz X je oblike $p(x) + (g)$, kjer je $st(p) < n$. Če je

$$p(x) + (g) = 0 = 0 + (g),$$

morajo biti vsi koeficienti polinoma p enaki 0. Torej je množica X linearno neodvisna. Dokažimo še, da je množica X ogrodje vektorskega prostora $K[x]/(g)$ nad K. Vsak polinom $p \in K[x]$ lahko zapišemo kot

$$p(x) = \underbrace{k(x)g(x)}_{\in(g)} + r(x); st(r) < n.$$

Polinom r je torej linearna kombinacija elementov iz X, zato X razpenja $K[x]/(g)$. Ker je $K[x]/(g) \cong K(a)$, lahko bazne elemente iz množice X z izomorfizmom preslikamo v bazo prostora $K(a)$. Ugotovimo, da je množica $\{1, a, \ldots, a^{n-1}\}$ baza vektorskega prostora $K(a)$ nad K. Strnimo te ugotovitve še v izrek.

Izrek 2.33. *Naj bo F razširitev obsega K in $a \in F$ algebraičen nad K. Pri teh predpostavkah veljajo naslednje trditve.*

(1) Obstaja natanko en monični polinom $g \in K[x]$, ki ima ničlo v a in deli vse polinome, ki imajo ničlo v a. Imenujemo ga minimalni polinom *za a nad K.*
(2) $K(a) \cong K[a] \cong K[x]/(g)$.
(3) $[K(a) : K] = st(g)$. Za bazo vektorskega prostora $K(a)$ nad K lahko vzamemo $\{1, a, \ldots, a^{n-1}\}$. Številu $[K(a) : K]$ pravimo stopnja razširitve *obsega $K(a)$ nad K.*

Namesto o stopnji minimalnega polinoma za a nad K, lahko govorimo kar o stopnji a nad K: $[K(a) : K] = st(g) = st_K(a)$.

Izrek 2.34. *Če je F končna razširitev K, potem za vsak $a \in F$ velja:*

$$st_K(a) | [F : K].$$

(Stopnja a nad K deli stopnjo razširitve F nad K.)

Dokaz. To sledi direktno iz izreka 2.31. Naj bo $[F : K] = n$.

$$n = [F : K] = [F : K(a)] \underbrace{[K(a) : K]}_{=st_K(a)}.$$

□

Primer 2.35. Naj bo $[F : K] = 2$ in $a \in F \setminus K$. Stopnja a nad K deli 2, torej imamo dve možnosti. Recimo, da je $\mathrm{st}_K(a) = 1$. V tem primeru je a ničla linearnega polinoma s koeficienti v K. Minimalni polinom za a je $p(x) = x - a$. To pa pomeni, da je $a \in K$, kar je v nasprotju našo predpostavko.

Torej mora biti $\mathrm{st}_K(a) = 2$. Torej je

$$\underbrace{[F : K]}_{=2} = \underbrace{[F : K(a)]}_{\text{mora biti } =1} \underbrace{[K(a) : K]}_{=2}$$

To pa pomeni, da je $F = K(a)$. ♢

3. Konstrukcije z ravnilom in šestilom

Vsebina tega poglavja je povzeta po viru [3]. Najprej bomo definirali konstruktibilne točke. Nato bomo izpeljali izrek, ki za vsako točko pove, ali je konstruktibilna ali ni. Posledica tega izreka je med drugim tudi ta, da so tri starogrške konstrukcije, ki so bile omenjene v uvodnem poglavju, nemogoče. Da bomo to lahko pokazali, moramo najprej natančno definirati problem.

Pri reševanju starogrških problemov smemo uporabljati le šestilo in ravnilo brez oznak. Torej, če imamo dani različni točki A in B, lahko z ravnilom narišemo premico skozi ti dve točki. Označimo jo z $L(A, B)$. S šestilom pa lahko narišemo krožnico s središčem v eni izmed teh dveh točk, druga točka pa leži na krožnici. Krožnico s središčem v A, ki vsebuje B, bomo označili s $C(A; B)$. Točke, ki ležijo v preseku dveh takih premic, premice in krožnice ali dveh krožnic, bomo imenovali *konstruktibilne točke.*

Za začetek bomo v ravnino $\mathbb{R}^2$ vpeljali koordinatni sistem. Izberimo si dve različni točki v ravnini, A in $\overline{A}$. Premica, na kateri ležita ti dve točki, bo naša abscisna os. S

šestilom narišemo krožnici $C(A;\overline{A})$ in $C(\overline{A};A)$, ki se sekata v dveh točkah. Premica skozi ti dve novi točki bo naša ordinatna os, presečišče abscisne osi z ordinatno osjo pa izhodišče O. Dolžina daljice $|OA|$ bo naša enota 1. Sedaj lahko natančno definiramo konstruktibilna števila.

Definicija 3.1. Naj bodo E, F, G in H (ne nujno različne) točke v ravnini. Točka Z je *konstruktibilna iz točk* E, F, G in H, če je izpolnjena ena od trditev

(1) $Z \in L(E,F) \cap L(G,H)$, kjer $L(E,F) \neq L(G,H)$,
(2) $Z \in L(E,F) \cap C(G;H)$,
(3) $Z \in C(E;F) \cap C(G;H)$, kjer $C(E;F) \neq C(G;H)$.

Točka Z je *konstruktibilna*, če je $Z = A$ ali $Z = \overline{A}$ ali pa obstajajo točke $P_1, \ldots P_n$, kjer je $Z = P_n$ in je P_{j+1} konstruktibilna iz točk v množici $\{A, \overline{A}, P_1, \ldots, P_j\}$ za vse $j \geq 0$.

V nadaljevanju bomo ravnino $\mathbb{R}^2$ identificirali z množico kompleksnih števil $\mathbb{C}$. Na ta način bomo lažje formulirali izreke v tem poglavju.

Definicija 3.2. Kompleksno število $z = a + ib$ je *konstruktibilno*, če je konstruktibilna točka (a, b). Realno število x je *konstruktibilno*, če je konstruktibilna točka $(x, 0)$.

Preden se lotimo iskanja konstruktibilnih točk, si oglejmo dve konstrukciji, ki ju bomo kasneje večkrat uporabili.

(1) *Konstrukcija simetrale dane daljice.*
Naj bosta A in B različni točki in $L(A,B)$ premica, ki jo ti dve točki določata. V množici $C(A;B) \cap C(B;A)$ sta natanko dve točki S_1 in S_2. Premica $L(S_1, S_2)$ je simetrala daljice $|AB|$.

(2) *Konstrukcija vzporednice h konstruktibilni premici skozi dano točko A.*
Naj bo $L(P,Q)$ dana premica. Izberimo tisto izmed točk P in Q, ki ni pravokotna projekcija točke A na premico $L(P,Q)$. Ker sta točki različni, vsaj ena od njiju ustreza temu pogoju. Recimo, da je to točka P. Konstruiramo krožnico $C(A;P)$. Ker P ni pravokotna projekcija točke A na premico $L(P,Q)$, je v preseku

$$C(A;P) \cap L(P,Q)$$

poleg točke P še točka P'. Simetrala daljice $|PP'|$ je premica $L(A,R)$, kjer je R razpolovišče daljice $|PP'|$. Sedaj lahko konstruiramo krožnico $C(A;R)$ in dobimo novo točko $R' \in L(A,R)$. Simetrala daljice $|RR'|$ teče skozi točko A. Ker je premica $L(P,Q)$ pravokotna na premico $L(A,R)$ in je premica $L(A,R)$ pravokotna na simetralo daljice $|RR'|$, sta premica $L(P,Q)$ in simetrala daljice $|RR'|$ vzporedni. To je torej iskana vzporednica.

Lema 3.3. *Točka (x,y) je konstruktibilna natanko tedaj, ko sta x in y konstruktibilni števili.*

Dokaz. Če sta števili x in y konstruktibilni, sta konstruktibilni točki $P = (x,0)$ in $Q = (y,0)$. Točka $Q' = (0,y)$ je konstruktibilna, saj leži v preseku osi y in krožnice $C(O;Q)$. Skozi točko P narišemo vzporednico z osjo y , skozi točko Q' pa vzporednico z osjo x . V preseku teh dveh premic je točka (x,y), zato je konstruktibilna.

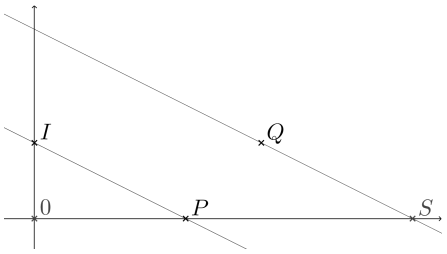
Obratno, če je točka (x,y) konstruktibilna, lahko skoznjo narišemo vzporednici z obema koordinatnima osema. V preseku osi s tema premicama sta točki $(x,0)$ in $(0,y)$. Krožnica $C(O;(0,y))$ seka x os v točki $(y,0)$. Torej sta števili x in y konstruktibilni. □

Lema 3.4. *Množica vseh konstruktibilnih števil K je podobseg v obsegu $\mathbb{C}$. Velja še več: če je $a \in K$, potem je $\sqrt{a} \in K$.*

Dokaz. V prvih štirih točkah točkah dokaza predpostavljamo, da sta števili $a, b \in K$.

(1) *Število $-a$ je konstruktibilno.* Če je točka $(a, 0)$ konstruktibilna, je točka $(-a, 0)$ drugi presek osi x s krožnico $C(O; (a, 0))$.

(2) *Število $a + b$ je konstruktibilno.* Označimo $I = (0, 1), P = (a, 0)$ in $Q = (b, 1)$. Točka Q je konstruktibilna, saj sta njeni komponenti konstruktibilni števili. Narišimo premico $L(P, I)$ in njeno vzporednico skozi točko Q. Ta seka os x v točki S. Točke I, Q, P in S določajo paralelogram, saj je premica $L(P, I)$ vzporedna $L(Q, S)$ in premica $L(I, Q)$ vzporedna $L(P, S)$. Zato je $|QI| = |PS| = b$. Ker je $|OP| = a$, je $|OS| = a + b$. Torej je $S = (a + b, 0)$. Na sliki 1 sta a in b pozitivni, vendar enaka konstrukcija deluje tudi v ostalih primerih.

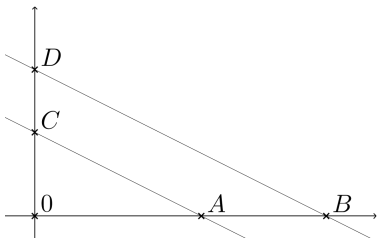


Slika 1. Vsota konstruktibilnih števil.

(3) *Število ab je konstruktibilno.* Brez izgube splošnosti lahko privzamemo, da sta a in b pozitivni. Označimo $A = (1, 0), B = (1 + a, 0)$ in $C = (0, b)$. Točka D je presek osi y in premice skozi B, ki je vzporedna $L(A, C)$. Trikotnika OAC in OBD sta si podobna, zato velja

$$|OB|/|OA| = |OD|/|OC| \quad \text{oziroma} \quad (a + 1)/1 = (b + x)/b.$$

Od tod izračunamo, da je $x = ab$. Sledi, da je točka $D = (0, b + ab)$. Torej je $b + ab$ konstruktibilno število in je zato tudi $ab = (b + ab) - b$ konstruktibilno število.

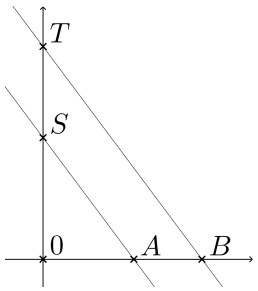


Slika 2. Produkt konstruktibilnih števil.

(4) *Za $a \neq 0$ je število a^{-1} konstruktibilno.* Označimo $A = (1, 0), S = (0, a)$ in $T = (0, 1 + a)$. Točka B je presek x osi in premice skozi T, ki je vzporedna $L(A, S)$. Torej je $B = (1 + u, 0)$ za neki u. Trikotnika OSA in OTB sta si podobna, od koder dobimo zvezo

$$(1 + a)/a = (1 + u)/1.$$

Od tod sledi, da je $u = a^{-1}$, ki je konstruktibilno.



Slika 3. Inverz konstruktibilnega števila.

(5) *Če je $z \in \mathbb{C}$ konstruktibilno, je tudi $\sqrt{z}$ konstruktibilno.*

Trditev bomo najprej dokazali za nenegativna realna števila. Naj bo $c \in \mathbb{R}$ in $c \geq 0$. Označimo $A = (1, 0)$ in $P = (1 + c, 0)$. Točka Q naj bo razpolovišče daljice OP. Najprej konstruiramo vzporednico z osjo y skozi točko A. Nato konstruiramo še krožnico $C(Q; P)$. V preseku te premice in krožnice je točka R (s pozitivno y komponento). Označimo kote trikotnikov AOR in ARP takole: kot $AOR = \alpha$, $ORA = \beta$, $ARP = \gamma$ in $RPA = \delta$. Ker sta trikotnika AOR in ARP pravokotna, vemo, da je

$$\alpha + \beta = \frac{\pi}{2} \quad \text{in} \quad \gamma + \delta = \frac{\pi}{2}.$$

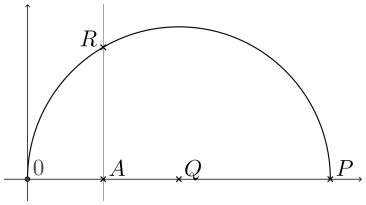
Talesov izrek nam pove, da je

$$\beta + \gamma = \frac{\pi}{2}.$$

Iz teh enakosti izračunamo $\alpha = \gamma$ in $\beta = \delta$. Sledi, da sta si trikotnika AOR in ARP podobna. Zato je

$$1/y = y/c, \quad \text{kjer je} \quad y = |AR|$$

in je $y = \sqrt{a}$.



Slika 4. Koren konstruktibilnega števila.

Pokažimo trditev še za $z \in \mathbb{C}$. Predpostavimo, da $z \neq 0$. Naj bo $z = a + ib = re^{i\theta}$. Tako kartezični kot polarni zapis števila z bomo potrebovali za dokaz trditve. Vemo, da je $r = \sqrt{a^2 + b^2}$. Ker je $z \in K$ konstruktibilno število, sta tudi $a, b \in K$. V prejšnjih točkah dokaza smo videli, da je K obseg, zato je tudi $a^2 + b^2 \in K$. Število $a^2 + b^2$ je nenegativno realno število, zato je $\sqrt{a^2 + b^2} = r \in K$. To pomeni, da je $e^{i\theta} = r^{-1}z \in K$. Ker je $r > 0$, je $\sqrt{r} \in K$. Trditev bo dokazana, če pokažemo, da je $e^{i\theta/2} \in K$. Ker je $e^{i\theta} = \cos\theta + i \sin\theta$, je točka $A = (\cos\theta, \sin\theta)$ konstruktibilna. Označimo $I = (1, 0)$. Točka I in točka A sta enako oddaljeni od izhodišča O, saj obe ležita na enotski krožnici $C(O; I)$. To sledi iz dejstva, da je $\cos^2\theta + \sin^2\theta = 1$. Krožnici $C(A; I)$ in $C(I; A)$ imata enaka polmera, saj je razdalja $|AI| = |IA|$. Sekata se v dveh točkah, ki ju označimo z S_1 in S_2. Premica $L(S_1, O)$ je simetrala kota AOI, saj je razdalja $|S_1I| = |S_1A|$. V preseku premice $L(S_1, O)$ in krožnice $C(O; I)$

je točka $(\cos\theta/2, \sin\theta/2)$. Torej je $\cos\theta/2 + i\sin\theta/2 = e^{i\theta/2} \in K$. Sledi, da je $\sqrt{z} = \sqrt{r}e^{i\theta/2} \in K$. □

Opomba 3.5. Če je kompleksno število z konstruktibilno, je tudi $\overline{z}$ konstruktibilno število.

Posledica 3.6. *Če so števila a, b in c konstruktibilna, sta tudi ničli polinoma $ax^2 + bx + c$ konstruktibilni števili.*

Dokaz. To je direktna posledica zgornje leme in formule za ničli kvadratnih polinomov. □

Naslednji lemi nam povesta, kako se geometrijski problem iskanja presečišč premic in krožnic prevede v algebraični problem. Druga lema bo ključnega pomena pri karakterizaciji konstuktibilnih števil na algebraičen način.

Lema 3.7. *Naj bo F podobseg $\mathbb{C}$, ki vsebuje i in je zaprt za konjugacijo. Naj bosta $z = a + ib, w = c + id \in F$, $P = (a, b), Q = (c, d)$ in $a, b, c, d \in \mathbb{R}$. Veljajo naslednje trditve.*

(1) Če je $a + ib \in F$, sta $a, b \in F$.
(2) Če je enačba premice $L(P, Q)$ enaka $y = mx + q$ za neka $m, q \in \mathbb{R}$, potem sta $m, q \in F$.
(3) Če je enačba krožnice $C(P; Q)$ enaka $(x-p)^2+(y-q)^2 = r^2$ za neke $p, q, r \in \mathbb{R}$, potem je $r^2 \in F$.

Dokaz. (1) Če je $z = a + ib \in F$, je $a = (z + \overline{z})/2 \in F$ in $b = (z - \overline{z})/2i \in F$.

(2) Če je premica $L(P, Q)$ navpična, je njena enačba $x = a$, saj je $P \in L(P, Q)$. Vemo, da je $b \in F$ po točki (1). Sicer ima premica $L(P, Q)$ enačbo

$$y - b = m(x - a)$$

Če vstavimo Q v enačbo, dobimo $m = (d - b)/(c - a) \in F$, saj so $a, b, c, d \in F$. Torej je $q = -ma + b \in F$.

(3) Krožnica $C(P; Q)$ ima enačbo $(x - a)^2 + (y - b)^2 = r^2$, zato je

$$r^2 = (c - a)^2 + (d - b)^2 \in F.$$ □

Lema 3.8. *Naj bo F podobseg $\mathbb{C}$, ki vsebuje i in je zaprt za konjugacijo. Naj bodo P, Q, R, S točke s komponentami v F in $\alpha = u + iv \in \mathbb{C}$. Če je*

$$\alpha \in L(P, Q) \cap L(R, S), \text{ kjer } L(P, Q) \neq L(R, S)$$

ali

$$\alpha \in L(P, Q) \cap C(R; S)$$

ali

$$\alpha \in C(P; Q) \cap C(R; S), \text{ kjer } C(P; Q) \neq C(R; S),$$

potem je $[F(\alpha) : F] \leq 2$.

Dokaz. Oglejmo si stopnjo razširitve $[F(\alpha) : F]$ za vsak primer posebej.

(1) Če je $\alpha \in L(P, Q) \cap L(R, S)$, imamo linearni sistem dveh enačb z dvema spremenljivkama. Ker se premici sekata, vemo, da ima ta sistem rešitev. To je iskana točka (u, v), katere komponenti ležita v F. Torej je $[F(\alpha) : F] = 1$.

(2) Enačba premice $L(P,Q)$ je bodisi $y = mx + q$ bodisi $x = a$, enačba krožnice $C(R;Q)$ pa $(x-c)^2 + (y-d)^2 = r^2$. Vemo že, da so $m, q, r^2 \in F$. Ker je $\alpha = u + iv$ v preseku premice in krožnice, je

$$r^2 = (u-c)^2 + (v-d)^2 = (u-c)^2 + (mu + q - d)^2.$$

Torej je u ničla kvadratnega polinoma s koeficienti v F. Zato je $[F(\alpha) : F] \leq 2$.

(3) Naj bo enačba $C(P;Q)$ enaka $(x-a)^2+(y-b)^2 = r^2$ in enačba $C(R;S)$ enaka $(x-c)^2 + (y-d)^2 = s^2$. Vemo že, da sta $r^2, s^2 \in F \cap \mathbb{R}$. Ker je α v preseku krožnic, velja

$$r^2 = (u-a)^2 + (v-b)^2 \quad \text{in} \quad s^2 = (u-c)^2 + (v-d)^2.$$

Enačbi nato zapišemo po potencah u in v, drugo enačbo odštejemo od prve in dobimo

$$(2c-2a)u + (2d-2b)v + (a^2 - c^2 + b^2 - d^2 - r^2 - s^2) = 0.$$

To je enačba premice s koeficienti v F. Sedaj lahko uporabimo enačbo te premice in enačbo ene od krožnic in pridemo do enakega sklepa kot v točki (2). □

Sedaj lahko dokažemo glavni izrek tega poglavja, ki karakterizira konstruktibilna števila na algebraičen način.

Izrek 3.9. *Kompleksno število z je konstruktibilno natanko tedaj, ko obstaja tako končno zaporedje obsegov*

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n,$$

da je $z \in K_n$ in $[K_{j+1} : K_j] \leq 2$ za $0 \leq j < n$.

Dokaz. ($\Rightarrow$) Če je z konstruktibilno, obstaja zaporedje $1, -1, z_1, \ldots, z_n = z$, kjer je vsak z_j konstruktibilen iz $\{1, -1, z_1, \ldots, z_{j-1}\}$. Definirajmo

$$K_j = \mathbb{Q}(z_1, \ldots, z_j).$$

Torej obstajajo točke $E, F, G, H \in K_j$, da velja ena od spodnjih trditev

$$z_{j+1} \in L(E,F) \cap L(G,H);$$
$$z_{j+1} \in L(E,F) \cap C(G;H);$$
$$z_{j+1} \in C(E;F) \cap C(G;H).$$

Da bomo lahko uporabili lemo 3.8, moramo pokazati še, da je K_j zaprt za konjugacijo za $1 \leq j \leq n$. Imaginarna enota i je konstruktibilno število, saj je $i = (0,1)$. Zato lahko brez izgube splošnosti privzamemo, da je $z_1 = i$. Torej je množica

$$K_1 = \mathbb{Q}(i) = \{a + ib; a, b \in \mathbb{Q}\},$$

za katero vemo, da je zaprta za konjugacijo. Obseg K_1 izpolnjuje pogoje leme 3.8, zato je $[K_2 : K_1] \leq 2$. Prva možnost je, da je $[K_2 : K_1] = 1$. To pomeni, da je $z_2 \in K_1$ in je zato $K_1 = K_2$. Druga možnost je, da je $[K_2 : K_1] = 2$. V tem primeru ima minimalni polinom razširitve stopnjo 2 in ima ničlo v z_2. Ker je K_2 vektorski prostor nad K_1 z bazo $\{1, z_2\}$, lahko vsak element $x \in K_2$ zapišemo kot $x = a + bz_2$ za neka $a, b \in K_1$. Torej je $\overline{x} = \overline{a} + \overline{b}\overline{z_2}$. Ker je K_1 zaprt za konjugacijo, sta $\overline{a}, \overline{b} \in K_1$, vemo pa tudi, da je $\overline{z_2} \in K_2$, saj je to konjugirana vrednost konstruktibilnega števila. Torej je $\overline{x}$ konstruktibilno in je zato K_2 zaprt za konjugacijo. Obseg K_2 v obeh primerih izpolnjuje vse predpostavke leme 3.8. Na enak način kot zgoraj pokažemo, da je K_3 zaprt za konjugacijo. Ta postopek lahko ponovimo za vsak $K_j, 2 \leq j \leq n$ in tako dokažemo prvi del izreka.

($\Leftarrow$) Za dokaz obrata trditve zadošča pokazati sledeče: če je $[B : F] = 2$, kjer je F podobseg obsega konstruktibilnih števil K, potem je $B = F(\beta)$, za neko konstruktibilno število β. Od tod bo sledilo, da je $B \subseteq K$. Naj bo torej $[B : F] = 2$. Vzemimo $\alpha \in B \setminus F$. Po izreku 2.34 (natančeje po njegovi posledici 2.35) je $\mathrm{st}_F(\alpha) = 2$. Torej obstaja minimalni polinom za α nad $F[x]$. Označimo ga z $f(x) = x^2 + bx + c$. Definirajmo $\beta = \sqrt{b^2 - 4c}$. Torej je

$$\alpha = \frac{-b \pm \beta}{2}.$$

To vstavimo v $f(x)$ in dobimo minimalni polinom za β, ki je $g(x) = x^2 + 4c - b^2$. To je res minimalni polinom, saj je β njegova ničla in je nerazcepen, saj bi bila sicer β (in tudi α) vsebovana v F. Videti moramo še, da je β konstruktibilno število. Vemo, da je

$$\beta^2 = b^2 - 4c \in F \subseteq K.$$

Torej je β^2 konstruktibilno število. Pokazali smo, da so kvadratni koreni konstruktibilnih števil tudi konstruktibilna števila. Sledi, da je $\beta \in K$. □

Posledica 3.10. *Če je kompleksno število z konstruktibilno, potem je $[\mathbb{Q}(z) : \mathbb{Q}] = 2^k$ za neki $k \in \mathbb{N}$.*

Dokaz. Upoštevamo zgornji izrek in dejstvo, da se stopnje zaporednih razširitev množijo med seboj (izrek 2.31). □

Sedaj se lahko na zelo enostaven način prepričamo, da sta dva od treh starogrških problemov nerešljiva.

Podvojitev kocke. Dano imamo kocko s prostornino 1 in želimo konstruirati kocko s prostornino 2. Pri tem smemo uporabljati le šestilo in ravnilo. Stranica prvotne kocke ima dolžino 1. Problem bomo rešili, če bomo znali konstruirati stranico dolžine $\alpha = \sqrt[3]{2}$.

Minimalni polinom za α nad $\mathbb{Q}[x]$ je $p(x) = x^3 - 2$. Jasno je, da je α ničla tega polinoma. Da bomo dokazali, da je to minimalni polinom za α, moramo pokazati še, da je nerazcepen nad $\mathbb{Q}[x]$. Oglejmo si splošen polinom q z racionalnimi koeficienti stopnje 3, ki je razcepen nad $\mathbb{Q}[x]$. Polinom q lahko zapišemo kot

$$q(x) = (x - \alpha)(x^2 + \beta_0 x + \beta_1).$$

Iz zgornjega zapisa je jasno vidno, da je $q(\alpha) = 0$. Torej ima vsak razcepen polinom stopnje 3 nad $\mathbb{Q}[x]$ racionalno ničlo. Za dokaz nerazcepnosti polinoma $p(x) = x^3 - 2$ je torej dovolj pokazati, da p nima racionalne ničle. Ker je polinom $p \in \mathbb{Z}[x]$, si oglejmo, kaj lahko povemo o racionalnih ničlah polinoma v $\mathbb{Z}[x]$. Naj bo

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

in racionalno število a/b njegova ničla. Predpostavimo še, da sta si a in b tuji števili. Torej je

$$0 = f\left(\frac{a}{b}\right) = a_n \left(\frac{a}{b}\right)^n + \cdots + a_1 \frac{a}{b} + a_0.$$

Enakost pomnožimo z b^n in dobimo

$$0 = a_n a^n + \cdots + a_1 a b^{n-1} + a_0 b^n.$$

Sledi, da je

$$a_n a^n \equiv 0 \pmod{b}$$
$$\text{in}$$
$$a_0 b^n \equiv 0 \pmod{a}$$

Ker sta si števili a in b tuji, mora $a|a_0$ in $b|a_n$. Kandidati za racionalne ničle polinoma v $\mathbb{Z}[x]$ so torej oblike $\pm c/d$, kjer $c|a_0$ in $d|a_n$.

Kandidati za racionalno ničlo polinoma $p(x) = x^3 - 2$ so torej števila ± 1 in ± 2. Izračunamo $p(-1) = -3$, $p(1) = -1$, $p(-2) = -10$ in $p(2) = 6$. Sledi, da polinom p nima racionalne ničle in je zato nerazcepen nad $\mathbb{Q}[x]$. Torej je $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ in zato $\sqrt[3]{2}$ ni konstruktibilno število.

Trisekcija kota. Pokazali bomo, da je nemogoče poljuben kot razdeliti na 3 enake dele. Zadošča torej pokazati, da obstaja kot ϕ, za katerega ne moremo konstruirati kota $\phi/3$. Kot ϕ je konstruktibilen, če lahko konstruiramo točko $(\cos\phi, \sin\phi)$. Pokazali bomo, da za $\phi = \pi/3$, $\cos(\phi/3)$ ni konstruktibilno število.Z uporabo adicijskih izrekov in drugih enakosti, ki jih poznamo iz trigonometrije lahko izpeljemo

$$\begin{aligned}
\cos\phi &= \cos\left(3\frac{\phi}{3}\right) = \cos\left(2\frac{\phi}{3}\right)\cos\left(\frac{\phi}{3}\right) - \sin\left(2\frac{\phi}{3}\right)\sin\left(\frac{\phi}{3}\right) \\
&= \cos\left(\frac{\phi}{3}\right)\left(\cos^2\left(\frac{\phi}{3}\right) - \sin^2\left(\frac{\phi}{3}\right)\right) - 2\cos\left(\frac{\phi}{3}\right)\sin^2\left(\frac{\phi}{3}\right) \\
&= \cos\left(\frac{\phi}{3}\right)\left(2\cos^2\left(\frac{\phi}{3}\right) - 1\right) - 2\cos\left(\frac{\phi}{3}\right)\left(1 - \cos^2\left(\frac{\phi}{3}\right)\right) \\
&= 4\cos^3\left(\frac{\phi}{3}\right) - 3\cos\left(\frac{\phi}{3}\right)
\end{aligned}$$

Z uvedbo nove spremenljivke $u = 2\cos(\phi/3)$ se enačba prevede v

$$u^3 - 3u - 1 = 0.$$

Torej je u ničla polinoma $p(x) = x^3 - 3x - 1$. Pokažimo, da je ta polinom nerazcepen. Pri podvojitvi kocke smo pokazali, da ima vsak razcepen polinom stopnje 3 nad $\mathbb{Q}[x]$ racionalno ničlo. Pokazali smo tudi, kako poiščemo kandidate za racionalne ničle polinoma v $\mathbb{Z}[x]$. Edina kandidata za racionalni ničli polinoma p sta števili ± 1. Ker je $p(1) = -3$ in $p(-1) = 1$, polinom p nima racionalne ničle in je zato nerazcepen nad $\mathbb{Q}[x]$. Sledi, da je $[\mathbb{Q}(u) : \mathbb{Q}] = 3$ in da število u ni konstruktibilno.

Kvadratura kroga. Dan imamo krog s polmerom 1. Z uporabo šestila in ravnila želimo konstruirati kvadrat s ploščino, ki je enaka ploščini enotskega kroga tj. π. Povedano drugače: želimo konstruirati stranico kvadrata dolžine $\sqrt{\pi}$. Ta problem je težji kot prejšnja dva. Pokazati je mogoče, da je π transcenentno število, tj. število, ki ni ničla nobenega polinoma z racionalnimi koeficienti. Posledica tega dokaza je, da π ni konstruktibilno število. Ta dokaz bomo izpustili, saj zahteva bolj obširno znanje matematike, je pa naveden v knjigi [1].

Slovar strokovnih izrazov

algebraic number algebraično število – število a je algebraično nad obsegom F, če je ničla kakšnega polinoma s koeficienti v F

ring isomorphism izomorfizem kolobarjev – bijektivni homomorfizem kolobarjev

constructible number konstruktibilno število – realno število, ki ga lahko konstruiramo s pomočjo šestila in ravnila

monic polynomial moničen polinom – polinom, ki ima vodilni koeficient enak 1

irreducible polynomial nerazcepen polinom – polinom s koeficienti v obsegu F, ki ga ne moremo zapisati kot produkt dveh polinomov s koeficienti v obsegu F stopnje vsaj 1

Literatura

[1] C. R. Hadlock, *Field theory and its classical problems*, The Carus Mathematical Monographs **19**, The Mathematical Association of America, 1978.

[2] T. W. Hungerford, *Algebra*, Graduate Texts in Mathematics **73**, Springer-Verlag, New York, 1974.

[3] J. Rotman, *Galois Theory*, Springer, New York, 1998.