

Prof. dr. sc. Almir Huskanović

NEKE OSOBINE KOMAKSIMALNIH IDEALA

Sažetak

Za dva ideala I i J komutativnog prstena R kažemo da su komaksimalni ako je $I + J = R$.

Činjenica da su ideali komaksimalni je ekvivalentna sa činjenicom da su odgovarajući prirodni brojevi relativno prosti. Ako je ispunjen taj uslov, tada možemo izvesti nekoliko značajnih tvrdnji. Najpoznatija od njih je Kineska teorema o ostacima. Osim toga, pomoću izvedenih tvrdnji, možemo dalje dobiti neke poznate stavove iz teorije brojeva.

Ključne riječi: komaksimalni ideali, Kineska teorema o ostacima

Uvod

U ovom radu se podrazumijeva da je R komutativni prsten sa jediničnim elementom 1. Skup svih njegovih maksimalnih ideala označavat ćemo sa $\Omega(R)$. Međutim, za proizvoljni netrivialni ideal I prstena R , oznaka $\Omega(I)$ označava skup svih maksimalnih ideala prstena R koji sadrže ideal I .

Definicija 1: Za ideale I i J prstena R kažemo da su komaksimalni ako je $I + J = R$.

Za proizvoljne ideale I i J prstena R poznato je da su $I \cap J$ i

$$I \cdot J = \{\sum_{i=1}^n x_i y_i \mid x_i \in I, y_i \in J\} \cup \{0\}$$

takođe ideali prstena R , što se direktno pokaže, te da je $I \cdot J \subseteq I \cap J$.

Teorema 1: Ako su ideali I i J prstena R komaksimalni, tada je $I \cdot J = I \cap J$.

Dokaz: Iz $I + J = R$ slijedi da postoje elementi $u \in I, v \in J$ takvi da je $u + v = 1$. Tada za proizvoljno $x \in I \cap J$ imamo da je

$$x = x \cdot 1 = x \cdot (u + v) = x \cdot u + x \cdot v \in I \cdot J.$$

Time smo dokazali da je $I \cap J \subseteq I \cdot J$, što zajedno sa $I \cdot J \subseteq I \cap J$ povlači da je $I \cdot J = I \cap J$. ■

Posljedica 1: Za svaki prirodni broj n vrijedi tvrdnja: ako bismo imali n ideala $I_1, I_2, \dots, I_n$ prstena R tako da su svaka dva od njih komaksimalni, tada je $I_1 \cdot I_2 \cdot \dots \cdot I_n = I_1 \cap I_2 \cap \dots \cap I_n$.

Dokaz: Slijedi direktno iz Teoreme 1 pomoću matematičke indukcije. ■

Kineska teorema o ostacima i druge tvrdnje

U teoriji brojeva, tačnije iz oblasti modularne aritmetike je poznata Kineska teorema o ostacima koja omogućava jednostavno rješavanje sistema od konačno mnogo linearnih kongruencija po različitim modulima (koji su relativno prosti po parovima). Ova teorema je dobila ime po kineskom matematičaru Sun Zi Suanjingu koji je u 3. vijeku prvi postavio zadatak koji bi se mogao rješavati pomenutom teoremom. Razmotrit ćemo analognu teoremu koja vrijedi za ideale (njih konačno mnogo) istog prstena R u komutativnoj algebri i još nekoliko drugih tvrdnji u kojima je glavni uslov da su ideali komaksimalni. Relacija kongruencije po nekom modulu $\equiv (\text{mod } m), m \in \mathbb{N}$ u skupu cijelih brojeva se koristi kada dva cijela broja daju isti ostatak pri dijeljenju sa prirodnim brojem m . U algebri, ako je I ideal prstena R , tada $x \equiv y (\text{mod } I) \Leftrightarrow x - y \in I$ (v. [1])

Teorema 2: Ako su $m_1, m_2, \dots, m_n$ u parovima relativno prosti prirodni brojevi, te $a_1, a_2, \dots, a_n$ proizvoljni cijeli brojevi, tada sistem linearnih kongruencija

$$x \equiv a_i (\text{mod } m_i), i = 1, 2, \dots, n \quad (1)$$

ima rješenje.

Dokaz ove teoreme se može naći u knjizi [1]. Pokazat ćemo da je ova teorema ekvivalentna sa sljedećom:

Teorema 3: Neka je R prsten, a $I_1, I_2, \dots, I_n$ su ideali prstena R , komaksimalni u parovima (tj. $I_i + I_j = R, i \neq j$). Za proizvoljne elemente $a_1, a_2, \dots, a_n \in R$ postoji element $a \in R$ tako da je

$$a \equiv a_i (\text{mod } I_i) \text{ za sve } i \in \{1, 2, \dots, n\}.$$

Dokaz: Dokažimo ovu tvrdnju najprije u specijalnom slučaju kada je $a_1 = 1$ i $a_j = 0$, za $j > 1$. Tada je $I_1 + I_j = R$ ($j > 1$), pa postoje elementi $b_j \in I_1, c_j \in I_j$ tako da je $b_j + c_j = 1$ za sve $j > 1$. To dalje povlači da je $\prod_{j=2}^n (b_j + c_j) = 1$.

Množenjem izraza na lijevoj strani, uzimajući u obzir da svaki element u obliku proizvoda u kome se javlja b_j (za proizvoljno $j = 2, 3, \dots, n$) pripada idealu I_1 i da $c_2 c_3 \dots c_n \in \prod_{j=2}^n I_j$, zaključujemo da postoje elementi $b \in I_1$ i $a \in \prod_{j=2}^n I_j$, takvi da je $b + a = 1$. Za element a tada očito vrijedi da je $a \equiv 1 (\text{mod } I_1)$ i $a \equiv 0 (\text{mod } I_i), i > 1$. Jasno je onda da analogno možemo naći element $a \in R$ takav da je $a \equiv 1 (\text{mod } I_i)$ i $a \equiv 0 (\text{mod } I_j), i > 1, j \neq i$.

Neka su sada $a_1, a_2, \dots, a_n$ proizvoljni elementi prstena R . Za svaki indeks $i \in \{1, 2, \dots, n\}$ prema prvom dijelu dokaza postoje elementi $c_i \in R$ sa osobinom da je $c_i \equiv 1 (\text{mod } I_i)$ i $c_i \equiv 0 (\text{mod } I_j), j \neq i$. Uzmimo onda da je $a = a_1 c_1 + a_2 c_2 + \dots + a_n c_n$.

Tvrdimo da je $a \equiv a_i \pmod{I_i}$ za sve $i \in \{1, 2, \dots, n\}$. Zaista, $a - a_i = a - a_i c_i + a_i(c_i - 1)$ dok je $a - a_i c_i = \sum_{j \neq i} a_j c_j \equiv 0 \pmod{I_i}$ i $a_i(c_i - 1) \equiv 0 \pmod{I_i}$, što znači da je $a \equiv a_i \pmod{I_i}$ za sve $i \in \{1, 2, \dots, n\}$. ■

Poznato je da su svi ideali prstena $\mathbb{Z}$ cijelih brojeva glavni, tj. oblika

$$m\mathbb{Z} = \{0, \pm m, \pm 2m, \dots\}$$

gdje je m neki prirodni broj ili 0. Tada se još koristi oznaka $(m) = m\mathbb{Z}$.

Za proizvoljno $i \in \{1, 2, \dots, n\}$ uslov (1) je ekvivalentan sa:

$$x \equiv a_i \pmod{m_i \mathbb{Z}}, i = 1, 2, \dots, n$$

a uslov komaksimalnosti dva ideala $m\mathbb{Z}$ i $n\mathbb{Z}$ je ekvivalentan uslovu da je $(m, n) = 1$, gdje je (m, n) —najveći zajednički djelilac brojeva m i n . Naime, poznato je da su prirodni (a važi i za cijele) brojevi m i n relativno prosti (tj. $(m, n) = 1$) ako i samo ako postoje cijeli brojevi x i y tako da je $mx + ny = 1$.

Time smo pokazali ekvivalentnost Teoreme 3 i Teoreme 2.

Sljedeća teorema je posljedica Teoreme 3.

Teorema 4: Ako je R prsten, a $I_1, I_2, \dots, I_n$ su ideali prstena R , komaksimalni u parovima, tada je

$$R / \prod_{i=1}^n I_i \cong \prod_{i=1}^n R / I_i$$

Dokaz: Definišimo preslikavanje $f: R \rightarrow \prod_{i=1}^n R / I_i$ ovako:

$$f(a) = (a + I_1, a + I_2, \dots, a + I_n) \quad (a \in R).$$

Direktno se dokaže da je f homomorfizam prstena.

Dokažimo da je ovo preslikavanje surjektivno. Ako uzmemo proizvoljni element

$$(a_1 + I_1, a_2 + I_2, \dots, a_n + I_n) \in \prod_{i=1}^n R / I_i$$

pri čemu su $a_1, a_2, \dots, a_n \in R$ proizvoljni, prema Teoremi 3 postoji element $a \in R$ takav da je $a \equiv a_i \pmod{I_i}, i = 1, 2, \dots, n$, tj. $a + I_i = a_i + I_i$ ($i = 1, 2, \dots, n$). Tada je

$$f(a) = (a + I_1, a + I_2, \dots, a + I_n) = (a_1 + I_1, a_2 + I_2, \dots, a_n + I_n).$$

Dakle, f je surjektivni homomorfizam prstena, pa je $Im(f) = \prod_{i=1}^n R / I_i$.

S druge strane, $f(a) = (0 + I_1, 0 + I_2, \dots, 0 + I_n) = (I_1, I_2, \dots, I_n) \Leftrightarrow a \in \bigcap_{i=1}^n I_i$ što znači da je

$$Ker(f) = \bigcap_{i=1}^n I_i = \prod_{i=1}^n I_i.$$

Za zadnji zaključak smo iskoristili Posljedicu 1. Tvrdnja teoreme tada direktno slijedi iz prve teoreme izomorfije za prstene (v. [1], [3]). ■

Teorema 5: Ako je R prsten, a $I_1, I_2, \dots, I_n$ su ideali prstena R , komaksimalni u parovima, tada je familija skupova $\{\Omega(I_i) | i = 1, 2, \dots, n\}$ particija skupa $\Omega(\cap_{i=1}^n I_i)$.

Dokaz: Treba dokazati da je

$$\Omega(\cap_{i=1}^n I_i) = \cup_{i=1}^n \Omega(I_i) \text{ i } \Omega(I_i) \cap \Omega(I_j) = \emptyset \text{ za } i \neq j.$$

Uzimajući proizvoljni maksimalni ideal $M \in \Omega(\cap_{i=1}^n I_i)$ znamo da je $\cap_{i=1}^n I_i \subseteq M$. Pošto je M maksimalan ideal, on je i prost (v. [3]), pa zato postoji $j \in \{1, 2, \dots, n\}$ tako da je $I_j \subseteq M$, dakle, $M \in \Omega(I_j)$.

Time smo dokazali da je

$$\Omega\left(\bigcap_{i=1}^n I_i\right) \subseteq \bigcup_{i=1}^n \Omega(I_i) \quad (2)$$

Ako $M \in \cup_{i=1}^n \Omega(I_i)$ to znači da $M \in \Omega(I_j)$ za neko $j \in \{1, 2, \dots, n\}$, tj.

$$I_j \subseteq M \Rightarrow \bigcap_{i=1}^n I_i \subseteq M \Rightarrow M \in \Omega\left(\bigcap_{i=1}^n I_i\right) \Rightarrow \bigcup_{i=1}^n \Omega(I_i) \subseteq \Omega\left(\bigcap_{i=1}^n I_i\right) \quad (3)$$

Iz (2) i (3) slijedi $\Omega(\cap_{i=1}^n I_i) = \cup_{i=1}^n \Omega(I_i)$.

Dokažimo sada da je $\Omega(I_i) \cap \Omega(I_j) = \emptyset$, ako je $i \neq j$. Zbog činjenice da je $I_i + I_j = R$, uzimajući proizvoljni maksimalni ideal $M \in \Omega(I_i)$ jasno je da $M \notin \Omega(I_j)$ jer u suprotnom bismo imali $I_i \subseteq M$ i $I_j \subseteq M$ iz čega slijedi da je $I_i + I_j \subseteq M \Rightarrow M = R$, što je nemoguće. Teorema je dokazana. ■

Napomena: Pomoću Teorema 4. i 5. mogu se dokazati neke značajne osobine tzv. maksimalnih ideala, v. [2].

Primjeri:

- a) Ako su p i q dva proizvoljna prosta broja, a $\mathbb{Z}_n$ nam označava prsten ostataka po modulu $n, n \in \mathbb{N}$, pomoću Teoreme 4 se može dobiti da je $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$.

Ovaj rezultat slijedi kad se uzme da je $n = 2, R = \mathbb{Z}, I_1 = (p), I_2 = (q)$. Osim toga, treba uzeti u obzir poznatu činjenicu da je $\mathbb{Z}/(p) \cong \mathbb{Z}_p$ i analogno $\mathbb{Z}/(q) \cong \mathbb{Z}_q$, te $(p) \cap (q) = (pq)$, (v. [1], [3], [4]). Zapravo u jednakosti $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ umjesto

prostih brojeva p i q možemo uzeti da su p i q bilo koja dva prirodna broja koji su relativno prosti.

- b) Rezultat iz primjera a) se može poopštiti na n proizvoljnih različitih prostih brojeva $p_1, p_2, \dots, p_n$, dakle $\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \dots \times \mathbb{Z}_{p_n} \cong \mathbb{Z}_{p_1 p_2 \dots p_n}$, odnosno u slučaju da imamo prirodni broj $n = n_1 n_2 \dots n_k$ napisan u obliku proizvoda konačno mnogo prirodnih brojeva koji su relativno prosti u parovima, tada je $\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k}$.
- c) Ako je prirodni broj n napisan u kanonskom obliku: $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, gdje su $p_1, p_2, \dots, p_k$ različiti prosti brojevi, a $\alpha_1, \alpha_2, \dots, \alpha_k$ prirodni brojevi, tada je prema b):

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \dots \times \mathbb{Z}_{p_k^{\alpha_k}} \quad (4)$$

U prstenu $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ invertibilni su elementi $\bar{x}$, gdje je $x \in \{0, 1, \dots, n-1\}$ broj relativno prost sa n . Skup svih invertibilnih elemenata u prstenu $\mathbb{Z}_n$ označit ćemo sa $\mathbb{Z}_n^*$ – direktno se provjeri da je $(\mathbb{Z}_n^*, \cdot)$ grupa. Prsten $\mathbb{Z}_n$ ima ukupno $\varphi(n)$ invertibilnih elemenata, gdje je φ Ojlerova funkcija. S druge strane, za proizvoljni prosti broj p i α prirodan broj očito je:

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$$

tako da je broj invertibilnih elemenata prstena $\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \dots \times \mathbb{Z}_{p_k^{\alpha_k}}$ jednak:

$$(p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{\alpha_2} - p_2^{\alpha_2-1}) \dots (p_k^{\alpha_k} - p_k^{\alpha_k-1}) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)$$

pa ako izjednačimo broj invertibilnih elemenata sa lijeve i desne strane u (4), dolazimo do formule za Ojlerovu funkciju

$$\varphi(n) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right).$$

Zaključak

Teorija ideala komutativnih prstena se može iskoristiti da se izvedu brojni rezultati iz teorije brojeva. Ta teorija se u matematici prvobitno pojavila upravo prilikom rješavanja problema iz teorije brojeva. Naime, pojam ideala prstena uveo je njemački matematičar Dedekind (Julius Wilhelm Richard Dedekind, 1831.-1916.) koristeći Kummerovu ideju “idealnog broja” (Ernst Eduard Kummer, 1810.-1893., njemački matematičar) kojeg je on uveo u pokušaju dokazivanja tzv. Fermatovog velikog teorema (Pierre de Fermat, 1607.-1665., francuski matematičar i pravnik). Iako Kummer nije uspio dokazati Fermatovu veliku

teoremu, njegova ideja vezano za ideale prstena je bila veoma značajna u oblasti komutativne algebre.

Literatura

- [1] A. Huskanović, H. Alajbegović: *Diskretna matematika*, Politehnički fakultet Univerziteta u Zenici, 2020.,
- [2] A. Huskanović: *Karakterizacija prstena čiji se konačno generisani moduli razlažu u sumu cikličkih modula*, magistarski rad, PMF Sarajevo, 2005.
- [3] H. Jamak: *Algebra*, NIK Sezam, Sarajevo, 2004.
- [4] S. Lang: *Algebra*, Springer, New York, 2002.

SOME PROPERTIES OF COMAXIMAL IDEALS

Abstract

Two ideals I and J of a commutative ring are comaximal if $I + J = R$. The fact that ideals are comaximal is equivalent to the fact that corresponding integers are relatively prime. If this condition is met, than it is possible to derive several important statements. The most famous among them is Chinese remainder theorem. Besides, on the basis of the derived statements it is possible to further achive some known facts from the number theory.

Key words: *comaximal ideals, Chinese remainder theorem*