Univerzitet u Beogradu
Matematički fakultet

O matricama nad komutativnim prstenima

master rad

student
Branislava Perić

mentor
dr Zoran Petrović

Beograd, 2011.

Sadržaj

UVOD

Rešavanje sistema linearnih jednačina spada u jedan od osnovnih i široko primenjivih zadataka linearne algebre. Standardni problem da se utvrdi da li postoji skup rešenja se najčešće svodi na diskusiju ranga matrice koeficijenata sistema, i naravno zavisi od samih jednačina tj. komponenata matrice, ali takođe i od dostupnih vrednosti, tj. da li se radi o celim brojevima, realnim brojevima, i slično. Iako se u takvim, školskim zadacima uglavnom podrazumeva da sistem rešavamo nad nekim poljem, sasvim je međutim jasno da možemo posmatrati rešavanje sistema i nad prstenom celih brojeva na primer, ili prstenom ostataka po nekom modulu. Takođe, postoji mnogo situacija kada komponente matrice nisu elementi polja, već to mogu biti polinomi sa konačnim brojem neodređenih, ili elementi bilo kog komutativnog prstena uopšte.

Tema ovog rada se upravo odnosi na osobenosti operacija sa matricama čije su komponente elementi nekog komutativnog prstena, što dalje vodi do zanimljivih posledica ukoliko rešavanje sistema linearnih jednačina posmatramo nad komutativnim prstenima. Cilj je bio kako da se ukaže na značajne činjenice u vezi sa algebrom komutativnih prstena uopšte, njihovih ideala i modula nad tim prstenima, tako i da se jasno istaknu razlike u odnosu na klasični slučaj kada se ovi zadaci rešavaju nad poljem. Dokazi tvrđenja su kad god je bilo moguće izvođeni sa tačke gledišta matričnog računa, kako bi se izveli i zaključci u vezi samih operacija nad matricama. Namera je, takođe, bila da se tekst lako nadoveže na elementarna predznanja iz linearne algebre, pa je naveden veliki broj detaljno razrađenih primera.

§1 PRSTENI

Prsten $(K,+,\cdot)$ je algebarska struktura sa dve binarne operacije za koje važi:

P1) $(K,+)$ je komutativna grupa,

P2) $(K,\cdot)$ je monoid,

P3) druga operacija je distributivna u odnosu na prvu, $(a+b)\cdot c = a\cdot c+b\cdot c$

$c\cdot(a+b) = c\cdot a+a\cdot b$, za svako $a,b,c\in K$.

Same operacije prstena obično obeležavamo sa $+$ i $\cdot$ (tim redom) i nazivamo sabiranjem i množenjem. Neutral aditivne grupe $(K,+)$ nazivamo nulom samog prstena i obeležavamo sa 0, dok multiplikativni neutral nazivamo jedinicom u prstenu i obeležavamo sa 1, pri čemu podrazumevamo da je $1\neq 0$. Stoga prsten K sadrži bar dva različita elementa.

Skup svih ne-nula elemenata prstena K obeležavaćemo sa $K^*=K\setminus\{0\}$.
Za element $x\in K$ kažemo da je levi **delitelj nule** u tom prstenu ako za bar jedno $y\in K^*$ važi $xy = 0$, odnosno desni delitelj nule ako važi $yx = 0$. Označićemo sa $Z(K)$ skup elemenata prstena K koji su ili levi ili desni delitelji nule u tom prstenu. Element $x\in K$ koji nije ni levi niti desni delitelj nule u tom prstenu nazivamo **regularnim**. Dakle, skup $Reg(K) = K\setminus Z(K)$ je skup regularnih elemenata prstena K. Naravno, sama nula prstena je delitelj nule, jer je $0\cdot 1=0$, $1\neq 0$. Dakle, $0\in Z(K)$, dok za preostale delitelje nule u tom prstenu kažemo da su **pravi**. Jedinica je regularni element u prstenu K, tj. $1\in Reg(K)$.

Ako je množenje u prstenu komutativno tada kažemo da je sam prsten komutativan. Komutativne prstene ćemo nadalje uvek obeležavati sa R. Kod komutativnih prstena levi delitelji nule su istovremeno i desni, pa ćemo sa $Z(R)$ obeležavati skup delitelja nule prstena R. Komutativne prstene koji nemaju pravih delitelja nule nazivamo **oblastima celih** ili **domenima**. Drugim rečima, oblast celih je svaki komutativan prsten R, sa bar dva elementa, u kome važi

$$ab=0 \Leftrightarrow a=0 \vee b=0 \text{ za svako } a,b\in R$$

tj. u kome su svi ne-nula elementi i regularni. Tipični predstavnici takvih prstena su: skup celih brojeva $\mathbb{Z}$, zatim proizvoljno polje F (kao komutativan prsten u kome jedino nula nema inverz), na primer, polje racionalnih brojeva $\mathbb{Q}$, kao i prsten polinoma $F[X_1, ..., X_n]$ sa koeficijentima iz bilo kog polja F.

S druge strane, skup $M_2(R)$ svih kvadratnih matrica reda 2, na primer, sa komponentama iz datog prstena R, je i sam jedan prsten u odnosu na operacije sabiranja i množenja matrica. Zovemo ga i **prstenom matrica reda 2** nad prstenom R. Njegova nula je nula-matrica $\boldsymbol{O}$, a jedinica jedinična matrica E,

$$\boldsymbol{O}=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix} \quad \text{i} \quad E=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}.$$

Ali, prsten $M_2(R)$ nije komutativan, jer množenje matrica u opštem slučaju nije komutativno. Takođe, u ovom prstenu proizvod dve matrica A i B može da bude nula, a da to nisu ni A ni B, pa ovaj prsten nije oblast celih.

Primer 1. Neka su date matrice $A, B \in M_2(\mathbb{Z})$,

$$A = \begin{bmatrix} 2 & -1 \\ 6 & -3 \end{bmatrix} \text{ i } B = \begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix}.$$

Njihov proizvod je $AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

Jasno, date matrice A i B su delioci nule u posmatranom prstenu kvadratnih matrica reda 2 nad prstenom celih brojeva $\mathbb{Z}$.

Uopšte, razmotrimo sledeći

Primer 2. Ako je R komutativan prsten, tada je matrica A delitelj nule u prstenu $M_2(R)$ kvadratnih matrica ako i samo ako je njena determinanta delitelj nule u prstenu R.

($\Rightarrow$) Ako je matrica A delitelj nule onda postoji bar jedna ne-nula matrica B takva da je $AB=0$.

Zaista, ako su matrice $A,B \in M_2(R)$, $B \neq 0$, na primer

$$A = \begin{bmatrix} a & b \\ p & q \end{bmatrix} \qquad \text{i} \qquad B = \begin{bmatrix} x & u \\ y & v \end{bmatrix}$$

onda je $AB = \begin{bmatrix} ax+by & au+bv \\ px+qy & pu+qv \end{bmatrix}$ pa je relacija $AB=0$ ekvivalentna uslovima

$$\begin{cases} ax+by=0 \\ px+qy=0 \end{cases} \quad \text{i} \quad \begin{cases} au+bv=0 \\ pu+qv=0 \end{cases} \quad \text{u prstenu } R. \qquad (*)$$

Za rešenja prvog sistema važi $\Delta \cdot x = \Delta_x$, $\Delta \cdot y = \Delta_y$, a drugog $\Delta \cdot u = \Delta_u$, $\Delta \cdot v = \Delta_v$,
gde je $\Delta = \det A = aq - bp$ determinanta matrice A, dok su determinante

$$\Delta_x = \begin{vmatrix} 0 & b \\ 0 & q \end{vmatrix} = 0, \text{ i takođe, } \Delta_y = \Delta_u = \Delta_v = 0.$$

Dakle, mora biti i $\Delta \cdot x = 0$, $\Delta \cdot y = 0$, $\Delta \cdot u = 0$, $\Delta \cdot v = 0$. (**)
Međutim, kako je matrica $B \neq 0$ to je bar neki od $x, y, u, v \neq 0$. Samim tim, ako je $AB=0$ za bar jednu matricu $B \neq 0$, tada je i $\Delta \cdot \lambda = 0$ za bar jedno $\lambda \neq 0$ u prstenu R, tj. Δ je delitelj nule u R.

($\Leftarrow$) Obratno, ako je $\Delta \cdot \lambda = 0$ za bar jedno $\lambda \neq 0$ iz R, biće $(aq-bp) \cdot \lambda = 0$ tj. $aq\lambda - bp\lambda = 0$ pa uslovi (*) važe za npr. $x = q\lambda$, $y = -p\lambda$, $u = -b\lambda$, $v = a\lambda$.
Pri tom, ako je $q\lambda = p\lambda = b\lambda = a\lambda = 0$ tada (**) važi i za $x = y = u = v = \lambda \neq 0$ pa bar u jednom od tih slučajeva mora biti $AB=0$ i $B \neq 0$.
Dakle, matrica A je delitelj nule u prstenu $M_2(R)$ ako i samo ako je njena determinanta $\Delta = \det A$ delitelj nule u samom prstenu R.

Dakle, ako je, na primer, prsten R prsten celih brojeva $\mathbb{Z}$, onda je matrica $A \in M_2(\mathbb{Z})$ regularna ako i samo ako je $\det A \neq 0$, jer je nula jedini neregularan element u $\mathbb{Z}$.
Ako je, opet, $R = \mathbb{Z}_6$ prsten ostataka po modulu 6, matrica $A \in M_2(\mathbb{Z}_6)$ će biti regularna ako i samo ako je $\det A \neq 0, 2, 3, 4$.

Za element $x \in K$ kažemo da je **inverzibilan** u prstenu K ako je $xy = yx = 1$ za neki $y \in K$.
Ako sa $U(K)$ označimo skup svih inverzibilnih elemenata prstena K, onda je $(U(K), \cdot)$ grupa sadržana u K^*.

Za dva elementa a i b komutativnog prstena R kažemo da su **ekvivalentni** ili **pridruženi** u tom prstenu, i označavamo $a \sim b$, ako se može napisati $b=\lambda a$, za neki $\lambda \in U(R)$. Primetimo da je $\sim$ jedna relacija ekvivalencije u prstenu R

(a) $a \sim a$ za sve $a \in R$, jer je $a = 1 \cdot a$, $1 \in U(R)$ (refleksivnost),
(b) Za sve $a,b \in R$, $a \sim b \Leftrightarrow b \sim a$, jer je $b=\lambda a \Leftrightarrow a=\lambda^{-1} b$ (simetričnost), i slično
(c) Za sve $a,b,c \in R$, ako je $a \sim b$ *i* $b \sim c$, onda je $a \sim c$ (tranzitivnost). Zaista, ako je $b=\lambda a$ i $c=\mu b$, *za* $\lambda, \mu \in U(R)$, onda je $c=\mu\lambda a$ tj. $a \sim c$.

Na primer, $m \sim n$ u skupu celih brojeva $\mathbb{Z}$ znači da je $m = n$ ili $m = -n$ jer je skup inverzibilnih elemenata $U(\mathbb{Z}) = \{1, -1\}$.

IDEALI PRSTENA

Svaki neprazan podskup U datog prstena $(K,+,\cdot)$ koji zadovoljava uslove

I1) $(U,+)$ je podgrupa grupe $(K,+)$, i

I2) $a\in K,\ u\in U \Rightarrow a\cdot u\in U$

nazivamo **levim idealom** prstena K.

Slično, svaku aditivnu podgrupu $(U,+)$ grupe $(K,+)$ prstena $(K,+,\cdot)$ zatvorenu za desno množenje tj. u kojoj je

$a\in K,\ u\in U \Rightarrow u\cdot a\in U$

nazivamo **desnim idealom** prstena K.

Obostrani ideal, ili naprosto **ideal** je svaki podskup U u prstenu K koji je istovremeno i levi i desni ideal u tom prstenu tj. za koji važi

$a\in K,\ u\in U \Rightarrow a\cdot u,\ u\cdot a\in U$

Ukoliko je sam prsten K komutativan, tada se njegovi levi, desni i obostrani ideali podudaraju.

Nula-ideal prstena je onaj koji je sastavljen samo od aditivno-neutralnog člana, dok je **jedinični ideal** onaj koji se podudara sa samim prstenom, naime iz drugog uslova ideala upravo sledi da je tu i $1\in U$ ako i samo ako je $U=K$.

Primer 3. Za element a komutativnog prstena R kažemo da je **nilpotentan** ako je $a^n=0$ za bar jedan $n\in N$. Skup $Nil(R)$ svih nilpotentnih elemenata komutativnog prstena R predstavlja jedan ideal tog prstena koji nazivamo i njegovim **nilradikalom**.

$$Nil(R)=\{x\in R \mid (\exists n\in N)\ x^n=0\}$$

1) Dokažimo najpre da je $(Nil(R),+)$ podgrupa grupe $(R,+)$.

Neka su elementi $x,y\in Nil(R)$. Tada postoje prirodni brojevi m i n takvi da je $x^m=0$ i $y^n=0$.

Kako je $$(x+y)^{m+n}=\sum_{k=1}^{m+n}\binom{m+n}{k}\underbrace{x^{m+n-k}}_{0}\cdot\underbrace{y^k}_{\text{ili } 0}=0,$$ za $m+n\in N$,

sledi da element $x+y$ pripada skupu $Nil(R)$.

Naime, ako je $k<n$ biće $m+n-k>m$, pa je tada $x^{m+n-k}=0$, a ako je $k\geq n$ onda je $y^k=0$.

Nula prstena R je takođe i nula grupe $(Nil(R),+)$, jer $0^n=0$ za $\forall n\in \mathrm{N}$, otuda je $0\in Nil(R)$.

Opozit elementa $x\in Nil(R)$ je element $-x$. Zaista, $(-x)^m=(-1)^m x^m=(-1)^m\cdot 0=0$, pa $-x\in Nil(R)$.

2) Dokažimo i da za svako $a\in \mathrm{R}$, $x\in Nil(R)\Rightarrow ax,\ xa\in Nil(R)$.

Neka je $x\in Nil(R)$. To znači da postoji $m\in N$ takav da je $x^m=0$.

Najpre, važi da je $ax=xa$ jer je prsten R komutativan.

Kako je $(ax)^m=a^m x^m=a^m\cdot 0=0$, to znači da i element ax pripada skupu $Nil(R)$.

Dakle nilradikal prstena R jeste i jedan ideal tog prstena.

Ako su X i Y podskupovi nekog većeg skupa Γ, kažemo da je X pravi podskup skupa Y, i pišemo $X\subset Y$, ako i samo ako je $X\subseteq Y$ i $X\neq Y$. Isto tako, za ideal U kažemo da je **pravi ideal** prstena K ako je $U\subset K$. Dakle, $\{0\}$ je pravi ideal prstena K, dok sam K to nije.

Za sam prsten K kažemo da je **prost** ako nije trivijalan i ako nema pravih ideala. Jasno je da to svojstvo imaju npr. svako polje ili telo.

Primer 4. Neka je $K = M_2(\mathbb{Z})$ skup kvadratnih matrica formata 2x2 sa komponentama iz skupa celih brojeva $\mathbb{Z}$. Kada se operacije nad matricama sa racionalnim komponentama iz $M_2(\mathbb{Q})$ ograniče na celobrojne komponente, jasno je da $(K,+,\cdot)$ predstavlja jedan nekomutativni prsten. Takođe,

a) Skup $U=\left\{\begin{bmatrix}0 & 0\\ x & y\end{bmatrix} \mid x,y\in\mathbb{Z}\right\}$ je pravi desni ideal prstena K.

Zaista, za svake dve matrice $A,\ B\in U$ i njihov zbir $A+B$ pripada skupu U, a za proizvoljnu matricu $T\in K$, proizvod AT takođe pripada skupu U.

Neka je $T=\begin{bmatrix}a & b\\ c & d\end{bmatrix}$, $a,b,c,d\in\mathbb{Z}$, tada je

$$\begin{bmatrix}0 & 0\\ x & y\end{bmatrix}\begin{bmatrix}a & b\\ c & d\end{bmatrix}=\begin{bmatrix}0 & 0\\ xa+yc & xb+yd\end{bmatrix}\in U.$$

b) Slično, skup $V=\left\{\begin{bmatrix}x & 0\\ y & 0\end{bmatrix} \mid x,y\in\mathbb{Z}\right\}$ je pravi levi ideal prstena K.

I ovde za svake dve matrice $A,\ B\in V$ važi da i njihov zbir $A+B$ pripada skupu V, kao i da za proizvoljnu matricu $T\in K$, proizvod TA pripada skupu V.

Neka je $T=\begin{bmatrix}a & b\\ c & d\end{bmatrix}$, $a,b,c,d\in\mathbb{Z}$, tada

$$\begin{bmatrix}a & b\\ c & d\end{bmatrix}\begin{bmatrix}x & 0\\ y & 0\end{bmatrix}=\begin{bmatrix}ax+by & 0\\ cx+dy & 0\end{bmatrix}\in V.$$

c) Skup $W=\left\{\begin{bmatrix}x & y\\ t & z\end{bmatrix} \mid x,y,z,t \text{ su parni celi brojevi}\right\}$ je takođe pravi ideal u K.

Naime, komponente koje nastaju kao zbir ili proizvod parnih komponenata u matricama biće takođe parni brojevi.

Ako je prsten R komutativan, to svojstvo ima i svaki od skupova

$$aR=\{ap \mid p\in R\},\ \text{gde } a\in R.$$

Ovakve skupove zovemo **glavnim idealima** prstena R. Takođe kažemo da je ideal aR generisan elementom $a\in R$ pri čemu se često koristi oznaka $\langle a\rangle = aR$. Posebno je $0R=\{0\}$ nula-ideal tj. trivijalni ideal koji je sastavljen samo od aditivnog neutrala, dok je $1R = R$ jedinični ideal koji se podudara sa samim prstenom. Pošto je $0\neq 1$, prsten R uvek sadrži bar dva ideala, $\{0\}$ i R.

Neka je, sada, R bilo koji komutativan domen i elementi $a,b\in R$. Za element $a\neq 0$ kažemo da **deli** element b u prstenu R, i pišemo $a \mid b$, ako je $b = aq$ za bar jedno, a time i tačno jedno $q\in R$. To upravo znači da je tada $b\in aR$, pa je zato i

$$a \mid b \Leftrightarrow bR \subset aR,\ \text{gde je } aR=\{ax \mid x\in R\}\ \text{glavni ideal prstena } R.$$

Ovako definisana relacija deljivosti, $\mid$, je očigledno refleksivna i tranzitivna, ali ne mora biti i antisimetrična tj. ovde je za svaka dva elementa $a,b\in R$

$$a \mid b \wedge b \mid a \Leftrightarrow b=aq \wedge a=bp$$

pa je $a = aqp$, a kako je R oblast celih, element $a\neq 0$ je regularan, te je $pq = 1$, odakle sledi da je element p inverzibilan, $p\in U(R)$. Dakle, elementi a i b su pridruženi, $a\sim b$, u prstenu R, pa važi

$$a \mid b \wedge b \mid a \Leftrightarrow a\sim b \Leftrightarrow aR = bR.$$

Posebno, svaki element iz R deli 0, a ako $0 \mid y$ onda je $y = 0$.

Za komutativan prsten R kažemo da je glavni ili **glavnoidealski** ako su svi ideali u tom prstenu glavni, tj. ako je svaki ideal $U = xR$ za neki $x \in U$. Drugim rečima, prsten R je glavnoidealski ako je svaki njegov ideal generisan (određen) jednim uočenim elementom. Na primer, prsten celih brojeva $(\mathbb{Z}, +, \cdot)$ je glavnoidealski jer su svi njegovi ideali generisani pojedinim celim brojevima, tj. oblika $k\mathbb{Z}$ za neki ceo broj k. Posebno, sam prsten $\mathbb{Z}$ je generisan jedinicom.
Glavnoidealski prsten koji je i oblast celih (domen) nazivamo **glavnoidealskim domenom**.
Pored pomenutog prstena celih brojeva $\mathbb{Z}$, i prsten polinoma $F[X]$ nad bilo kojim poljem F je jedan glavnoidealski domen. Razmotrimo ovu tvrdnju u sledećem primeru

Primer 5. Neka je $U \subseteq K$ bilo koji ideal u prstenu polinoma $K=F[X]$ nad poljem F. Tada je ili
- $U = \{0\} = 0 \cdot K$ što je trivijalan slučaj, ili je
- $U \neq \{0\}$ pa postoji neki ne-nula polinom $p \in U$. Samim tim, postoji i polinom najmanjeg stepena $b \in U$, $b \neq 0$. Kako je U jedan ideal, to je $ba \in U$ za svaki $a \in K$, pa je otuda

$$bK \subset U \qquad (1)$$

Uočimo sada bilo koji element $p \in U$. Kako je svakako $p \in K = F[X]$, može se zapisati u obliku $p = bq + r$, gde je r polinom manjeg stepena od b, $d^\circ r < d^\circ b$. Odatle je $r = p - bq$, pa $r \in U$, jer je $(U,+)$ podgrupa grupe $(K,+)$. Međutim, to se protivi pretpostavci da je b polinom najmanjeg stepena u idealu U, pa zato mora biti $r = 0$. Dakle, $p = bq$, $q \in K$, što znači da je

$$U \subset bK \qquad (2)$$

Sada, iz relacija (1) i (2) sledi da je $U = bK$, drugim rečima proizvoljni ideal U je i glavni ideal u prstenu K. Dakle, svi ideali u prstenu polinoma $F[X]$ nad bilo kojim poljem F jesu glavni, pa je prsten $F[X]$ glavnoidealski.

■

Naravno, komutativan prsten R može biti glavnoidealski i ako nije domen. Na primer, domen $\mathbb{Z}$ je glavnoidealski, dok će glavnoidealski prsten $\mathbb{Z}/n\mathbb{Z}$ biti i domen jedino ako je n prost broj.

Neka je skup U ideal prstena $(K,+,\cdot)$. Količnički skup

$$K/U = \{a+U \mid a \in K\}$$

koji je pri tom komutativna grupa u odnosu na operaciju $(a+U) + (b+U) = (a+b) + U$ i monoid u odnosu na $(a+U)\cdot(b+U) = ab + U$, nazivamo **količničkim prstenom** prstena K po idealu U.
Nula ovog prstena je upravo sam ideal $U = 0+U$, a jedinica $1+U$.
Prsten K/U nema pravih delitelja nule ako i samo ako je relacija $(a+U)\cdot(b+U) = 0 + U$ moguća jedino za $a+U = U$ ili $b+U = U$, odnosno ako i samo ako $ab \in U \Rightarrow a \in U \vee b \in U$.
S tim u vezi, za ideal U prstena K kažemo da je **prost** ako je $U \neq K$ i ako za svako $a,b \in K$ važi $ab \in U \Rightarrow a \in U \vee b \in U$.

Primer 6. U prstenu celih brojeva $(\mathbb{Z}, +, \cdot)$ skup sadržalaca broja 3 je jedan ideal. Zaista ovaj prsten je komutativan, zbir dva sadržaoca broja 3 je i sam deljiv sa 3, i ako se neki sadržalac broja 3 pomnoži bilo kojim celim brojem dobiće se ponovo broj deljiv sa 3.
Dakle, ideal $3\mathbb{Z} = \{3k \mid k \in \mathbb{Z}\}$ je glavni jer je generisan jednim elementom, $3 \in \mathbb{Z}$, a pored toga je i jedan prost ideal, jer ako je proizvod dva broja deljiv sa 3 tada je bar jedan od tih brojeva sadržalac broja 3.
Nasuprot tome, ideal sadržalaca broja 4 neće biti prost ideal, jer je $4 = 2\cdot 2$ i broj 4 je član tog ideala dok broj 2 to nije.

Ideal U prstena K nazivamo **maksimalnim** ako je pravi ideal koji nije sadržan ni u jednom drugom pravom idealu prstena K.
Posebno, bilo koji komutativan ne-nula prsten R sa jedinicom ima bar jedan maksimalan ideal (Krullova[1] teorema). Dokaz ove teoreme se oslanja na Zornovu[2] lemu (Ako svaki lanac u nepraznom i uređenom skupu A ima gornju granicu, onda i sam skup A ima maksimalni element.)

Primer 7. Razmotrimo dokaz Krullove teroeme:

Označimo sa $\mathfrak{I}$ skup koji se sastoji od svih pravih (dvostranih) ideala u prstenu R, koji je neprazan pošto sadrži bar trivijalni ideal $\{0\}$. Ovaj skup je parcijalno uređen relacijom "biti podskup", $(\mathfrak{I}, \subseteq)$. Pokažimo da postoji maksimalan element u skupu $\mathfrak{I}$. Sam ideal R ne razmatramo, jer su maksimalni ideali po definiciji različiti od R.

Neka je T jedan lanac, tj. potpuno uređen podskup skupa $\mathfrak{I}$. Pokažimo da T ima gornju granicu, odnosno da postoji ideal koji je veći od svih ostalih članova u T, ali još uvek manji od samog R, jer inače ne bi mogao biti u skupu $\mathfrak{I}$.

Označimo sa $\mathfrak{A}$ uniju svih ideala u skupu T i pokažimo najpre da je $\mathfrak{A}$ jedan ideal.

Ako su a i b elementi iz $\mathfrak{A}$, onda postoje dva ideala J i $K \in T$ takva da je $a \in J$ i $b \in K$. Pošto je skup T potpuno uređen, mora biti $J \subseteq K$ ili $K \subseteq J$. U prvom slučaju oba elementa a i b pripadaju idealu K, pa stoga i njihova suma $a+b$ pripada idealu K takođe, što pokazuje da je $a+b \in \mathfrak{A}$.

U drugom slučaju, oba elementa a i b pripadaju idealu J, pa slično zaključujemo da $a+b \in \mathfrak{A}$. Nadalje, ako je $r \in R$, onda element ar pripada idealu J, pa sledi da $ar \in \mathfrak{A}$. I slično, $br \in \mathfrak{A}$. Ovim smo pokazali da je unija $\mathfrak{A}$ svih ideala u skupu T takođe jedan ideal u prstenu R.

Konačno, proverimo da li je ideal $\mathfrak{A}$ manji od R. Ako bi $\mathfrak{A}$ bio jednak prstenu R onda bi morao da sadrži jedinicu, a s druge strane, ako $1 \in \mathfrak{A}$ i ako je $r \in R$ proizvoljan element, onda je $r \cdot 1 = r$ takođe element ideala, pa je taj ideal jednak sa R. Znači, kada bi ideal $\mathfrak{A}$ bio jednak sa R onda bi on sadržao jedinicu, što znači da bi tada neki od ideala, članova skupa T, sadržao jedinicu i zbog toga bi i sam bio jednak prstenu R, ali u tom slučaju on ne bi bio pravi ideal kako smo na početku pretpostavili.

Ovo nam upravo omogućava primenu Zornove leme, na osnovu koje sledi da je maksimalni element skupa $\mathfrak{I}$, ujedno i maksimalni ideal prstena R.

■

Dakle, u slučaju komutativnog prstena R, element $x \in R$ nije inverzibilan ako i samo ako je sadržan u nekom maksimalnom idealu prstena R. Naime, ako bi maksimalni ideal U sadržao inverzibilni element $y \in R$, onda bi sadržao i proizvod $y^{-1}y = 1$, za inverz $y^{-1} \in R$, jer je U ideal, a to znači da bi tada sadržao i jedinicu, odnosno podudarao bi se sa samim prstenom R, što je u suprotnosti sa tvrdnjom da je U maksimalan. Obratno, ako element $x \in R$ nije inverzibilan, onda on generiše pravi ideal xR, jer ne sadrži jedinicu, pa je tada ideal xR sadržan u nekom maksimalnom idealu prstena R. Drugim rečima, maksimalni ideali prstena ne sadrže jedinicu (multiplikativni neutral) tog prstena niti njegove inverzibilne elemente.

Svakako, važan primer ideala proizvoljnog prstena K je njegov **Jacobsonov**[3] **radikal** $J(K)$.

Označimo sa $L(K)$ skup svih pravih levih ideala prstena K. To je neprazan skup, jer je $\{0\} \subset L(K)$. Možemo urediti elemente skupa $L(K)$ relacijom poretka „biti podskup", $\subseteq$. Na osnovu Zornove leme, skup $L(K)$ ima maksimalan element, neka je to levi ideal $U \in L(K)$. Dakle, ako je $B \in L(K)$

[1] Wolfgang Krull (1899 – 1971.god.), nemački matematičar
[2] Max August Zorn (1906 – 1993.god.), nemački matematičar
[3] Nathan Jacobson (1910 - 1999.god.), američki matematičar

levi ideal prstena K i $U \subseteq B$, onda je $U=B$ jer je ideal U maksimalan u $L(K)$ s obzirom na relaciju parcijalnog uređenja $\subseteq$. Presek svih maksimalnih levih ideala prstena K nazivamo Jacobsonovim radikalom prstena K i označavamo sa

$$J(K)= \cap \{ U \in L(K) \mid U \text{ je maksimalan levi ideal} \}.$$

Analogno, Jacobsonov radikal prstena bi mogli definisati i kao presek svih maksimalnih desnih ideala u tom prstenu. Ukoliko je prsten R komutativan, onda se skup svih levih ideala prstena R poklapa sa skupom svih desnih ideala, odnosno sa skupom svih ideala tog prstena, pa je Jacobsonov radikal $J(R)$ komutativnog prstena R naprosto presek svih njegovih maksimalnih ideala. Jasno je da je, kao takav, Jacobsonov radikal prstena i sam jedan pravi ideal u tom prstenu.

Navedimo sada tvrđenja koja bliže određuju elemente Jacobsonovog radikala prstena.

Tvrđenje 1. Jacobsonov radikal $J(K)$ prstena K je skup svih elemenata $r \in K$ sa svojstvom da je element $1- kr$ inverzibilan sleva u prstenu K, za svaki $k \in K$.

Dokaz: Neka su $r \in J(K)$, $k \in K$. Razmotrimo levi ideal $K(1- kr)$.
Ako je $K(1- kr) = K$, onda $1 \in K(1- kr)$, pa je $y(1- kr) = 1$ za neki $y \in K$, odnosno element $1- kr$ je inverzibilan sleva.
Ako je $K(1- kr) \neq K$, onda je ideal $K(1- kr)$ sadržan u nekom pravom maksimalnom levom idealu U. Tada je $1- kr \in U$ pa kako je $kr \in J(K) \subset U$, zaključujemo da mora biti $1 \in U$, međutim to bi značilo da je $U=K$, a to je kontradikcija.
Neka je sada element $1- kr$ inverzibilan sleva za svaki $k \in K$. Ako $r \notin J(K)$, onda postoji pravi maksimalni levi ideal V takav da $r \notin V$, pa je otuda $Kr + V = K$, odnosno $kr + j = 1$, pa za element $j \in V$, $j = 1- kr$ ispada da nije inverzibilan jer pripada pravom maksimalnom idealu V, a to je kontradikcija, pa element $r \in J(K)$.

■

Odgovarajuća računska predstava kada govorimo o Jacobsonovom radikalu prstena je kvaziregularnost.
Da bismo uveli pojam kvaziregularnog elementa u prstenu K, definišimo najpre novu operaciju $\circ$ za proizvoljna dva elementa $x,y \in K$ na sledeći način

$$x \circ y \overset{def}{=} x + y - xy .$$

Operacija $\circ$ definiše preslikavanje $\circ\colon K \times K \to K$ dato sa $\circ\colon (x,y) = x \circ y$.

Primer 8. Pokažimo da je struktura $(K, \circ, 0)$ jedan asocijativni monoid u odnosu na operaciju $\circ$.

Zaista, kako je $(K, +, \cdot)$ prsten u odnosu na sabiranje i množenje, to za bilo koje $x,y \in K$ i element $x \circ y$ pripada skupu K, jer

$$x \circ y = \underbrace{x + y}_{\in K} - \underbrace{xy}_{\in K} ;$$

Za sve $x,y,z \in K$ važi $x \circ (y \circ z) = x \circ (y + z - yz) = x + y + z - yz - x(y + z - yz) =$

$$= x + y + z - yz - xy - xz + xyz =$$
$$= x + y - xy + z - (x + y - xy)z =$$
$$= (x \circ y) + z - (x \circ y)z = (x \circ y) \circ z ,$$

tj. operacija $\circ$ je asocijativna.

Neka je $0 \in K$ nula u prstenu K. Tada je $0 \circ x = 0 + x - 0 \cdot x = x = x + 0 - x \cdot 0 = x \circ 0$,
pa sledi da je 0 ujedno i neutral u monoidu $(K, \circ)$.

Neka je K dati prsten. Za element $x \in K$ kažemo da je **kvaziregularan** sleva ako je element $y \circ x = 0$ za neki $y \in K$, tj. ako ima levi inverz u monoidu $(K, \circ, 0)$. Takav element $y \in K$ nazivamo levim **kvazi-inverzom** elementa x u prstenu K. Slično, za element $x \in K$ kažemo da je kvaziregularan zdesna ako je $x \circ z = 0$ za neki $z \in K$, koji nazivamo desnim kvazi-inverzom od x. Element $x \in K$ je kvaziregularan u prstenu K ako je kvaziregularan i sleva i zdesna u tom prstenu.
Sa ovim u vezi, za levi (desni) ideal U kažemo da **kvaziregularan** ako je svaki element tog ideala kvaziregularan sleva (odnosno, zdesna).

Primer 9. Neka je K proizvoljan prsten. Pokažimo da je element $z \in K$ kvaziregularan ako i samo ako je $z \circ y = y \circ z = 0$ za neki $y \in K$.
Po definiciji, element $z \in K$ je kvaziregularan u prstenu K ako je kvaziregularan i sleva i zdesna u tom prstenu. Dakle, $z \circ x = 0$ za neki $x \in K$, i $y \circ z = 0$ za neki $y \in K$.
Pošto je operacija $\circ$ asocijativna, važi $y = y \circ 0 = y \circ (z \circ x) = (y \circ z) \circ x = 0 \circ x = x$.
Znači $y = x$, odnosno $z \circ y = 0 = y \circ z$, pa možemo reći da su kvaziregularni elementi u prstenu K upravo oni elementi koji su inverzibilni u monoidu $(K, \circ, 0)$.

■

Lema 1. Neka je K prsten.

1) Element $x \in K$ je kvaziregularan sleva (zdesna) ako i samo ako je element $1 - x$ inverzibilan sleva (zdesna) u prstenu K.
2) Element $x \in K$ je kvaziregularan ako i samo ako je element $1 - x$ inverzibilan u prstenu K.
3) Ako je levi (ili desni) ideal U prstena K kvaziregularan, onda je svaki element tog ideala kvaziregularan.

Dokaz:

1) ($\Rightarrow$) Neka je element $x \in K$ kvaziregularan sleva u prstenu K. Tada je $y \circ x = 0$ za neki $y \in K$, tj. $y + x - yx = 0$. Dakle, $1 + y + x - xy = 1$, odnosno $1 - y - x + xy = 1$, pa je $(1 - y)(1 - x) = 1$ što upravo znači da je element $1 - x$ inverzibilan sleva u prstenu K.
($\Leftarrow$) Obratno, pretpostavimo da je element $1 - x$ inverzibilan sleva u prstenu K, tj. da postoji neko $z \in K$ za koje je $z(1 - x) = 1$. Neka je $z = 1 - y$, za neki element $y \in K$. Tada je $(1 - y)(1 - x) = 1$, što je ekvivalentno sa $y + x - yx = 0$ tj. $y \circ x = 0$, pa je stoga element $x \in K$ kvaziregularan sleva.
Slično se dokazuje i da je element $x \in K$ kvaziregularan zdesna u prstenu K ako i samo ako je element $1 - x$ inverzibilan zdesna u tom prstenu.

2) Dokaz sledi iz prethodnog dokaza tvrđenja (1) ove leme,

3) Neka je U kvaziregularni levi ideal u prstenu K i neka je $u \in U$ element tog ideala. Tada je element u kvaziregularan sleva po definiciji, pa važi $y \circ u = 0 = y + u - yu$ za neki $y \in K$. Pošto je U levi ideal u prstenu K, iz relacije $y + u - yu = 0$ sledi da $y \in U$. To sada znači da je i element y kvaziregularan sleva, pa je $z \circ y = 0$, za neki $z \in K$. Sada možemo ponovo upotrebiti asocijativnost i pokazati da je $z = u$. Zaista, $z = z \circ 0 = z \circ (y \circ u) = (z \circ y) \circ u = 0 \circ u = u$. Dakle, $u \circ y = y \circ u = 0$, pa svaki element $u \in U$ jeste kvaziregularan.
Slično se dokazuje i da je svaki element kvaziregularnog desnog ideala kvaziregularan.

■

Primer 10. Neka je K proizvoljan prsten. Pokažimo da je svaki nilpotentni element prstena K kvaziregularan.

Najpre, podsetimo se, za element $x\in K$ kažemo da je nilpotentan u prstenu K ako je $x^n=0$ za bar jedan $n\in N$. Dakle, neka je element $x\in K$ nilpotentan. Pođimo od faktorizacije

$$1 - x^n = (1- x)(1+ x + .. + x^{n-1}) .$$

Ako uvedemo smenu $1+ x+ .. +x^{n-1} = y\in K$ i uzmemo u obzir da je $x^n=0$, onda je $(1- x)\cdot y =1$, što znači da je element $1- x$ inverzibilan u prstenu K. Na osnovu leme 1 (2) to upravo znači da je element $x\in K$ kvaziregularan u prstenu K.

■

Već smo napomenuli da je kvaziregularnost pogodan koncept za računsko određivanje Jacobsonovog radikala prstena. Konkretno, svaki element Jakobsnovog radikala prstena je kvaziregularan, dok s druge strane, ne mora svaki kvaziregularni element u prstenu pripadati Jacobsnovom radikalu. Važi sledeća

Teorema 1. Neka je K prsten.

1) Jacobsonov radikal $J(K)$ prstena K je kvaziregularni levi ideal koji sadrži svaki kvaziregularni levi ideal u K.
2) Jacobsonov radikal $J(K)$ prstena K je skup
$$J(K) = \{ z\in K \mid Kz \text{ je kvaziregularan levi ideal}\}.$$

Dokaz: 1) Neka je $z\in J(K)$. Pretpostavimo da element z nije kvaziregularan sleva. Tada, prema lemi 1 sledi da $1- z$ nije inverzibilan sleva u prstenu K, a to, ekvivalentno, znači da je skup $K(1- z)$ pravi levi ideal u prstenu K. Prema Zornovoj lemi, postoji maksimalni levi ideal U prstena K takav da je $K(1- z) \subseteq U$, pa pošto tada $1- z\in U$ i $z\in J(K) \subset U$ jer je $J(K)$ presek svih maksimalnih levih ideala, to bi značilo da i $1\in U$ što je nemoguće, pa zaključujemo da element z mora biti kvaziregularan sleva, a kako je to proizvoljno izabran element skupa $J(K)$, sledi da je i sam Jacobsonov radikal $J(K)$ prstena K jedan kvaziregularan levi ideal u K.
Neka je sada B proizvoljan kvaziregularni levi ideal u prstenu K. Pretpostavimo da se on ne sadrži u Jacobsonovom radikalu prstena, $J(K)$. Neka je U maksimalni levi ideal prstena K takav da B nije sadržano u U. Pošto je ideal U maksimalan i $U < U+B$, biće $U+B = K$. To praktično znači da je $z+b =1$ za neke $z\in U$ i $b\in B$. Kako je ideal B kvaziregularan levi ideal to je element $b\in B$ kvaziregularan, pa je stoga $z = 1- b$ inverzibilan sleva u prstenu K prema lemi 1. Ako je $yz = 1$ za neki $y\in K$, onda pošto $yz\in U$ jer je U levi ideal u K, sledi da $1\in U$ a to nije moguće. Zaključujemo zato da je $B \subseteq J(K)$.

2) Najpre, inkluzija sleva na desno sledi direktno iz tvrđenja (1) ove teoreme.
Pretpostavimo sada da je $z\in K$ i da je Kz kvaziregularan levi ideal. Tada je na osnovu tvrđenja (1) ove teoreme $Kz \subseteq J(K)$. Posebno, takav element z pripada Jacobsonovom radikalu $J(K)$.

■

Kao što smo napomenuli, Jacobsonov radikal $J(R)$ komutativnog prstena R je presek svih njegovih maksimalnih ideala. Pri tome, iz Zornove leme proističe da element $x\in R$ nije inverzibilan ako i samo ako je sadržan u nekom maksimalnom idealu prstena R. Sada na osnovu teoreme 1(2) važi da element $z\in J(R)$ ako i samo ako je element yz kvaziregularan sleva za sve $y\in R$ tj. ako i samo ako je $1-yz$ inverzibilan element u prstenu R, $1-yz\in U(R)$, za sve $y\in R$.
Konačno, s obzirom na ranija razmatranja, možemo dati sledeću karakterizaciju Jacobsonovog radikala komutativnog prstena.

Posledica 1: Neka je R komutativan prsten.

1) Jacobsonov radikal $J(R)$ prstena R je presek svih maksimalnih ideala tog prstena
$$J(R) = \cap\{\ U \mid U \text{ je maksimalni ideal u prstenu } R\ \}.$$
2) Jacobsonov radikal $J(R)$ prstena R je skup
$$J(R) = \{\ z\in R \mid 1\text{-}yz \in U(R) \text{ za sve } y\in R\}.$$ ■

Navešćemo još jedno tvrđenje u vezi sa Jacobsonovim radikalom prstena, ali uvedimo najpre pojmove dekomopozicije (razlaganja) prstena i elementa.

Neka je K prsten. Element $e\in K$ nazivamo **idempotentnim** u prstenu K ako je $\boldsymbol{e^2 = e}$.
Prsten K, koji sadrži idempotentni element e, možemo predstaviti kao direktnu sumu potprstena s obzirom na dati idempotentni element e. Takvo predstavljanje (razlaganje) prstena poznato je kao Peirceova[4] dekompozicija prstena. Postoje leva, desna i dvostrana Peirceova dekompozicija prstena, koje su definisane sa

$$K = Ke + K(1- e) \qquad \text{leva dekompozicija}$$
$$K = eK + (1- e)K \qquad \text{desna dekompozicija}$$
$$K = eKe + eK(1- e) + (1- e)Ke + (1- e)K(1- e) \quad \text{dvostrana}$$

Zaista, ako bi razmotrili, na primer, element koji pripada i potprstenu Ke i potprstenu $K(1- e)$, onda bi on bio oblika $xe\in Ke$, za $x\in K$, a takođe i $xe = y(1\text{-}e)\in K(1\text{-}e)$, $y\in K$. Međutim, množenjem jednakosti

$$xe = y(1\text{-}e)$$

sa desne strane idempotentnim elementom $e\in K$ dobijamo

$$xe^2 = y(1\text{-}e)\cdot e = y\cdot 0 = 0 \text{ , dakle } xe = 0.$$

Drugim rečima, presek skupova $Ke \cap K(1- e)$ je trivijalan, odnosno suma jeste direktna.

Ako prsten K nema neutral, onda se po definiciji stavlja da je

$$K(1\text{-}e) = \{\ x - xe \mid x\in K\},$$
$$(1\text{-}e)Ke = \{\ xe - exe \mid x\in K\}, \text{ i}$$
$$(1\text{-}e)K(1- e) = \{\ x - ex - xe + exe \mid x\in K\}.$$

Skupovi $(1- e)K$ i $eK(1- e)$ se definišu analogno.
S tim u vezi, za svaki element $x\in K$ postoje leva, desna i dvostrana Pirsova dekompozicija elementa s obzirom na idempotentni element $e\in K$, tj. svaki $x\in K$ se može razložiti na neki od sledeća tri načina

$$x = xe + (x - xe) \qquad \text{leva dekompozicija,}$$
$$x = ex + (x - ex) \quad \text{desna dekompozicija, ili}$$
$$x = exe + ex(1 - e) + (1 - e)xe + (1 - e)x(1 - e) \quad \text{dvostrana}$$

Svaki od navedenih načina zapisa elementa $x\in K$ se lako proverava množenjem sa desne strane jednakosti.

Dakle, ako je K prsten sa idempotentnim elementom $e\in K$, $e^2=e$, onda je i eKe takođe prsten sa neutralom e. Dalje, prsten eKe ima svoj Jacobsonov radikal $J(eKe)$ koji je i jedan ideal u tom prstenu. S druge strane, jasno je da je skup $eJ(K)e$ takođe ideal u prstenu eKe. Sledeća lema govori da su ova dva ideala jednaka u prstenu eKe.

[4] Benjamin Peirce (1809 -1880.god.), američki matematičar

Lema 2. Neka je K prsten i $e \in K$ njegov idempotentni element. Tada za Jacobsonov radikal prstena eKe važi $J(eKe) = eJ(K)e$.

Dokaz: Dokažimo najpre da je $eJ(K)e \subseteq J(eKe)$.

Pretpostavimo da element $x \in J(K)$. Pošto je $J(K)$ presek svih maksimalnih levih (ili, analogno, desnih) ideala u prstenu K, dakle i sam jedan levi ideal u prstenu K, jasno je da tada i $ex \in J(K)$. Međutim, to znači da je element ex kvaziregularan sleva u prstenu K, odnosno da je $1- ex$ inverzibilan sleva tj. da je

$$y(1- ex) = 1, \text{ za neki } y \in K$$

Množenjem ove jednakosti sleva i zdesna sa e dobijamo

$$e \cdot y(1- ex) \cdot e = e \cdot 1 \cdot e$$

odnosno, pošto je $e^2 = e$, $\quad e \cdot y(1- ex) \cdot e = e$

$$(eye) \cdot (e - exe) = e$$

a kako je e neutral u prstenu eKe, ova poslednja jednakost znači da je element $e – exe$ inverzibilan sleva, a to dalje znači da je exe kvaziregularan sleva u prstenu eKe. Slično se pokazuje da je element exe kvaziregularan i zdesna, pa kako je, dakle, proizvoljan element $exe \in eJ(K)e$ kvaziregularan, zaključujemo da je i sam ideal $eJ(K)e$ kvaziregularan. Prema teoremi 1(1) Jacobsonov radikal $J(eKe)$ prstena eKe sadrži sve kvaziregularne ideale tog prstena, pa je zato $eJ(K)e \subseteq J(eKe)$.

Dokažimo sada i da je $J(eKe) \subseteq eJ(K)e$.

Neka je $z \in J(eKe)$ i neka je $a \in K$ proizvoljni element. Element a možemo predstaviti razloženog po dvostranoj Peirceovoj dekompoziciji na sledeći način

$$a = eae + ea(1- e) + (1- e)ae + (1- e)a(1- e).$$

Sada je $\quad za = zeae + zea(1- e) + z(1- e)ae + z(1- e)a(1- e)$

ali kako je $z(1- e) = 0$ jer $z \in eKe$

imamo da je $\quad za = zeae + zea(1- e).$

Kako je $z \in J(eKe)$, a Jacobsonov radikal $J(eKe)$ je jedan ideal u prstenu eKe, onda je i $zeae \in J(eKe)$. To znači da je element $zeae$ kvaziregularan u prstenu eKe, odnosno da postoji element $z' \in eKe$ koji je kvazi-inverz elementa $zeae$. Dakle,

$zeae \circ z' = z' \circ zeae = 0$, u prstenu eKe.

Pošto je $eKe \subseteq K$, onda prethodna relacija važi i u prstenu K, tj. element $zeae$ je kvaziregularan i u prstenu K. Dakle, po definiciji operacije $\circ$ važi

$$za \circ z' = [zeae – zea(1- e)] \circ z' = zeae + zea(1- e) + z' – (zeae + zea(1- e))z' =$$
$$= zeae \circ z' + zea(1- e) – zea(1- e)z' = zea(1- e)$$

jer je, kao što smo videli, $zeae \circ z' = 0$ i $zea(1- e)z' = 0$ jer $z' \in eKe$.

Dakle,

$$za \circ z' = zea(1- e) \qquad (*)$$

Element $zea(1- e)$ je, međutim, nilpotentan stepena $n \leq 2$ jer je $z \in eKe$, pa na osnovu jednakosti (*) element $za \circ z'$ kvaziregularan. Kako je rezultat operacije $\circ$ nad dva kvaziregularna zdesna elementa takođe element kvaziregularan zdesna, to je

$$za = za \circ 0 = za \circ (z' \circ zeae) = (za \circ z') \circ (zeae)$$

pa je i element za kvaziregularan zdesna. Dakle, upravo smo pokazali da je za proizvoljan $z \in J(eKe)$ i element za kvaziregularan zdesna u prstenu K, za bilo koje $a \in K$, pa je $J(eKe)$ kvaziregularan ideal u K. Na osnovu teoreme 1 (1) važi da je $J(eKe) \subseteq J(K)$.

Sada je $eKe \cap U = eUe$ za bilo koji ideal U prstena K. Zbog toga je

$J(eKe) \subseteq eKe \cap J(K) = eJ(K)e$, odnosno $J(eKe) \subseteq eJ(K)e$, pa je zato $J(eKe) = eJ(K)e$.

■

MODULI NAD KOMUTATIVNIM PRSTENIMA

Modul $(M, +, \cdot)$ nad komutativnim prstenom R je algebarska struktura sa jednom binarnom operacijom $(u, v) \to u+v$ u skupu M, i jednom spoljnom operacijom $(\alpha, u) \to \alpha \cdot u$, $\alpha \in R$, $u \in M$ koje zadovoljavaju uslove:

M1) $(M, +)$ je komutativna grupa,

M2) $\alpha \cdot (u+v) = \alpha \cdot u + \alpha \cdot v$,

M3) $(\alpha+\beta) \cdot u = \alpha \cdot u + \beta \cdot v$,

M4) $\alpha \cdot (\beta u) = (\alpha\beta) \cdot u$,

M5) $1 \cdot u = u$.

Operacije modula M nad prstenom R obično obeležavamo sa + i $\cdot$ i nazivamo sabiranjem i množenjem skalarima, a elemente samog prstena R skalarima u tom modulu M.

Neka je M jedan R-modul, i neka je $\Gamma = \{ m_\alpha \mid \alpha \in \Delta \}$ podskup u M.

Uvedimo sada osnovne pojmove koji se odnose na bazu R-modula:

- Skup Γ je **generatrisa** R-modula M ako svaki element $m \in M$ možemo predstaviti kao konačnu linearnu kombinaciju elemenata iz Γ. Elemente generatrise Γ nazivamo **generatorima** modula M. Dakle, Γ je generatrisa modula M ako se svaki element $m \in M$ može predstaviti kao kombinacija $m = x_1 m_{\alpha(1)} + x_2 m_{\alpha(2)} + \ldots + x_n m_{\alpha(n)}$ konačno mnogo elemenata $m_{\alpha(1)}, m_{\alpha(2)}, \ldots, m_{\alpha(n)} \in \Gamma$ i skalara $x_1, x_2, \ldots, x_n \in R$. Pri tom, to što je skup Γ generatrisa modula M ne mora da znači da postoji samo jedan način da se element $m \in M$ izrazi kao linearna kombinacija generatora iz generatrise Γ.

- Za konačan podskup $\{ m_{\alpha(1)}, m_{\alpha(2)}, \ldots, m_{\alpha(n)} \}$ različitih elemenata skupa Γ kažemo da je **linearno nezavisan** nad prstenom R ako je relacija $x_1 m_{\alpha(1)} + x_2 m_{\alpha(2)} + \ldots + x_n m_{\alpha(n)} = 0$ za proizvoljne skalare $x_i \in R$ moguća jedino kada je $x_1 = x_2 = \ldots = x_n = 0$.

- Sam skup Γ je linearno nezavisan nad prstenom R ako je svaki konačan podskup različitih elemenata skupa Γ linearno nezavisan nad R.

- Skup Γ je **baza** R-modula M ako je generatrisa tog modula i ako je linearno nezavisan nad prstenom R. U tom slučaju se svaki ne-nula element $m \in M$ može na jedinstven način predstaviti kao linearna kombinacija elemenata iz Γ. Drugim rečima, postoje jednoznačno određeni indeksi $\alpha_{(1)}, \alpha_{(2)}, \ldots, \alpha_{(n)} \in \Delta$ i jedinstveni ne-nula skalari $x_1, x_2, \ldots, x_n \in R$ takvi da se svaki element $m \in M$ može izraziti kao $m = x_1 m_{\alpha(1)} + x_2 m_{\alpha(2)} + \ldots + x_n m_{\alpha(n)}$. Naravno, i element $m=0$ se može zapisati kao $m = 0 \cdot m_\alpha$, za bilo koji $\alpha \in \Delta$.

- Modul M je **slobodan *R*-modul** ako ima bar jednu bazu, tj. bar jednu linearno nezavisnu generatrisu. Dakle, i nula-modul $\{0\}$ je jedan slobodan R-modul sa praznim skupom $\varnothing$ kao bazom. Naravno, postoje i moduli koji nisu slobodni. Takav je, na primer, svaki od modula $\mathbb{Z}_k$ nad prstenom celih brojeva $\mathbb{Z}$. Naime, u njemu je $ku=0$ za svako $u \in \mathbb{Z}$, pa on nema pravih linearno nezavisnih podskupova.

- Za R-modul M kažemo da je konačnog tipa ili **konačno generisan** ako ima konačnu generatrisu $\Gamma = \{m_1, m_2, ..., m_n\}$. To još ne mora značiti da je generatrisa Γ i baza.

- Broj elemenata baze nazivamo i **dimenzijom** ili rangom uočenog slobodnog modula M. Pri tom, ako slobodan R-modul ima bar jednu konačnu generatrisu, onda su sve njegove generatrise konačne i imaju isti broj elemenata. Dokaz ove tvrdnje, kao i nastavak razmatranja o rangu modula navode se u poslednjem poglavlju ovog teksta.

Primer 11. a) Za svaki komutativan prsten R i svaki prirodan broj n, skup svih uređenih n-torki

$$R^n = \{(x_1, x_2, ..., x_n) \mid x_1, x_2, ..., x_n \in R\}$$

je jedan R-modul u odnosu na sabiranje i množenje skalarom

$$(a_1, a_2, ..., a_n) + (b_1, b_2, ..., b_n) = (a_1+b_1, a_2+b_2, ..., a_n+b_n),$$

$$\alpha\cdot(a_1, a_2, ..., a_n) = (\alpha a_1, \alpha a_2, ..., \alpha a_n).$$

Ovaj modul nazivamo **koordinatnim** R-modulom. Njegova nula je n-torka (0, 0,....,0), gde je $0=0_R$. Modul R^n je slobodan i konačno generisan R-modul svojom kanonskom bazom $\varepsilon = \{\varepsilon_1, \varepsilon_2, ..., \varepsilon_n\}$ koju čine n-torke $\varepsilon_1 = (1,0,...,0)$, $\varepsilon_2 = (0,1,...,0)$, ..., $\varepsilon_n = (0,0,...,1)$. Stoga je jasno da je rang ovog modula $r(R^n) = n$.
Posebno, za $n = 1$, sam prsten R je modul nad samim sobom, pri čemu se jednorka (x_1) poistovećuje sa elementom x_1 prstena, tj. $R^1=R$.

b) Svaki komutativan prsten R je modul nad bilo kojim njegovim potprstenom L, u kome $u+v$ i $\alpha\cdot u$ imaju ista značenja kao i u samom prstenu R. Tu posebno može biti i $R=L$, pa je sam prsten R i jedan R-modul sa skupom $\{1\}$ kao bazom, kao što smo već napomenuli.

Neka je M modul nad komutativnim prstenom R.
Skup $Ann(m) = \{x\in R \mid xm=0\}$ naziva se **anulatorom** uočenog elementa $m\in M$. Slično, skup $Ann(M) = \{x\in R \mid xm=0 \text{ za sve } m\in M\}$ naziva se anulatorom modula M. Oba pomenuta skupa, i $Ann(m)$ i $Ann(M)$, su ideali prstena R, pri čemu je $Ann(M) = \cap\{Ann(m) \mid m\in M\}$. Naravno, ako je M jedan slobodan ne-nula R-modul onda je $Ann(M) = \{0\}$.

Primer 12. Neka je $m\in M$ fiksiran element R-modula M. Dokažimo da je anulator $Ann(m)=\{x\in R \mid xm=0\}$ tog elementa i jedan (dvostrani) ideal u prstenu R.
Neka su $a,b\in$Ann(m) proizvoljni elementi. To znači da je $am=0$ i $bm=0$. Kako su $a,b\in R$, $m\in M$, to prema uslovu M3) modula važi

$$(a+b)\cdot m = am + bm = 0 + 0 = 0, \quad \text{pa je i } a+b\in Ann(\text{m}).$$

Nula prstena R takođe pripada anulatoru, naime $0_R\cdot m = 0_M$, pa je $0\in Ann(m)$, kao i opozit elementa $a\in Ann(m)$, jer $(-a)\cdot m = (-1)\cdot am = -1\cdot 0 = 0$, dakle $-a\in Ann(m)$. Ovim smo pokazali da $(Ann(m),+)$ jeste jedna podgrupa grupe (R,+).
Neka je sada $r\in R$, $a\in Ann(m)$. Tada prema uslovu M4) važi

$$(ar)\cdot m = (ra)\cdot m = r\cdot(am) = r\cdot 0 = 0, \quad \text{pa i elementi } ar, ra\in Ann(m).$$

Naravno, $ar = ra$ jer je prsten R komutativan. Dakle, $Ann(m) = \{x\in R \mid xm=0\}$ jeste jedan dvostrani ideal prstena R.

Za element $x\in R$ kažemo da je **delitelj nule** u R-modulu M ako postoji ne-nula element $m\in M$ takav da važi $xm=0$. Ako označimo skup delitelja nule modula M sa $Z(M)$ jasno je da tada važi $Z(M) = \cup\{Ann(m) \mid m\in M\setminus\{0\}\}$.

Sistem elemenata R-modula M može biti linearno zavisan i u slučaju kada ni jedan od njih nije linearna kombinacija preostalih. Štaviše, u modulu ne mora da važi da je $au = 0 \Leftrightarrow a=0 \vee u=0$.
S tim u vezi, za element $u \in M$ kažemo da je **torzioni** ako je $au = 0$ za bar jedno $a \neq 0$ iz prstena R. U suprotnom, taj element je torziono slobodan. Za sam modul M kažemo da je torzioni ako su to i svi njegovi elementi.

Za modul N nad prstenom skalara K kažemo da je **podmodul** datog R-modula M ako su njegove operacije podoperacije odgovarajućih operacija samog tog modula M. To posebno znači da je $N \subset M$ i da ovi moduli imaju isti prsten skalara $K=R$, kao i da za svako $m,n \in M$ važi

1) $m,n \in N \Rightarrow m+n \in N$,
2) $\alpha \in R,\ m \in N \Rightarrow \alpha \cdot m \in N$.

Privedimo ovu oblast kraju uvođenjem osnovnih pojmova koji se tiču homomorfizama R-modula. Neka su M i N dva modula nad nad komutativnim prstenom R.

- Za preslikavanje $f\colon M \to N$ kažemo da je jedan **homomorfizam** modula M u modul N nad istim prstenom skalara R, ako je saglasno sa parovima njihovih odgovarajućih operacija, tj. ako za svako $m,n \in M$ i $\alpha \in R$ važi

  H1) $f(m+n) = f(m) + f(n)$,

  H2) $f(\alpha \cdot m) = \alpha \cdot f(m)$.

  Skup svih homomorfizama R-modula M u N označavaćemo sa $Hom_R(M, N)$.

- Bijektivne (1-1 i NA) homomorfizme nazivamo **izomorfizmima**. S tim u vezi, za neki R-modul M ćemo reći da je izomorfan R-modulu N, i pisati $M \cong N$, ako postoji bar jedan izomorfizam $f\colon M \to N$. Ovako definisana relacija $\cong$ je i jedna ekvivalencija u klasi svih modula nad istim prstenom R.
- Ako je $f \in Hom_R(M, N)$ onda skup $Ker(f) = \{m \in M \mid f(m) = 0\}$ nazivamo **jezgrom** homomorfizma f.
- **Slika** homomorfizma $f \in Hom_R(M, N)$ je skup $Im(f) = \{n \in N \mid n = f(m), \text{ za neki } m \in M\}$.

Jezgro $Ker(f)$ svakog homomorfizma $f \in Hom_R(M, N)$ je i jedan R-podmodul modula M. Naravno, f je injektivno (1-1) preslikavanje ako i samo ako je $Ker(f) = \{0\}$.
Slično, slika $Im(f)$ svakog homomorfizma $f \in Hom_R(M, N)$ je uvek R-podmodul modula N. Preslikavanje f je surjektivno (NA) ako i samo ako je $Im(f) = N$.

§2 MATRICE NAD KOMUTATIVNIM PRSTENIMA

Neka je $M_{m\times n}(R)$ skup svih matrica formata $m\times n$ sa komponentama iz komutativnog prstena R. Skup $M_{m\times n}(R)$ je i jedan R-modul u odnosu na operacije sabiranja matrica i množenja matrica skalarima. Naime, ako su matrice $A,\ B\in M_{m\times n}(R)$ i $\alpha\in R$ onda su i matrice $A+B$ i αA takođe formata $m\times n$ i određene su sa

$$[A+B]_{ij}=[A]_{ij}+[B]_{ij} \qquad \text{i} \qquad [\alpha A]_{ij}=\alpha[A]_{ij},$$

gde $[A]_{ij}$ predstavlja (i,j)-tu komponentu matrice A, tj komponentu u i-toj vrsti i j-toj koloni matrice A. Nula u ovom modulu je upravo nula-matrica $\boldsymbol{O}$ čije su sva komponente nula.

Označimo sa E_{ij} matricu iz $M_{m\times n}(R)$ čije su sve komponente 0, osim što je (i,j)-ta komponenta jednaka 1 za svako $i=1, 2, ..., m$ i $j= 1, 2, ..., n$

$$\left[E_{ij}\right]_{pq}=\begin{cases}1, \text{ako } (p,q)=(i,j)\\ 0, \text{ako } (p,q)\neq(i,j)\end{cases}, \text{ za indekse } p= 1,...,m,\ q= 1,...,n$$

Ovakvu matricu E_{ij} nazivamo (i,j)-tom **moničnom matricom** formata $m\times n$. Familija ovakvih matrica $\Gamma=\{\ E_{ij}\mid 1\le i\le m,\ 1\le j\le n\ \}$ je i linearno nezavisna generatrisa tj. baza R-modula $M_{m\times n}(R)$. Drugim rečima, svaka matrica $A\in M_{m\times n}(R)$ se može zapisati kao

$$A=\sum_{i=1}^{m}\sum_{j=1}^{n}[A]_{ij}E_{ij}.$$

Zbog toga je skup $M_{m\times n}(R)$ jedan konačno generisan slobodan modul ranga mn.

U narednim razmatranjima koristićemo sve pojmove i teoreme koji važe u klasičnoj linearnoj algebri i teoriji matrica nad poljem F, a koji nastavljaju da važe i ukoliko se polje F zameni komutativnim prstenom R. Naravno, s tim razlogom nećemo govoriti o vektorskom prostoru, već o modulu $M_{m\times n}(R)$ nad komutativnim prstenom R. Ipak, pored mnogih tvrđenja koja ostaju na snazi, postoje i izvesne razlike, na koje vredi obratiti pažnju. U osnovi tih razlika je činjenica da prsten može imati i ne-nula elemenata koji nemaju inverz, kao i pravih delitelja nule.

Primer 13: Skup $M_2(R)$ svih kvadratnih matrica reda 2 nad komutativnim prstenom R je, kao što smo već rekli, jedan R-modul u odnosu na operacije sabiranja matrica $(A,\ B)\to A+B$ i množenja matrica skalarom $(\alpha,\ A)\to\alpha\cdot A$.

Ako je $R=\mathbb{Z}_6$ prsten ostataka po modulu 6 i ako je, na primer, matrica

$$A=3E=\begin{bmatrix}3 & 0\\ 0 & 3\end{bmatrix}$$

tada je $2\cdot A=0$, jer je

$$2\cdot A=2\cdot\begin{bmatrix}3 & 0\\ 0 & 3\end{bmatrix}=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$$

u prstenu $\mathbb{Z}$, iako je $2\neq 0$ u prstenu $\mathbb{Z}_6$ i $A\neq 0$ u samom modulu $M_2(R)$.

Podsetimo se, za početak, nekih osnovnih teorema koje se tiču blok-množenja matrica, a koje ostaju da važe i u slučaju modula $M_{m\times n}(R)$.

Neka je matrica $A \in M_{m\times n}(R)$.

$$A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{bmatrix}$$

Matricu A formata $m\times n$ možemo na proizvoljne načine podeliti na podmatrice. Tako se, na primer, i sami elementi matrice se mogu smatrati za podmatrice formata 1×1, zatim vrste za podmatrice formata $1\times n$ (ili dužine n), a kolone za podmatrice formata $m\times 1$. Uopšte, za neku matricu $B = [b_{rs}]$ domena $I\times J$ kažemo da je **podmatrica** matrice $A = [a_{pq}]$ domena $P\times Q$ ako je $I\subset P$, $J\subset Q$ i $a_{rs} = b_{pq}$, za svako $r\in I$, $s\in J$. Takođe, matrice često određujemo i tako što, u odgovarajućim tabličnim zapisima, razdvojimo vertikalnim, odnosno horizontalnim linijama neke od njihovih kolona, odnosno vrsta. Na taj način dobijamo tzv. **blok-podelu** (particiju) date matrice A. Naravno, različite particije su samo različiti načini zapisa matrice A koji nam mogu olakšati neka izračunavanja nad matricama.

Kao što smo rekli, za fiksirano $i \le m$ restrikcija matrice A na podskupu $\{(i, 1), (i, 2), \dots, (i, n)\}$ skupa $m\times n$ je jedna vrsta-matrica dužine n

$$A_{i\rightarrow} = \begin{bmatrix} a_{i1} & a_{i2} & \dots & a_{in} \end{bmatrix}.$$

Ovako definisanu matricu $A_{i\rightarrow}\in M_{1\times n}(R)$ nazivamo i-tom vrstom ili i-vrstom matrice A.

Slično se definiše i njena j-ta kolona $A_{\downarrow j}\in M_{m\times 1}(R)$, kao restrikcija matrice A na skupu $\{(1, j), (2, j), \dots, (m, j)\}$

$$A_{\downarrow \mathrm{j}} = \begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{bmatrix}.$$

Samu tu kolonu obično poistovećujemo sa m-torkom njenih komponenata $A_{\downarrow j} = (a_{1j}, a_{2j}, \dots, a_{mj})$.
Uvedimo oznaku $R^m = M_{m\times 1}(R)$. Kao što smo videli u primeru 11.a), R^m je jedan slobodan R-modul koji čine sve kolona-matrice formata m.
Za skup $M_{1\times n}(R)$ svih vrsta-matrica formata n nećemo uvoditi neku posebnu oznaku.
Dakle, ako matrica $A\in M_{m\times n}(R)$, onda su njene kolona-podmatrice $A_{\downarrow j}\in R^m$, za $j = 1, 2, \dots, n$, a vrsta-podmatrice $A_{i\rightarrow}\in M_{1\times n}(R)$, za $i = 1, 2, \dots, m$.
S tim u vezi, i samu matricu A možemo shvatiti kao sistem njenih vrsta

$$A = \begin{bmatrix} \underline{A_{1\rightarrow}} \\ \underline{A_{2\rightarrow}} \\ \vdots \\ \underline{A_{m\rightarrow}} \end{bmatrix} = \left(A_{1\rightarrow}; A_{2\rightarrow}; \dots; A_{m\rightarrow}\right)$$

Ovakvu podelu matrice A nazivamo njenom **particijom po vrstama**.

Na isti način možemo odrediti i particiju matrice A po kolonama

$$A = \left[A_{\downarrow 1} \mid \quad A_{\downarrow 2} \mid \quad \dots \quad \mid A_{\downarrow n} \right] = \left(A_{\downarrow 1};\ \ A_{\downarrow 2};\ \ A_{\downarrow n} \right).$$

Ako je $A \in M_{m\times n}(R)$ i $B \in M_{n\times p}(R)$, onda je proizvod matrica A i B matrica $AB \in M_{m\times p}(R)$ definisana sa

$$[AB]_{ij} = \sum_{k=1}^{n} [A]_{ik}[B]_{kj}, \text{ za sve } i=1, 2, \dots, m \text{ i } j= 1, 2, \dots, p.$$

Takođe, ukoliko su $A=[A_{rk}]$ i $B=[B_{ks}]$ blok-podele datih matrica A i B, određivanje proizvoda matrica A i B može se izvesti i kao određivanje proizvoda i zbirova njihovih odgovarajućih blokova, naravno uz uslov da su particije matrica A i B takve da su blokovi odgovarajućih formata tj. da su operacije koje želimo da izvršimo definisane.

Teorema 2: Neka su $A \in M_{m\times n}(R)$ i $B \in M_{n\times p}(R)$ matrice nad komutativnim prstenom R i neka su

$$A = \left[\begin{array}{c|c|c|c} A_{11} & A_{12} & \cdots & A_{1k} \\ \hline A_{21} & A_{22} & \cdots & A_{2k} \\ \hline \vdots & \vdots & & \vdots \\ \hline A_{r1} & A_{r2} & \cdots & A_{rk} \end{array}\right] \quad \text{i} \quad B = \left[\begin{array}{c|c|c|c} B_{11} & B_{12} & \cdots & B_{1t} \\ \hline B_{21} & B_{22} & \cdots & B_{2t} \\ \hline \vdots & \vdots & & \vdots \\ \hline B_{k1} & B_{k2} & \cdots & B_{kt} \end{array}\right]$$

blok-podele tih matrica takve da je svako A_{ij} podmatrica formata $m_i \times n_j$ i B_{jl} podmatrica formata $n_j \times p_l$, gde je $m_1 + m_2 + \dots + m_r = m$, $n_1 + n_2 + \dots + n_k = n$ i $p_1 + p_2 + \dots + p_t = p$. Za svako $i=1, 2, \dots, r$ i $j= 1, 2, \dots, t$ proizvod AB je takođe jedna blok-podela matrice AB, pri čemu je svaki blok C_{ij} suma proizvoda odgovarajućih blokova A_{iq} i B_{qj} matrica A i B,

$C_{ij} = \sum_{q=1}^{k} A_{iq} B_{qj}$.

$$C = \left[\begin{array}{c|c|c|c} C_{11} & C_{12} & \cdots & C_{1t} \\ \hline C_{21} & C_{22} & \cdots & C_{2t} \\ \hline \vdots & \vdots & & \vdots \\ \hline C_{r1} & C_{r2} & \cdots & C_{rt} \end{array}\right]$$

Navedimo nekoliko specijalnih slučajeva u kojima je primena teoreme 2 posebno praktična.

Primer 14. Ako je $A \in M_{m\times n}(R)$ i $\xi = (x_1, x_2, \dots, x_n)^t \in R^n$ jedna kolona-matrica, tj. $\xi \in M_{n\times 1}(R)$, onda važi

$$A\xi = x_1 A_{\downarrow 1} + x_2 A_{\downarrow 2} + \dots + x_n A_{\downarrow n}.$$

Zaista,

$$A\xi = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \end{bmatrix} =$$

$$= x_1 \begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{bmatrix} + x_2 \begin{bmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{bmatrix} + \cdots + x_n \begin{bmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{bmatrix}.$$

Za proizvoljnu matricu $A \in M_{m\times n}(R)$ označimo sa $CS(A) = \{ A\xi \mid \xi \in R^n \}$ podmodul modula R^m generisan kolonama matrice A. Ovako definisan R-modul $CS(A)$ nazivamo prostorom kolona matrice A.

Primer 15. Neka su date matrice $A \in M_{m\times n}(R)$ i $B \in M_{n\times p}(R)$. Ako matricu B shvatimo kao sistem njenih kolona tj. kao njen blok-zapis $B = [B_{\downarrow 1} | B_{\downarrow 2} | \ldots | B_{\downarrow p}]$ formata $1\times p$, onda je

$$AB = (AB_{\downarrow 1} | AB_{\downarrow 2} | \ldots | AB_{\downarrow p}).$$

Primenimo teoremu 1:

$$AB = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} & \ldots & b_{1p} \\ b_{21} & b_{22} & \ldots & b_{2p} \\ \vdots & \vdots & & \vdots \\ b_{n1} & b_{n2} & \ldots & b_{np} \end{bmatrix} =$$

$$= \left[\begin{array}{l|l|c|l} a_{11}b_{11} + a_{12}b_{21} + \ldots + a_{1n}b_{n1} & a_{11}b_{12} + a_{12}b_{22} + \ldots + a_{1n}b_{n2} & \cdots & a_{11}b_{1p} + a_{12}b_{2p} + \ldots + a_{1n}b_{np} \\ \hline a_{21}b_{11} + a_{22}b_{21} + \ldots + a_{2n}b_{n1} & a_{21}b_{12} + a_{22}b_{22} + \ldots + a_{2n}b_{n2} & \cdots & a_{21}b_{1p} + a_{22}b_{2p} + \ldots + a_{2n}b_{np} \\ \hline \vdots & \vdots & & \vdots \\ \hline a_{m1}b_{11} + a_{m2}b_{21} + \ldots + a_{mn}b_{n1} & a_{m1}b_{12} + a_{m2}b_{22} + \ldots + a_{mn}b_{n2} & \cdots & a_{m1}b_{1p} + a_{m2}b_{2p} + \ldots + a_{mn}b_{np} \end{array}\right] =$$

$$= \left[\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} b_{11} \\ b_{21} \\ \vdots \\ b_{n1} \end{bmatrix} \middle| \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} b_{12} \\ b_{22} \\ \vdots \\ b_{m2} \end{bmatrix} \middle| \ldots \middle| \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} b_{1p} \\ b_{2p} \\ \vdots \\ b_{mp} \end{bmatrix} \right] =$$

$$= \left[AB_{\downarrow 1} \middle| AB_{\downarrow 2} \middle| \ldots \middle| AB_{\downarrow p} \right]$$

Možemo primetiti da je svaka kolona matrice AB ustvari jedna linearna kombinacija kolona matrice A sa skalarima iz odgovarajuće kolone matrice B.
Konačno, možemo zaključiti da je $\mathrm{CS}(AB) \subseteq \mathrm{CS}(A)$.

Takođe, ukoliko matricu A podelimo u vrste, ponovo će važiti odgovarajuća tvrđenja:

Primer 16. Ako je $A \in M_{m\times n}(R)$ i $\delta = (x_1, x_2, \ldots, x_m) \in M_{1\times m}(R)$, jedna vrsta-matrica, onda važi

$$\delta A = x_1 A_{1\rightarrow} + x_2 A_{2\rightarrow} + \ldots + x_m A_{m\rightarrow} .$$

$$\delta A = \begin{bmatrix} x_1 & x_2 & \cdots & x_m \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} =$$

$$= \left[x_1a_{11} + x_2a_{21} + \cdots + x_ma_{m1} \;\middle|\; x_1a_{12} + x_2a_{22} + \cdots + x_ma_{m2} \;\middle|\; \cdots \;\middle|\; x_1a_{1n} + x_2a_{2n} + \cdots + x_ma_{mn} \right] =$$

$$= \left[x_1a_{11} \;\middle|\; x_1a_{12} \;\middle|\; \cdots \;\middle|\; x_1a_{1n} \right] + \left[x_2a_{21} \;\middle|\; x_2a_{22} \;\middle|\; \cdots \;\middle|\; x_2a_{2n} \right] + \cdots + \left[x_ma_{m1} \;\middle|\; x_ma_{m2} \;\middle|\; \cdots \;\middle|\; x_ma_{mn} \right] =$$

$$= x_1A_{1\rightarrow} + x_2A_{2\rightarrow} + \cdots + x_mA_{m\rightarrow}$$

Za proizvoljnu matricu $A \in M_{m\times n}(R)$ označićemo sa $\mathrm{RS}(A) = \{ \delta A \mid \delta \in R^n \}$ podmodul modula $M_{1\times m}(R)$ generisan vrstama matrice A, koji nazivamo prostorom vrsta matrice A.

Primer 17. Neka su $A \in M_{m\times n}(R)$ i $B \in M_{n\times p}(R)$. Ako matricu A zapišemo u blok-podeli po njenim vrstama $A = [A_{1\rightarrow}\ ;\ A_{2\rightarrow}\ ;\ \ldots\ ;\ A_{m\rightarrow}]$ onda važi

$$AB = [A_{1\rightarrow}B\ ;\ A_{2\rightarrow}B\ ;\ \ldots\ ;\ A_{m\rightarrow}B]$$

$$AB = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} & \ldots & b_{1p} \\ b_{21} & b_{22} & \ldots & b_{2p} \\ \vdots & \vdots & & \vdots \\ b_{n1} & b_{n2} & \ldots & b_{np} \end{bmatrix} =$$

$$= \left[\begin{array}{c|c|c|c} a_{11}b_{11}+a_{12}b_{21}+\ldots+a_{1n}b_{n1} & a_{11}b_{12}+a_{12}b_{22}+\ldots+a_{1n}b_{n2} & \cdots & a_{11}b_{1p}+a_{12}b_{2p}+\ldots+a_{1n}b_{np} \\ \hline a_{21}b_{11}+a_{22}b_{21}+\ldots+a_{2n}b_{n1} & a_{21}b_{12}+a_{22}b_{22}+\ldots+a_{2n}b_{n2} & \cdots & a_{21}b_{1p}+a_{22}b_{2p}+\ldots+a_{2n}b_{np} \\ \hline \vdots & \vdots & & \vdots \\ \hline a_{m1}b_{11}+a_{m2}b_{21}+\ldots+a_{mn}b_{n1} & a_{m1}b_{12}+a_{m2}b_{22}+\ldots+a_{mn}b_{n2} & \cdots & a_{m1}b_{1p}+a_{m2}b_{2p}+\ldots+a_{mn}b_{np} \end{array}\right] =$$

$$= \left[\begin{array}{c} [a_{11}\ \ a_{12}\ \ \cdots\ \ a_{1n}] \begin{bmatrix} b_{11} & b_{12} & \ldots & b_{1p} \\ b_{21} & b_{22} & \ldots & b_{2p} \\ \vdots & \vdots & & \vdots \\ b_{n1} & b_{n2} & \ldots & b_{np} \end{bmatrix} \\ \hline [a_{21}\ \ a_{22}\ \ \cdots\ \ a_{2n}] \begin{bmatrix} b_{11} & b_{12} & \ldots & b_{1p} \\ b_{21} & b_{22} & \ldots & b_{2p} \\ \vdots & \vdots & & \vdots \\ b_{n1} & b_{n2} & \ldots & b_{np} \end{bmatrix} \\ \hline \vdots \\ \hline [a_{m1}\ \ a_{m2}\ \ \cdots\ \ a_{mn}] \begin{bmatrix} b_{11} & b_{12} & \ldots & b_{1p} \\ b_{21} & b_{22} & \ldots & b_{2p} \\ \vdots & \vdots & & \vdots \\ b_{n1} & b_{n2} & \ldots & b_{np} \end{bmatrix} \end{array}\right] = \begin{bmatrix} \underline{A_{1\rightarrow}B} \\ \underline{A_{2\rightarrow}B} \\ \vdots \\ \underline{A_{m\rightarrow}B} \end{bmatrix} = (A_{1\rightarrow}B; A_{2\rightarrow}B; \ldots; A_{m\rightarrow}B)$$

Dakle, svaka vrsta matrice AB predstavlja i jednu linearnu kombinaciju vrsta matrice B sa skalarima iz odgovarajuće vrste matrice A. Takođe je $\mathrm{RS}(AB) \subseteq \mathrm{RS}(B)$ za matrice $A \in M_{m\times n}(R)$ i $B \in M_{n\times p}(R)$.

Razmotrimo sada osobine množenja moničnih matrica

$$\left[E_{ij}\right]_{pq} = \begin{cases} 1, \text{ ako } (p,q)=(i,j) \\ 0, \text{ ako } (p,q)\neq(i,j) \end{cases}, \text{ za indekse } p,\ q = 1,\ldots,n.$$

Odranije smo uveli oznaku $\Gamma = \{\ E_{ij} \mid 1 \le i,\ j \le n\ \}$ za skup svih moničnih matrica reda n, koji je ujedno i baza R-modula $M_n(R)$.

Primer 18. Proizvod dve monične matrice je monična matrica

$$E_{ij}E_{kl} = \begin{cases} E_{il}, \text{ ako } j=k \\ 0, \text{ ako } j\neq k \end{cases} \text{ za sve } i, j, k, l = 1, \ldots, n.$$

Primer 19. Ako je matrica $A=[a_{ij}]\in M_n(R)$, onda za sve $p,q = 1, \ldots, n$ važi

$$AE_{pq} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1p} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2p} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{np} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & \cdots 0 \\ 0 & 0 & \cdots & & \vdots & \vdots \\ \vdots & \vdots & 0 & \cdots & 1_{pq} & \cdots 0 \\ 0 & 0 & \cdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots 0 & \cdots 0 \end{bmatrix} = \sum_{i=1}^{n}\left(\sum_{j=1}^{n} a_{ij}E_{ij}\mathrm{E}_{pq}\right) = \sum_{i=1}^{n} a_{ip}E_{iq} =$$

$$= \begin{bmatrix} 0 & \cdots & 0 & a_{1p} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & a_{2p} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & a_{np} & 0 & \cdots & 0 \end{bmatrix} = \left[\begin{array}{c|c|c|c|c|c|c} 0 & \cdots & 0 & A_{\downarrow p} & 0 & \cdots & 0 \end{array}\right]$$

q-ta kolona -

Ovde $A_{\downarrow p}$ predstavlja q-tu kolonu matrice AE_{ij}, koja je ustvari jednaka p-toj koloni matrice A.

Primer 20. Za matricu $A=[a_{ij}]\in M_n(R)$ i sve $p,q = 1, \ldots, n$ važi i

$$E_{pq}A = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & \cdots 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1_{pq} & \cdots 0 \\ \vdots & \vdots & \cdots & & \vdots & \vdots \\ 0 & 0 & \cdots & & 0 & \cdots 0 \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \vdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{q1} & a_{q2} & \cdots & a_{qn} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} = E_{pq}\left(\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}E_{ij}\right) = \sum_{j=1}^{n}\left(\sum_{i=1}^{n} a_{ij}E_{pq}E_{ij}\right) =$$

$$= \sum_{j=1}^{n} a_{qj}E_{pj} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \\ a_{q1} & a_{q2} & \cdots & a_{qn} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ \hline A_{q\rightarrow} \\ \hline 0 \\ \vdots \\ \hline 0 \end{bmatrix}$$

- p-ta vrsta

Ovde $A_{q\rightarrow}$ predstavlja p-tu vrstu martrice $E_{pq}A$ koja je, ujedno, jednaka q-toj vrsti matrice A.

Primer 21. Ako je $A=[a_{ij}]\in M_n(R)$, onda za sve $k,s,p,q = 1, \dots, n$ važi $E_{ks}AE_{pq} = a_{sp}E_{kq}$.
Zaista,

$$E_{ks}AE_{pq} = E_{ks}\sum_{i=1}^{n} a_{ip}E_{iq} = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & \cdots 0 \\ 0 & 0 & \cdots & & \vdots & \vdots \\ \vdots & \vdots & 0 & \cdots & 1_{ks} & \cdots 0 \\ 0 & 0 & \cdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 0 \cdots 0 & & \cdots 0 \end{bmatrix} \begin{bmatrix} 0 & \cdots & 0 & a_{1p} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & a_{2p} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & a_{np} & 0 & \cdots & 0 \end{bmatrix} =$$

$$= \sum_{i=1}^{n} a_{ip}E_{ks}E_{iq} = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & \cdots 0 \\ 0 & 0 & \cdots & & \vdots & \vdots \\ \vdots & \vdots & 0 & \cdots & a_{sp} & \cdots 0 \\ 0 & 0 & \cdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 0 \cdots 0 & & \cdots 0 \end{bmatrix} - k-ta \quad vrsta = a_{sp}E_{kq}$$

q-ta kolona

Dakle, $E_{ks}AE_{pq}$ je kvadratna matrica reda n koja ima samo (k,q)-tu komponentu jednaku a_{sp}, dok su joj ostale komponente nula.

Za matricu $A=[a_{ij}]\in M_{m\times n}(R)$ kažemo da je **dijagonalna** ako je $a_{ij} = 0$ za svako $i \neq j$. Dijagonalna matrica ne mora da bude kvadratna, naime razlikovaćemo sledeće slučaje

1) ako je $m \leq n$, dijagonalna matrica će biti oblika

$$\mathrm{Diag}(d_1,\cdots,d_r) = \begin{bmatrix} d_1 & 0 & \dots & 0 & 0 \cdots 0 \\ 0 & d_2 & \dots & 0 & 0 \cdots 0 \\ \vdots & \vdots & & \vdots & \vdots \quad \vdots \\ 0 & 0 & \dots & d_r & 0 \cdots 0 \end{bmatrix}$$

2) odnosno, ako je $m \geq n$, onda je

$$\mathrm{Diag}(d_1,\cdots,d_r) = \begin{bmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & d_r \\ 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix}$$

DETERMINANTE

Neka je $A=[a_{ij}]\in M_n(R)$ proizvoljna kvadratna matrica reda n nad komutativnim prstenom R.

$$A=\begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix}$$

Preslikavanje det: $M_n(R)\to R$ kojim se matrici A pridružuje skalar $\det A\in R$ definisan sa

$$\det A=\sum_{\sigma\in S_n}\operatorname{sgn}\sigma\, a_{1\sigma 1}a_{2\sigma 2}\cdot\ldots a_{n\sigma n}$$

naziva se **determinanta** matrice A. U zapisu determinante često koristimo i oznaku

$$\Delta=\det A=\begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}$$

Skup S_n označava skup svih permutacija skupa $\{1, 2, \dots, n\}$, dok je $\operatorname{sgn}\sigma = 1$ ili $\operatorname{sgn}\sigma = -1$ znak permutacije σ. U opštem slučaju, navedena suma ide preko svih $n!$ permutacija skupa S_n, tj. ima $n!$ sabiraka.

Neka je $A\in M_{m\times n}(R)$ i neka je $1\le k\le \min\{m, n\}$. **Minor reda *k*** matrice A je determinanta njene kvadratne podmatrice formata $k\times k$. Ako podmatricu formata $k\times k$ formiramo izborom k vrsta $(i_1, \dots, i_k)$ i k kolona $(j_1, \dots, j_k)$ matrice A, onda nam oznaka za minor $\Delta(i_1, \dots, i_k; j_1, \dots, j_k)$ precizno ukazuje pomoću kojih vrsta i kolona smo formirali podmatricu čiju determinantu određujemo. Naravno, ovde je $1\le i_1\le \dots\le i_k\le m$, $1\le j_1\le \dots\le j_k\le n$, što govori da data matrica A može imati minore reda $1\times 1, 2\times 2, \dots, r\times r$, gde je $r=\min\{m, n\}$. Uz to, pod minorom reda $k=0$ podrazumevamo samu jedinicu prstena R.

Primer 22. Neka je data matrica $A\in M_{2\times 4}(\mathbb{Z})$,

$$A=\begin{bmatrix} 1 & 2 & 3 & -4 \\ 1 & 0 & 5 & -1 \end{bmatrix}.$$

Tada je $\Delta(1;2)=2$, a $\Delta(2;4)=-1$, dok je, na primer, $\Delta(1,2;2,4)=\det\begin{bmatrix} 2 & -4 \\ 0 & -1 \end{bmatrix}=-2$.

Neka je sada $A\in M_n(R)$ kvadratna matrica.
Minor $(n-1)$-og reda dobijen izostavljanjem i-te vrste i j-te kolone matrice A obeležavaćemo sa $M_{ij}(A)$, gde su $i, j = 1, \dots, n$.
Za fiksirano (i, j) skalar $A_{ij}=(-1)^{i+j}M_{ij}$ nazivamo (i,j)-tim **kofaktorom** matrice A, ili kofaktorom njene (i,j)-te komponente. Dakle, $A_{ij}=(-1)^{i+j}\Delta(1, \dots, \hat{\imath}, \dots, n; 1, \dots, \hat{\jmath}, \dots, n)$, gde su $\hat{\imath}$ i $\hat{\jmath}$ izostavljena vrsta, odnosno kolona matrice A. Jasno je da se kofaktor A_{ij} i minor M_{ij} matrice A mogu razlikovati samo u znaku.
Adjungovana matrica (adjunkt) uočene matrice A, u oznaci $\operatorname{adj}A$, je transponovana matrica matrice kofaktora A_{ij} matrice A. Dakle, $[\operatorname{adj}A]_{ij}=A_{ji}$, odnosno

$$\mathrm{adj}A = \begin{bmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \vdots & \vdots & & \vdots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{bmatrix}$$

U opštem slučaju vrednost determinante izračunavamo metodom razvijanja determinante po elementima bilo koje vrste ili kolone. Ovaj razvoj determinante nazivamo Laplaceovim[5] razvojem. Suština metode sastoji se u tome da se izračunavanje vrednosti determinante *n*-tog reda svodi na izračunavanje vrednosti *n* determinanata (*n-1*)-og reda, determinante (*n-1*)-og reda opet svodimo na izračunavanje determinanti (*n-2*)-og reda, i postupak ponavljamo sve dok ne dodemo do determinanti drugog reda.

Pre nego što navedemo teoremu, uvedimo i pojam Kroneckerove[6] delta funkcije

$$\delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

Teorema 3. (Laplaceov razvoj determinante)

Ako je $A = [a_{ij}] \in M_n(R)$, važi

(1) $\sum_{j=1}^{n} a_{ij} A_{kj} = \delta_{ik} \det A$, za sve $i, k=1, .. , n$;

(2) $\sum_{i=1}^{n} a_{ij} A_{ik} = \delta_{jk} \det A$, za sve $j, k=1, .. , n$.

Drugim rečima, determinanta je jednaka zbiru proizvoda elemenata ma koje vrste (odnosno kolone) i odgovarajućih kofaktora tj. važi

$\det A = a_{i1}A_{i1} + a_{i2}A_{i2} + \cdots + a_{in}A_{in} = \sum_{k=1}^{n} a_{ik}A_{ik}$, za $i = 1, 2, \dots , n$ (razvoj po elementima *i*-te vrste)

i, slično

$\det A = a_{1j}A_{1j} + a_{2j}A_{2j} + \cdots + a_{nj}A_{nj} = \sum_{k=1}^{n} a_{kj}A_{kj}$, za $j = 1, 2, \dots , n$ (razvoj po elementima *j*-te kolone)

I ukratko, kao posledicu Laplaceove formule za razvoj determinante, možemo zapisati da je

$$A \cdot \mathrm{adj}A = \mathrm{adj}A \cdot A = \det A \cdot E_n \qquad (*)$$

gde je E_n jedinična matrica reda *n*. Zaista, za $A \in M_n(R)$, imamo

$$A \cdot \mathrm{adj}A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \vdots & \vdots & & \vdots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{bmatrix} = \begin{bmatrix} \sum_{j=1}^{n} a_{kj}A_{ij} \end{bmatrix} = \begin{bmatrix} \det A & 0 & \dots & 0 \\ 0 & \det A & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & \det A \end{bmatrix} = \det A \cdot E$$

jer je $\sum_{j=1}^{n} a_{kj}A_{ij} = \begin{cases} \det A, & k = i \\ 0, & k \neq i \end{cases}$.

Naime, $\sum_{j=1}^{n} a_{kj}A_{ij}$ je determinanta matrice koja nastaje iz matrice A zamenom *k*-te vrste njenom *i*-tom vrstom, pa u slučaju $k \neq i$ ta matrica bi imala dve jednake vrste i njena determinanta je 0.

[5] Pierre –Simon Marquis de Laplace (1749 -1827.god.), francuski matematičar i astronom

[6] Leopold Kronecker (1823 -1891.god.), nemački matematičar

Posebno, ako skalar $\Delta=\det A$ u relaciji $(*)$ ima inverz u prstenu R, onda množenjem relacije sa Δ^{-1} odmah sledi da je i sama matrica A inverzibilna u prstenu $M_n(R)$, kao i da važi

$$A^{-1} = \frac{1}{\det A}\operatorname{adj} A$$

Posledica 2: Matrica A je inverzibilna u prstenu $M_n(R)$ ako i samo ako njena determinanta ima inverz u prstenu R.

Dokaz: ($\Rightarrow$) Pretpostavimo da je matrica A inverzibilna u prstenu $M_n(R)$, $A\in U(M_n(R))$. Tada postoji matrica $B\in M_n(R)$, takva da je $AB = BA = E$. Sada je

$$1 = \det E = \det AB = \det A\cdot\det B$$

a to upravo znači da je $\det A$ inverzibilan skalar u prstenu R, $\det A\in U(R)$.

($\Leftarrow$) Obratno, ako je $\det A\in U(R)$, onda iz relacije $(*)$, deljenjem sa inverzom $(\det A)^{-1}$ sledi

$$A\cdot[(\det A)^{-1}\operatorname{adj} A] = [(\det A)^{-1}\operatorname{adj} A]\cdot A = E$$

pa je zato matrica A inverzibilna u prstenu $M_n(R)$, a njen inverz je upravo

$$A^{-1} = (\det A)^{-1}\operatorname{adj} A.$$

■

U dokazu smo koristili multiplikativno svojstvo determinante, da je $\det AB = \det A\cdot\det B$ što je posledica činjenice da je determinanta višelinearno preslikavanje u odnosu na svoje vrste, odnosno kolone.

Konačno, važno je da primetimo da za razliku od matrica koje su definisane nad poljem F, kada je matrica A inverzibilna ako i samo ako je njena determinanta različita od nule u tom polju, $\det A\neq 0$, kod matrica definisanih nad komutativnim prstenom više ne možemo zaključivati na taj način. Jer, nula je jedini element polja koji nema inverz, pa ako je $\det A\neq 0$ to upravo znači da je skalar $\det A$ inverzibilan u polju F. S druge strane, ako govorimo o matricama definisanim nad prstenom celih brojeva $\mathbb{Z}$, na primer, tu je skup inverzibilnih elemenata dvočlan, $U(\mathbb{Z}) = \{1, -1\}$, pa da bi matrica A bila inverzibilna u $M_n(\mathbb{Z})$, na osnovu navedene posledice, potrebno je da njena determinanta bude jednaka 1 ili -1.

Primer 23: Neka je data matrica $A\in M_2(\mathbb{Z})$,

$$A = \begin{bmatrix} 2 & 3 \\ 4 & 7 \end{bmatrix}.$$

Determinanta je $\det A = 2$, a broj 2 nije inverzibilan u prstenu $\mathbb{Z}$, pa prema prethodno navedenoj posledici 2, data matrica A nije inverzibilna u $M_2(\mathbb{Z})$.

Zaista, ukoliko bismo matricu A posmatrali nad poljem racionalnih brojeva, na primer, $A\in M_2(\mathbb{Q})$, tada bi determinanta $\det A = 2$ bila inverzibilan element u $\mathbb{Q}$, pa bi odgovarajuća inverzna matrica bila

$$A^{-1} = \frac{1}{2}\begin{bmatrix} 7 & -3 \\ -4 & 1 \end{bmatrix}.$$

Uvedimo oznaku $\mathrm{GL}(n,R)$ za skup svih inverzibilnih matrica modula $M_n(R)$ nad komutativnim prstenom R. Dakle, $\mathrm{GL}(n,R) = U(M_n(R))$, pa je $\mathrm{GL}(n,R)$ i jedna grupa u odnosu na množenje matrica. Zovemo je **linearnom grupom** stepena n nad prstenom R. Neutral u ovoj grupi je jedinična matrica $E = E_n$, a iz navedene posledice 2 sledi i da je

$$\mathrm{GL}(n,R) = \{A\in M_n(R) \mid \det A \in U(R)\}.$$

§3 IDEALI U PRSTENU $M_n(R)$

Neka je U ideal komutativnog prstena R. Skup kvadratnih matrica reda n sa komponentama iz U,

$$M_n(U) = \{ A \in M_n(R) \mid [A]_{ij} \in U \text{ za sve } i,j = 1,...,n \}$$

je tada takođe jedan (dvostrani) ideal u $M_n(R)$. Štaviše, svaki ideal prstena $M_n(R)$ je ovog tipa, odnosno važi sledeća

Teorema 4: Neka je P ideal prstena $M_n(R)$. Tada je $P = M_n(U)$ za jedinstveni ideal U prstena R.

Dokaz: Neka je skup $U = \{ r \in R \mid r$ je komponenta neke od matrica ideala $P\}$.
Dokazaćemo najpre da je ovako definisan skup U i jedan ideal komutativnog prstena R, zatim da je upravo $P = M_n(U)$, i konačno jedinstvenost ideala U.

1) Najpre, jasno je da $0 \in U$ jer je P ideal, pa je nula-matrica $\boldsymbol{O} \subseteq P$. Neka su sada a i b proizvoljni elementi skupa U, $a,b \in U$. Tada postoje dve matrice A i B ideala P takve da je element a komponenta matrice A, a element b komponenta u B, na primer $a = [A]_{kp}$ i $b = [B]_{sq}$, gde su indeksi $k,p,s,q = 1, ..., n$. Ako je E_{ij}, $i,j = 1, ..., n$, odgovarajuća monična matrica, onda svaku od komponenata a i b možemo izraziti i kao $a = [AE_{pq}]_{kq}$, odnosno $b = [E_{ks}B]_{kq}$.
Pošto je P ideal u $M_n(R)$, sledi da $AE_{pq} \pm E_{ks}B \in P$.
Dakle, $a \pm b = [AE_{pq} \pm E_{ks}B]_{kq} \in U$, pa zaključujemo da $(U, +)$ jeste aditivna podgrupa u R.
Neka je, dalje $r \in R$, $a \in U$. Tada je $a = [A]_{kp}$ komponenta neke matrice $A \in P$, za indekse $p,q = 1, ..., n$. Ako je $\text{Diag}(r,..., r) \in M_n(R)$ dijagonalna matrica, onda je $\text{Diag}(r,..., r)A \in P$ jer je P ideal u $M_n(R)$, pa sledi da je (k,p)-ta komponenta $ra = [\text{Diag}(r,..., r)A]_{kp} \in U$.
Ovim smo pokazali da skup U jeste jedan ideal u prstenu R.
2) Kako je U skup svih komponenata matrica ideala P jasno je da je $P \subseteq M_n(U)$. Dokažimo da važi i obratno. Neka je $A \in M_n(U)$. Tada su sve njene komponente $a_{ij} \in U$, za $i,j = 1,..., n$, i važi

$$A = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} E_{ij} .$$

Pošto svaka komponenta $a_{ij} \in U$, ako fiksiramo neke određene indekse i,j, sledi da postoji matrica $B \in P$ takva da je a_{ij} njena (p,q)-ta komponenta $a_{ij} = [B]_{pq}$, $p,q = 1,...,n$. Ovo upravo znači da

$$a_{ij}E_{ij} = [B]_{pq}E_{ij} = E_{ip}BE_{qj} \in P ,$$

pa pošto je matrica A suma matrica oblika $a_{ij}E_{ij}$, možemo zaključiti da $A \in P$, odnosno da je i $M_n(U) \subseteq P$. Time smo pokazali da je $P = M_n(U)$, drugim rečima, da je svaki ideal prstena $M_n(R)$ ustvari oblika $M_n(U)$, gde je U jedan ideal u komutativnom prstenu R.
3) Konačno, ako postoji i neki ideal J takav da je $P = M_n(J)$, jasno je da tada $J \subseteq U$.
Neka je sada $a \in U$. Tada je $a = [B]_{pq}$, za neku matricu B iz ideala P i neke indekse $p,q \in \{1,... , n\}$.
Takođe je, na primer, $aE_{11} = E_{1p}BE_{q1} \in P = M_n(J)$, pa komponenta $a \in J$, a time je i $U \subseteq J$, pa možemo zaključiti da je $U = J$ tj. da je ovako definisan ideal U jedinstven.

■

Prethodna teorema ukazuje da postoji 1-1 pridruživanje između ideala komutativnog prstena R i ideala prstena matrica $M_n(R)$. Preciznije, preslikavanje $U \to M_n(U)$ je i jedna bijekcija skupa $L(R)$ svih ideala prstena R na skup $L(M_n(R))$ svih ideala prstena $M_n(R)$. To preslikavanje, pri tom, čuva poredak, presek, sumu i proizvod ideala iz $L(R)$ među idealima u $L(M_n(R))$, odnosno važi sledeće tvrđenje.

Tvrđenje 2. Neka su U_1 i U_2 dva ideala komutativnog prstena R, $U_1, U_2 \in L(R)$.
1) Ako je $U_1 \subseteq U_2$ u $L(R)$, onda je $M_n(U_1) \subseteq M_n(U_2)$;
2) $M_n(U_1 \cap U_2) = M_n(U_1) \cap M_n(U_2)$;
3) $M_n(U_1+U_2) = M_n(U_1) + M_n(U_2)$;
4) $M_n(U_1U_2) = M_n(U_1)\, M_n(U_2)$.

Ako je prsten R pri tome i polje, $R=F$, onda je skup njegovih ideala $L(F)=\{\{0\}, F\}$, jer su polja, kao što smo rekli prosti prsteni, tj. nemaju pravih ideala. Teorema 4 sada ima za posledicu da je skup ideala $L(M_n(F)) =\{\{0\}, M_n(F)\}$, što nas dalje vodi zaključku da je i prsten kvadratnih matrica $M_n(F)$ nad poljem F takođe prost prsten.

Posledica 3: Ako je F polje, onda je prsten matrica $M_n(F)$ nad tim poljem prost. ■

Prsten $M_n(R)$ nad komutativnim prstenom R, međutim, ima više pravih levih (ili desnih) ideala. Ako je, na primer, $A \in M_n(R)^*$ ne-nula matrica čija je determinanta $\det A=0$, onda je $M_n(R)A$ pravi levi ideal, a $AM_n(R)$ pravi desni ideal u prstenu $M_n(R)$. Naime, determinanta matrice A u tom slučaju nije inverzibilna u prstenu R, pa zato i sama matrica A nema inverz u prstenu $M_n(R)$, a svaki element prstena koji nema inverz generiše i jedan pravi ideal u tom prstenu.

Teorema 4 nam sada može pomoći da odredimo Jacobsonov radikal prstena matrica $M_n(R)$.
U dokazu sledeće teoreme koristićemo ranije dokazanu lemu 2§1, koja govori da za Jacobsonov radikal prstena eKe, gde je $e \in K$ idempotentni element, važi $J(eKe) = eJ(K)e$.

Teorema 5. Za bilo koji komutativan prsten R važi da je $J(M_n(R)) = M_n(J(R))$.

Dokaz: Odranije znamo da je Jacobsonov radikal prstena i jedan ideal u tom prstenu, pa je tako i $J(M_n(R))$ ideal u prstenu $M_n(R)$. Na osnovu teoreme 4, to znači da je $J(M_n(R))=M_n(U)$ za neki (jedinstveni) ideal U prstena R. Pokažimo da je $U=J(R)$.
Uočimo moničnu matricu E_{11} koja je i jedan idempotentni element prstena $M_n(R)$, jer je $E_{11}^2=E_{11}$. Prema pomenutoj lemi 2, važi da je

$$E_{11}M_n(U)E_{11} = E_{11}J(M_n(R))E_{11} = J(E_{11}M_n(R)E_{11}) \qquad (**)$$

Prsten $E_{11}M_n(R)E_{11}$ sadrži matrice oblika rE_{11} , $r \in R$, jer je za proizvoljnu matricu $A=[a_{ij}] \in M_n(R)$, proizvod $E_{11}AE_{11} = a_{11}E_{11}$, pa je sa $rE_{11} \to r$ određen i jedan izomorfizam prstena $E_{11}M_n(R)E_{11} =\{rE_{11} \mid r \in R\}$ u prsten R. To preslikavanje, takođe, prevodi i prsten $E_{11}M_n(U)E_{11}$ u ideal U, kao i Jacobsonov radikal $J(E_{11}M_n(R)E_{11})$ u $J(R)$. Sada, na osnovu (**) možemo zaključiti da je $U = J(R)$

■

Pretpostavimo da je $R= F[X]$ prsten polinoma sa koeficijentima iz polja F. Ovaj prsten je, kao što znamo, i jedan glavnoidealski domen, pa je njegov Jacobsonov ideal $J(R)$ glavni ideal generisan sa X. Teorema 5 nam sada ukazuje da je Jacobsonov radikal prstena matrica $M_n(F[X])$ ustvari skup

$$J(M_n(F[X])) = \{\ A=[a_{ij}] \in M_n(F[X]) \mid X \mid a_{ij} \text{ za sve } i,j=1,\ldots, n\ \}.$$

§4 RANG MATRICE

Neka je $A \in M_{m\times n}(R)$ proizvoljna matrica formata $m\times n$ sa komponentama iz komutativnog prstena R. Ideal prstena R generisan svim minorima reda t matrice A označavaćemo sa $\boldsymbol{I_t(A)}$, za svako $t = 1, ..., r = \min\{m, n\}$. Dakle, potrebno je izračunati determinante svih $t\times t$ podmatrica matrice A, pa odrediti $I_t(A)$ kao ideal prstena R generisan ovim determinantama. Prema teoremi 3, o Laplaceovom razvoju determinante, determinanta kvadratne matrice formata $t\times t$ se izračunava kao linearna kombinacija njenih minora reda $t-1$, pa otuda zaključujemo da svaki minor reda $t+1$ matrice A leži u idealu $I_t(A)$ generisanom minorima reda t te matrice, odnosno možemo reći da ovi ideali formiraju jedan opadajući lanac u prstenu R:

$$I_r(A) \subseteq I_{r-1}(A) \subseteq \ldots \subseteq I_2(A) \subseteq I_1(A) \subseteq R.$$

Proširimo definiciju ideala $I_t(A)$ za sve vrednosti $t\in\mathbb{Z}$ na sledeći način

$$I_t(A) = \begin{cases} \{0\}, & \text{ako je } t > \min\{m,n\} \\ R, & \text{ako je } t \le 0 \end{cases}$$

tako da sada važi

$$\{0\} = I_{r+1}(A) \subseteq I_r(A) \subseteq \ldots \subseteq I_1(A) \subseteq I_0(A) = R.$$

Lema 3. Neka je $B\in M_{m\times p}(R)$ i $C\in M_{p\times n}(R)$. Tada je $I_t(BC) \subseteq I_t(B) \cap I_t(C)$, za sve $t\in\mathbb{Z}$.

Dokaz: U trivijalnim slučajevima, za $t \le 0$ važi $I_t(BC) = I_t(B) = I_t(C) = R$ jer je $R \subseteq R\cap R$, odnosno, za $t > \min\{m, n\}$ važi $I_t(BC) = \{0\} \subseteq I_t(B) \cap I_t(C)$, što odgovara tvrđenju leme.
Pretpostavimo, zato, da je $1 \le t \le \min\{m, n\}$.
Podelićemo dokaz ove leme na dokaze tri tvrdnje, od kojih svaka ima i pojedinačni značaj i primenu.
Tvrdnja I: $I_t(BC) \subseteq I_t(C)$.
Da bismo dokazali ovu tvrdnju zapišimo matricu C podeljenu u particije po kolonama

$$C = \left(\delta_1 \middle| \, \delta_2 \middle| \cdots \middle| \, \delta_n \right).$$

Na osnovu primera 15, o blok-množenju matrica, imamo da važi

$$BC = \left(B\delta_1 \middle| \, B\delta_2 \middle| \cdots \middle| \, B\delta_n \right).$$

Neka je Δ minor reda $t\times t$ matrice BC, koji je generator ideala $I_t(BC)$. Pretpostavimo da minor Δ čine kolone $j_1 < j_2 < \ldots < j_t$ matrice BC. Pošto je $I_t((\, \delta_{j1} \mid \delta_{j2} \mid \ldots \mid \delta_{jt})) \subseteq I_t(C)$ i $\Delta \in I_t((\, B\delta_{j1} \mid B\delta_{j2} \mid \ldots \mid B\delta_{jt})) = I_t(\, B(\, \delta_{j1} \mid \delta_{j2} \mid \ldots \mid \delta_{jt}))$, dovoljno je pokazati da važi $I_t(\, B(\, \delta_{j1} \mid \delta_{j2} \mid \ldots \mid \delta_{jt})) \subseteq I_t((\, \delta_{j1} \mid \delta_{j2} \mid \ldots \mid \delta_{jt}))$. Drugim rečima, pri dokazu da je $\Delta \in I_t(C)$ možemo, bez gubitka na opštosti, smatrati da je $t = n \le m$. Stoga je $\Delta = \Delta(\, i_1, \ldots, i_n \,;\, 1, \ldots, n)$ za neki izbor vrsta sa indeksima $i_1, \ldots, i_n$, gde je $1 \le i_1 \le i_2 \le \ldots \le i_n \le m$.
Neka je $B = [b_{ij}] \in M_{m\times p}(R)$. Tada, na osnovu primera 17, imamo da je

$$(BC)_{i\to} = \sum\nolimits_{j=1}^{p} b_{ij} C_{j\to}, \text{ za sve } i = 1, \ldots, m.$$

Imajući u vidu da je determinanta višelinearno preslikavanje u odnosu na svoje vrste, važi

$$\Delta = \Delta(i_1, \dots, i_n; 1, \dots, n) = \det((BC)\, i_{1\rightarrow}; \dots; (BC)\, i_{n\rightarrow})) =$$

$$= \det((\sum_{j=1}^{p} b_{i_1 j} C_{j\rightarrow}; \cdots; \sum_{j=1}^{p} b_{i_n j} C_{j\rightarrow})) =$$

$$= \sum_{\alpha_1, \cdots, \alpha_n = 1}^{p} c_{\alpha_1, \cdots, \alpha_n} \det((C_{\alpha_1\rightarrow}; \cdots; C_{\alpha_n\rightarrow}))$$

gde su $c_{\alpha 1, \dots, \alpha n} \in R$ različite konstante u razvoju determinante. Sumiranje se vrši po indeksima $\alpha_1, \dots, \alpha_n$, pri čemu za svaki $i = 1, .., n$, indeks α_i uzima vrednosti od 1 do p. Za svaki izbor indeksa $\alpha_1, \dots, \alpha_n$, važi $\det(C_{\alpha 1\rightarrow}; \dots; C_{\alpha n\rightarrow}) \in I_t(C)$. Sve ove determinante su jednake nuli ako je $n > p$. U svakom slučaju je $\Delta(i_1, \dots, i_n; 1, \dots, n) \in I_t(C)$. Kako je determinanta Δ proizvoljni generator ideala $I_t(BC)$, možemo zaključiti da je $I_t(BC) \subseteq I_t(C)$.

Tvrdnja II: $I_t(A) = I_t(A^T)$ za svaki $t \in \mathbb{Z}$.

Ovo je jasno iz definicije. Naime, poznato je da je $\det A^T = \det A$, odnosno da su odgovarajući minori matrice A i njene transponovane matrice A^T jednaki, pa su otuda jednaki i ideali generisani tim minorima.

Tvrdnja III: $I_t(BC) \subseteq I_t(B)$ za svaki $t \in \mathbb{Z}$.

Neka je $t \in \mathbb{Z}$. Na osnovu tvrdnji I i II, imamo $I_t(BC) = I_t((BC)^T) = I_t(B^T C^T) \subseteq I_t(B^T) = I_t(B)$.

Sada, očigledno, tvrđenje leme proističe iz tvrdnji I i III.

■

Najvažnija posledica prethodne leme je sledeće tvrđenje

Posledica 4: Neka je $A \in M_{m\times n}(R)$ proizvoljna matrica, i $P \in \mathrm{GL}(m, R)$ i $Q \in \mathrm{GL}(n, R)$ inverzibilne matrice. Tada je $I_t(PAQ) = I_t(A)$, za svaki $t \in \mathbb{Z}$.

Dokaz: Najpre, prema lemi 3, važi $I_t(PA) \subseteq I_t(A)$, a kako je $I_t(A) = I_t(P^{-1}(PA)) \subseteq I_t(PA)$, imamo da važi $I_t(PA) = I_t(A)$, za svaki $t \in \mathbb{Z}$.

Slično, kako je $I_t(PAQ) \subseteq I_t(PA)$, i takođe $I_t(PA) = I_t((PAQ)\cdot Q^{-1}) \subseteq I_t(PAQ)$, sledi da je $I_t(PA) = I_t(PAQ)$. Konačno, $I_t(PAQ) = I_t(PA) = I_t(A)$.

■

Neka je $A \in M_{m\times n}(R)$ proizvoljna matrica.
Razmotrimo lanac ideala generisanih minorima matrice A u prstenu R

$$\{0\} = I_{r+1}(A) \subseteq I_r(A) \subseteq \dots \subseteq I_1(A) \subseteq I_0(A) = R.$$

Ukoliko odredimo anulatore svakog od ovih ideala, ponovo ćemo dobiti rastući lanac ideala

$$\{0\} = Ann_R(R) \subseteq Ann_R(I_1(A)) \subseteq Ann_R(I_2(A) \subseteq \dots \subseteq Ann_R(I_r(A)) \subseteq Ann_R(\{0\}) = R.$$

Pri tom, ako je $Ann_R(I_t(A)) \neq \{0\}$, onda je i $Ann_R(I_k(A)) \neq \{0\}$ za svaki $k \geq t$, jer je tada ideal $I_k(A) \subseteq I_t(A)$, pa je anulator $Ann_R(I_t(A)) \subseteq Ann_R(I_k(A))$.
Sada možemo definisati **rang** matrice $A \in M_{m\times n}(R)$ kao red maksimalnog minora matrice A, za koji je anulator ideala generisanog minorima tog reda trivijalan. Dakle, rang matrice $A \in M_{m\times n}(R)$ je broj

$$r(A) = \max\{\, t \mid Ann_R(I_t(A)) = \{0\}\}.$$

Navedimo neka osnovna svojstva koja ovako definisan rang matrice poseduje:

Tvrđenje 3. Za rang proizvoljne matrice $A \in M_{m\times n}(R)$ važe sledeće tvrdnje

1) $0 \le r(A) \le \min\{m, n\}$.
2) $r(A) = r(A^T)$.
3) $r(A) = r(PAQ)$ za sve inverzibilne matrice $P \in \mathrm{GL}(m, R)$ i $Q \in \mathrm{GL}(n, R)$.
4) $r(A) = 0$ ako i samo ako je $Ann_R(I_1(A)) \neq \{0\}$.
5) Ako je $m = n$, onda je $r(A) < n$ ako i samo ako je $\det A \in Z(R)$, tj. ako je $\det A$ delitelj nule u prstenu R.

Dokaz : 1) Zaista, kako je $I_0(A) = R$ i $Ann_R(R) = \{0\}$, jasno je da je $r(A) \ge 0$. S druge strane, ako je $t > \min\{m, n\}$, onda je $I_t(A) = \{0\}$, a pošto je $Ann_R(\{0\}) = R$, otuda je i $r(A) \le \min\{m, n\}$. Dakle, $0 \le r(A) \le \min\{m, n\}$.

2) Tvrđenje da je $r(A) = r(A^T)$ očigledno sledi iz tvrdnje II prethodne leme 3, da je $I_t(A^T) = I_t(A)$ za svaki $t \in \mathbb{Z}$.

3) Na osnovu prethodno navedene posledice 4 takođe očigledno sledi da je $r(A) = r(PAQ)$ za svaku matricu $A \in M_{m\times n}(R)$ i sve inverzibilne matrice $P \in \mathrm{GL}(m,R)$ i $Q \in \mathrm{GL}(n,R)$. Drugim rečima, ekvivalentne matrice imaju isti rang.

4) Tvrđenje direktno sledi iz definicije ranga, za slučaj $t \le 0$. Naime, ako je $Ann_R(I_1(A)) \neq \{0\}$, to s obzirom da anulatori ideala obrazuju rastući lanac $Ann_R(I_0(A)) \subseteq Ann_R(I_1(A))$, pri čemu je $I_0(A)=R$ i $Ann_R(R) = \{0\}$, sledi da je $Ann_R(I_t(A)) = \{0\}$ jedino za $t = 0$ tj. kada je $r(A) = 0$.

5) Ukoliko je $r(A) < n$, to prema definiciji ranga matrice znači da je anulator $Ann_R(I_n(A)) \neq \{0\}$, odnosno da postoji ne-nula element $x \in R$ takav da je $x \cdot m = 0$ za svaki $m \in I_n(A)$. Kako je ideal $I_n(A)$ generisan minorom reda n tj. samom determinantom $\det A$, to je $m = k\cdot\det A$ za neko $k \in R$, odnosno $y\cdot\det A = 0$ za $y = xk$, što znači da je $\det A \in Z(R)$.
Obratno, ako je determinanta matrice formata $n\times n$ delitelj nule u prstenu R, to znači da postoji bar jedan ne-nula element $x \in R$ takav da je $x\cdot\det A = 0$, a takav element pripada anulatoru $x \in Ann_R(I_n(A))$, pa je $Ann_R(I_n(A)) \neq \{0\}$, odakle prema definiciji sledi da n nije red maksimalnog minora za koji je anulator ideala generisanog tim minorom trivijalan, odnosno da rang $r(A) \neq n$, pa je $r(A) < n$ prema tvrđenju 3(1).

■

Neka je $A = [a_{ij}] \in M_{m\times n}(R)$. Na osnovu tačke (4) prethodnog tvrđenja, sledi da je $r(A) = 0$ ako i samo ako postoji ne-nula element $x \in R$ takav da je $xa_{ij} = 0$ za sve indekse $i = 1,..., m, j = 1,...,n$. Specijalno, za razliku od klasičnog slučaja kada je R polje, ovo znači da u slučaju komutativnog prstena i ne-nula matrica može imati rang jednak nuli.

Razmotrimo ove zaključke na sledećem primeru.

Primer 24. Neka je $R = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ prsten ostataka po modulu 6.

1) Neka je $A = \begin{bmatrix} 2 & 2 \\ 0 & 2 \end{bmatrix} \in M_2(\mathbb{Z}_6)$.

Kako je determinanta $\det A = 2\cdot 2 - 0\cdot 2 = 4 \in Z(R)$ tj. 4 je delitelj nule u prstenu $\mathbb{Z}_6$, na osnovu tačke (5) prethodnog tvrđenja možemo očekivati da je $r(A) < 2$.
Matrica A je, očigledno, ne-nula matrica, ali je svaka njena komponenta delitelj nule u prstenu $R = \mathbb{Z}_6$ i postoji ne-nula element $3 \in \mathbb{Z}_6$ takav da je i $3\cdot 0 = 0$ i $3\cdot 2 = 0$ u prstenu $\mathbb{Z}_6$, pa kao što smo rekli, na osnovu tačke (4) prethodnog tvrđenja sledi da je rang matrice A jednak nuli.
Zaista, kako je $\det A = 4$, to je ideal generisan minorom reda 2 jednak $I_2(A) = 4R$ pa je njegov anulator $Ann(4R) = 3R \neq \{0\}$. S druge strane, ideal $I_1(A) = 2R$, pa je i njegov anulator $Ann(2R) = 3R \neq \{0\}$. Dakle, na osnovu tačke (4) prethodnog tvrđenja, $r(A) = 0$.

2) Neka je $B = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} \in M_2(\mathbb{Z}_6)$.

Matrica B je, ponovo, ne-nula matrica čija je svaka komponenta delitelj nule u prstenu $R = \mathbb{Z}_6$, ali ne postoji ne-nula element $x \in \mathbb{Z}_6$ takav da je $xb_{ij} = 0$ za sve i,j, tj. rang matrice B neće biti nula. Pošto je, međutim, $\det B = 2 \cdot 3 - 0 = 0$ u $\mathbb{Z}_6$, na osnovu tačke (5) prethodnog tvrđenja sledi da je $r(B) < 2$. Da bi proverili da li je rang zaista jednak 1 odredićemo anulator ideala $I_1(B)$. Kako su odgovarajući minori jednaki 3, 0 i 2, njima je generisan ideal $I_1(B) = 2R + 3R = R$, pa je njegov anulator $Ann(R) = \{0\}$, odnosno rang matrice B je $r(B) = 1$.

3) Neka je $C = \begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix} \in M_2(\mathbb{Z}_6)$.

Kako determinanta $\det C = 1 \cdot 5 - 3 \cdot 2 = 5 - 0 = 5$ nije delitelj nule u $\mathbb{Z}_6$, na osnovu tačke (5) prethodnog tvrđenja će biti $r(C) = 2$, ali proverimo to i po definiciji. Kako je, naime, ideal $I_2(C) = 5R$ njegov anulator će biti $Ann(5R) = \{0\}$ pa je zaista $r(C) = 2$, te nema potrebe da razmatramo ideal $I_1(C)$.

Ukažimo sada na odnos ranga matrice sa komponentama iz komutativnog prstena R, definisanog na upravo izloženi način, i ranga matrice sa komponentama iz nekog polja F, definisanog na klasičan način. Kao što je poznato, rang $r_F(A)$ matrice $A \in M_{m\times n}(F)$, gde je F polje, se u linearnoj algebri definiše kao najveći broj linearno nezavisnih vrsta (kolona) matrice A. Drugim rečima, rang $r_F(A)$ je najveći ceo broj t za koji matrica A sadrži podmatricu formata $t \times t$ čija je determinanta različita od nule. S druge strane, ako primenimo definiciju da je rang matrice $r(A) = \max\{ t \mid Ann_F(I_t(A)) = \{0\}\}$, imajući pritom u vidu da je F polje, važiće da je anulator $Ann_F(I_t(A)) = \{0\}$ ako i samo ako je $I_t(A) \neq \{0\}$. To nas ponovo dovodi do zaključka da je rang $r(A)$ najveći ceo broj t za koji matrica A sadrži $t \times t$ podmatricu čija je determinanta koja generiše $I_t(A)$ različita od nule, odnosno da je $r_F(A) = r(A)$ u slučaju kada su komponente matrice A elementi polja F.

Pretpostavimo sada da je R oblast celih sa poljem razlomaka F. Neka je $A \in M_{m\times n}(R)$. Kako je $R \subseteq F$, biće i $M_{m\times n}(R) \subseteq M_{m\times n}(F)$, pa možemo matricu A smatrati i za matricu nad poljem F, tj. da $A \in M_{m\times n}(F)$. Pošto je R oblast celih, $Ann_R(I_t(A)) = \{0\}$ ako i samo ako je $I_t(A) \neq \{0\}$, pa je $r(A) = \max\{ t \mid$ matrica A poseduje ne-nula minor reda $t \}$, a taj rang je potpuno isti za slučaj kada je matrica $A \in M_{m\times n}(R)$ kao i u slučaju $A \in M_{m\times n}(F)$. Dakle, ako je prsten R oblast celih sa poljem razlomaka F, ponovo važi da je $r(A) = r_F(A)$.

Ukoliko je, međutim, R komutativan prsten sa pravim deliteljima nule može se, kao što smo videli, dogoditi da su minori koji generišu ideal $I_t(A)$ različiti od nule, ali su pravi delitelji nule u prstenu R, pa je tada anulator $Ann_R(I_t(A)) \neq \{0\}$, što prema definiciji znači da je rang $r(A) \neq t$. Dakle, klasična definicija da je rang matrice najveći ceo broj t za koji matrica A sadrži $t \times t$ podmatricu čija je determinanta različita od nule, u slučaju komutativnog prstena sa pravim deliteljima nule nije odgovarajuća.

Lema 4. Neka je $B \in M_{m\times p}(R)$ i $C \in M_{p\times n}(R)$. Tada je $r(BC) \leq \min\{r(B), r(C)\}$.

Dokaz: Dokažimo najpre da je $r(BC) \leq r(C)$.

Na osnovu leme 3, važi da je $R \supseteq I_1(C) \supseteq I_2(C) \supseteq \ldots$ kao i $R \supseteq I_1(BC) \supseteq I_2(BC) \supseteq \ldots$

Anulatori ovih ideala formiraju rastući lanac ideala u R

$\{0\} \subseteq Ann_R(I_1(C)) \subseteq Ann_R(I_2(C) \subseteq \ldots$, odnosno $\{0\} \subseteq Ann_R(I_1(BC)) \subseteq Ann_R(I_2(BC) \subseteq \ldots$

Pretpostavimo sada da je $r(C) = q$. Tada je $Ann_R(I_q(C)) = \{0\}$. S druge strane, to znači da je $Ann_R(I_{q+k}(C)) \neq \{0\}$, za sve $k > 0$. Kako je, prema lemi 3, $I_{q+k}(BC) \subseteq I_{q+k}(C)$, to je $Ann_R(I_{q+k}(C)) \subseteq Ann_R(I_{q+k}(BC))$, pa možemo zaključiti da je $Ann_R(I_{q+k}(BC)) \neq \{0\}$, za svaki $k > 0$. Otuda, važi da je $r(BC) \leq q$ tj. $r(BC) \leq r(C)$.
Slično se pokazuje i da je $r(BC) \leq r(B)$, što upravo znači da je $r(BC) \leq \min\{r(B), r(C)\}$.

■

Primer 25. Neka je matrica $A \in M_{m\times n}(R)$ i neka je $\boldsymbol{O}$ nula-matrica formata $m \times p$. Pokažimo da je $I_t(A \mid \boldsymbol{O}) = I_t(A)$ za svaki $t \in \mathbb{Z}$.

Posmatrajmo matrice

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \quad \text{i} \quad A \mid \boldsymbol{O} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & 0 & \cdots & 0 \end{bmatrix}_{m\times(n+p)}$$

Neka je Δ minor reda t matrice A koji je generator ideala $I_t(A)$, gde je $1 \leq t \leq min\{m, n\}$. Svaki takav minor je istovremeno sadržan u matrici $A \mid \boldsymbol{O}$, pa je istovremeno i generator ideala $I_t(A \mid \boldsymbol{O})$, otuda je i sam ideal $I_t(A) \subseteq I_t(A \mid \boldsymbol{O})$ za svako t. S druge strane, matrica $A \mid \boldsymbol{O}$ se sastoji upravo od kolona matrice A dopunjenih nula-kolonama. Neki njeni minori reda t jesu jednaki nuli, ali je svaki ne-nula minor reda t matrice $A \mid \boldsymbol{O}$ sačinjen upravo od vrsta i kolona koje potiču iz matrice A, pa otuda važi da je ideal $I_t(A \mid \boldsymbol{O}) \subseteq I_t(A)$, drugim rečima važi

$$I_t(A \mid \boldsymbol{O}) = I_t(A) \text{ za svaki } t \in \mathbb{Z}.$$

Sada možemo zaključiti da su i rangovi matrica A i $A \mid \boldsymbol{O}$ takođe jednaki, $r(A \mid \boldsymbol{O}) = r(A)$.

Primer 26. Neka je matrica $A \in M_{m\times n}(R)$ i neka je $\boldsymbol{O}$ nula-matrica formata $p \times n$. Slično prethodnom primeru, važi da je ideal $I_t\left(\frac{A}{\boldsymbol{O}}\right)$ generisan $t \times t$ minorima proširene matrice $\frac{A}{\boldsymbol{O}}$ jednak idealu $I_t(A)$ matrice A. Zaista, razmotrimo matrice

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \quad \text{i} \quad \frac{A}{\boldsymbol{O}} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}$$

Svaki ne-nula minor reda t matrice A sadržan je i u matrici $\frac{A}{\boldsymbol{O}}$, i obratno, pošto se matrica $\frac{A}{\boldsymbol{O}}$ sastoji upravo od vrsta matrice A dopunjenih nula–vrstama, onda je svaki ne-nula minor reda t matrice $\frac{A}{\boldsymbol{O}}$ takođe sadržan u matrici A. To znači da su i odgovarajući ideali jednaki, $I_t\left(\frac{A}{\boldsymbol{O}}\right) = I_t(A)$, a time i rangovi $r(A) = r\left(\frac{A}{\boldsymbol{O}}\right)$.

Navedimo kao ilustraciju postupka određivanja ranga matrice i sledeća dva primera.

Primer 27. Neka je $R = \mathbb{Z}_{30}$ prsten ostataka po modulu 30. To je komutativan prsten sa pravim deliteljima nule. Ako nad ovim prstenom razmotrimo matrice

$$A=\begin{bmatrix}2 & 0 & -3\\ 1 & 1 & 1\end{bmatrix} \qquad \text{i} \qquad B=\begin{bmatrix}2 & -3\\ 1 & 1\end{bmatrix}$$

uočićemo da su u njima svake dve kolone linearno zavisne.
Zaista, pokazuje se da je relacija

$$\alpha\begin{bmatrix}2\\1\end{bmatrix}+\beta\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}0\\0\end{bmatrix}, \text{ za skalare } \alpha,\ \beta\in R$$

moguća za npr. $\alpha=\beta=15$, što znači da su prve dve kolone matrice A linearno zavisne.
Slično, relacija nad prvom i trećom kolonom

$$\chi\begin{bmatrix}2\\1\end{bmatrix}+\delta\begin{bmatrix}-3\\1\end{bmatrix}=\begin{bmatrix}0\\0\end{bmatrix}, \text{ je moguća za } \chi=18,\ \delta=12$$

dok je relacija nad drugom i trećom kolonom

$$\mu\begin{bmatrix}0\\1\end{bmatrix}+\lambda\begin{bmatrix}-3\\1\end{bmatrix}=\begin{bmatrix}0\\0\end{bmatrix} \text{ moguća za vrednosti skalara } \mu=20,\ \lambda=10.$$

Dakle svake dve kolone matrice A su linearno zavisne.
Dalje, relacija

$$a\begin{bmatrix}2\\1\end{bmatrix}+b\begin{bmatrix}-3\\1\end{bmatrix}=\begin{bmatrix}0\\0\end{bmatrix}, \text{ za } a,\ b\in R$$

nad kolonama matrice B je moguća za npr. $a=3$ i $b=2$, pa su i one linearno zavisne nad prstenom $\mathbb{Z}_{30}$.

U matrici A su vrste linearno nezavisne, a svaki od minora reda 2 je delitelj nule u prstenu $\mathbb{Z}_{30}$ (2, 3 i 5). Ideal generisan tim minorima je $I_2(A) = 2R + 3R + 5R = R$ pa je njegov anulator $Ann(R) = \{0\}$, odnosno rang matrice je $r(A) = 2$.
Zaista, relacija

$$\alpha\begin{bmatrix}2 & 0 & -3\end{bmatrix}+\beta\begin{bmatrix}1 & 1 & 1\end{bmatrix}=\begin{bmatrix}0 & 0 & 0\end{bmatrix}, \text{ za skalare } \alpha,\ \beta\in R$$

tj. sistem uslova

$$\left.\begin{aligned}2\alpha+\beta&=0\\ \beta&=0\\ -3\alpha+\beta&=0\end{aligned}\right\} \Leftrightarrow \left.\begin{aligned}2\alpha&=0\\ -3\alpha&=0\end{aligned}\right\} \Leftrightarrow \alpha=0$$

je jedino moguć za $\alpha=0$ i $\beta=0$, tj. vrste matrice A su linearno nezavisne.
U matrici B su, s druge strane, i vrste linearno zavisne. Relacija

$$a\begin{bmatrix}2 & -3\end{bmatrix}+b\begin{bmatrix}1 & 1\end{bmatrix}=\begin{bmatrix}0 & 0\end{bmatrix} \text{ za } a,\ b\in R$$

moguća je za npr. $a=2$ i $b=6$. Njena determinanta je različita od nule, det$B$ = 5, ali je pravi delitelj nule u $\mathbb{Z}_{30}$, tako da je $r(B) < 2$ prema tvrđenju 3(5). Kako je, dalje, ideal $I_1(B) = R$, njegov anulator je $Ann(I_1(B))=\{0\}$ pa je rang matrice $r(B) = 1$.

Primer 28. Neka je sada $R = \mathbb{Z}_{12}$ prsten ostataka po modulu 12, takođe komutativan prsten sa pravim deliteljima nule (2, 3, 4, 6, 8, 9 i 10). Razmotrimo matrice

$$A = \begin{bmatrix} 2 & 2 \\ 4 & 6 \end{bmatrix} \qquad B = \begin{bmatrix} 2 & 3 & 5 \\ 2 & 0 & 2 \\ 2 & 4 & 6 \end{bmatrix} \qquad \text{i} \qquad C = \begin{bmatrix} 1 & 4 & 2 & 7 \\ 2 & 1 & 8 & 2 \\ 3 & 0 & 3 & 4 \end{bmatrix}$$

Najpre, $\det A = -8 = 4 \in Z(R)$ pa je $r(A) < 2$ na osnovu tvrđenja 3(5), ali kako je $I_1(A) = 2R$ i njegov anulator $Ann(I_1(B)) = 6R \neq \{0\}$, sledi da je $r(A)=0$.

Dalje, posmatrajmo matricu B, tu je $\det B = 0$ pa je rang $r(B) < 3$, minori reda 2 ovde su -8 (tj. 4 u prstenu $\mathbb{Z}_{12}$), $-4=8$, 8, $-2=10$, $-10=2$, 2, 6, $-6=6$ i -6, pa je njima generisan ideal $I_2(A) = 2R$ čiji je anulator $Ann(I_2(B)) = 6R \neq \{0\}$, tako da je konačno $I_1(B) = R$, odnosno rang matrice je $r(B) = 1$.

Na kraju, minori reda 3 matrice C su -3 (tj. 9 u prstenu $\mathbb{Z}_{12}$), $4, -1 = 11$ i 9, pa je njima generisan ideal $I_3(B)=R$, tj. $Ann(I_3(C))=\{0\}$, što znači da je $r(C) = 3$.

§5 SISTEMI LINEARNIH JEDNAČINA

U ovom poglavlju ćemo navesti osnovne teoreme koje se tiču rešavanja sistema linearnih jednačina nad komutativnim prstenom R.

Razmotrimo sledeći sistem od m linearnih jednačina sa n nepoznatih $x_1, ..., x_n$

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases}.$$

gde su koeficijenti a_{ij} i slobodni članovi $b_1, ..., b_m$ u ovim jednačinama elementi komutativnog prstena R. Ovaj sistem jednačina se, ekvivalentno, može zapisati u matričnom obliku kao

$$AX = B$$

gde je $A = [a_{ij}] \in M_{m\times n}(R)$ matrica koeficijenata, $X = [x_1, ..., x_n]^T \in (R[x_1, ..., x_n])^n$ kolona nepoznatih i $B = [\, b_1, ..., b_m \,]^T \in R^m$ kolona slobodnih članova.
Navedeni sistem jednačina **ima rešenje** (u R^n) ako postoji n-torka $\xi \in R^n$ takva da je $A\xi = B$.
Ako su svi slobodni članovi $b_i = 0$ tj. ako je $B = 0$, za sistem jednačina $AX = 0$ kažemo da je **homogen**. Homogeni sistem jednačina uvek ima bar jedno, **trivijalno** rešenje $\xi = \boldsymbol{O} = (0, .., 0)^T \in R^n$.
Rešenje $\xi \in R^n$ nazivamo **netrivijalnim** rešenjem homogenog sistema jednačina $AX = 0$ ako je $\xi \neq 0$ i $A\xi = 0$.

Navedimo sada poznatu McCoyovu[7] teoremu koja pruža potreban i dovoljan uslov da homogeni sistem jednačina ima netrivijalno rešenje.

Teorema 6. Neka je $A \in M_{m\times n}(R)$. Homogeni sistem linearnih jednačina $AX = 0$ ima netrivijalno rešenje ako i samo ako je rang matrice A manji od broja nepoznatih, $r(A) < n$.

Dokaz: ($\Rightarrow$) Pretpostavimo da sistem $AX = 0$ ima netrivijalno rešenje $\xi \in R^n$. Pošto je $\xi \neq 0$, bar neka koordinata n-torke $\xi = (\xi_1, ..., \xi_n)$ nije nula, na primer $\xi_k \neq 0$.
Ako je broj jednačina manji od broja nepoznatih, $m < n$, onda na osnovu tvrđenja 3(1) sledi da je $r(A) \leq \min\{m, n\} = m < n$.
Pretpostavimo, zato, da je $m \geq n$.
Neka je $\Delta = \Delta(\, i_1, ... , i_n \,;\, 1, ... , n)$ minor reda $n\times n$ matrice A.
Tada postoji permutaciona[8] matrica $P \in \mathrm{Gl}(m,R)$ takva da su vrste $i_1, ... , i_n$ matrice A na mestu prvih n vrsta matrice PA,
tj. važi $(PA)_{1\to} = A_{i1\to}, (PA)_{2\to} = A_{i2\to}, ... , (PA)_{n\to} = A_{in\to}$.

$$PA = \left[\begin{array}{cccc} a_{i_1 1} & a_{i_1 2} & \cdots & a_{i_1 n} \\ a_{i_2 1} & a_{i_2 2} & \cdots & a_{i_2 n} \\ \vdots & \vdots & & \vdots \\ \underline{a_{i_n 1}} & \underline{a_{i_n 2}} & \cdots & \underline{a_{i_n n}} \\ & & * & \end{array}\right]$$

[7] Neal McCoy (1904 – 2001.god.), američki matematičar
[8] Za matricu $A \in M_n(R)$ kažemo da je permutaciona ako se može dobiti iz jedinične matrice E permutovanjem njenih kolona.

Označimo podmatricu koja odgovara minoru Δ sa D

$$D=\begin{bmatrix} a_{i_1 1} & a_{i_1 2} & \cdots & a_{i_1 n} \\ a_{i_2 1} & a_{i_2 2} & \cdots & a_{i_2 n} \\ \vdots & \vdots & & \vdots \\ a_{i_n 1} & a_{i_n 2} & \cdots & a_{i_n n} \end{bmatrix}$$

Sada je $\Delta = \det D = \Delta(i_1, \dots, i_n; 1, \dots, n)$. Kako je $A\xi = 0$ to je i $D\xi = 0$ takođe, pa važi $\Delta\xi = (\Delta E_n)\xi = (\mathrm{adj}D\cdot D)\xi = \mathrm{adj}D\cdot(D\xi) = 0$ jer je, kao što je odranije poznato, $\mathrm{adj}D\cdot D = \det D\cdot E_n$. Ovo konkretno znači da je $\Delta\xi_k = 0$, odnosno, pošto je $\Delta = \Delta(i_1, \dots, i_n; 1, \dots, n)$ proizvoljan minor reda n matrice A, tj. $\Delta \in I_n(A)$, možemo zaključiti da je $\xi_k \in Ann_R(I_n(A))$, tj. pošto je $\xi_k \neq 0$, znači da $Ann_R(I_n(A)) \neq 0$, pa je $r(A) < n$.

($\Leftarrow$) Obratno, pretpostavimo da je $r(A) = r < n$.

Ako je rang matrice koeficijenata jednak broju jednačina sistema, $r = m$, možemo dati sistem dopuniti jednačinama koje imaju koeficijente nula, tako da on dobija sledeći oblik

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \\ \vdots \\ \\ \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \\ \vdots \\ \\ \\ 0 \end{bmatrix}$$

Očigledno, svako ne-nula rešenje $\xi \in R^n$ ovog sistema biće istovremeno netrivijalno rešenje polaznog sistema $AX = 0$. Kako je, za svako $t \in \mathbb{Z}$, ideal $I_t(A)$ generisan minorima reda t matrice A jednak idealu $I_t\left(\frac{A}{\boldsymbol{O}}\right)$ proširene matrice $\frac{A}{\boldsymbol{O}}$, gde je $\boldsymbol{O}$ nula-matrica formata $p \times n$, sledi da su i rangovi $r(A) = r\left(\frac{A}{\boldsymbol{O}}\right)$.

Dakle, možemo pretpostaviti da je $r < \min\{m, n\}$, jer se dati sistem ako je potrebno može, kao što smo videli, proširiti nula-jednačinama.

Kako je $r(A) = r$, ideal $Ann_R(I_{r+1}(A)) \neq \{0\}$ pa postoji neki ne-nula element $a \in Ann_R(I_{r+1}(A))$.

Ako je rang $r = 0$, tada $a \in Ann_R(I_1(A))$, pa je $\xi = (a, a, \dots, a) \in R^n$ netrivijalno rešenje sistema $AX = 0$.

Konačno, možemo pretpostaviti da je $1 \leq r < \min\{m, n\}$.

Iz $r(A) = r$, po definiciji, sledi da je ideal $Ann_R(I_r(A)) = \{0\}$. To, konkretno, znači da postoji minor $\Delta(i_1, \dots, i_r; j_1, \dots, j_r)$ reda r matrice A takav da $a \cdot \Delta(i_1, \dots, i_r; j_1, \dots, j_r) \neq 0$. Možemo pomnožiti matricu A odgovarajućim permutacionim matricama $P \in \mathrm{GL}(m,R)$ i $Q \in \mathrm{GL}(n,R)$ sa leve i desne strane, tako da vrste $i_1, \dots, i_r$ i kolone $j_1, \dots, j_r$ matrice A u novoj matrici PAQ budu na mestu prvih r vrsta i r kolona. Označimo odgovarajuću $r \times r$ podmatricu matrice PAQ sa C

$$PAQ = \left[\begin{array}{c|c} C & * \\ \hline * & * \end{array}\right] \text{ gde je } C \in M_r(R) \text{ i } \det C = \Delta(i_1, \dots, i_r; j_1, \dots, j_r).$$

Pretpostavimo da jednačina $(PAQ)X = 0$ ima netrivijalno rešenje $\beta \in R^n$. Pošto su matrice P i Q inverzibilne, ovde je $\xi = Q\beta \neq 0$ i $A\xi = 0$. Dakle, jednačina $AX = 0$ će imati netrivijalno rešenje.

Kako je, prema posledici leme 3, $I_t(PAQ) = I_t(A)$, za svaki $t \in \mathbb{Z}$, dovoljno je dokazati da jednačina $(PAQ)X = 0$ ima netrivijalno rešenje. Drugim rečima, ako je potrebno da umesto matrice A posmatramo matricu PAQ, možemo takođe, bez gubitka na opštosti, pretpostaviti da je

$$\Delta(i_1, \dots, i_r; j_1, \dots, j_r) = \Delta(1, \dots, r; 1, \dots, r).$$

Neka je $\Delta = \Delta(1, \dots, r; 1, \dots, r)$. Tada je i

$$A=\left[\begin{array}{c|c} C & * \\ \hline * & * \end{array}\right] \text{ za matricu } C=\begin{bmatrix} a_{11} & \cdots & a_{1r} \\ \vdots & & \vdots \\ a_{r1} & \cdots & a_{rr} \end{bmatrix}$$

pri čemu je $\Delta = \det D$ i, takođe, $a\Delta \neq 0$.
Neka je

$$C'=\begin{bmatrix} a_{11} & \cdots & a_{1r} & a_{1r+1} \\ \vdots & & \vdots & \vdots \\ a_{r1} & \cdots & a_{rr} & a_{rr+1} \\ a_{r+11} & \cdots & a_{r+1r} & a_{r+1r+1} \end{bmatrix} \in M_{(r+1)}(R).$$

Označimo sa $d_j = C'_{(r+1)j}$ kofaktor $(r+1,j)$-te komponente matrice C', za sve $j = 1, ..., r+1$.
Dakle, $d_1, ..., d_{r+1}$ su kofaktori poslednje vrste matrice C'. Na osnovu Laplasovog razvoja determinante imamo da je

$$\sum_{j=1}^{r+1} a_{r+1\,j}\, d_j = \det C' \in I_{r+1}(A)$$

Neka je $\xi = (ad_1, ..., ad_{r+1}, 0, ..., 0)^T \in R^n$. Kako je $a \cdot d_{r+1} = a\Delta \neq 0$, važi da je $\xi \neq 0$. Pokažimo da je ξ rešenje jednačine $AX = 0$.

Pošto je $A\xi = 0$ ako i samo ako je $\sum_{j=1}^{r+1} a_{ij}(ad_j) = 0$ za sve $i = 1,..., m$, potrebno je da razmotrimo sledeća dva slučaja:
Pretpostavimo, prvo, da je $1 \leq i \leq r$. Tada, prema teoremi 3(1) o Laplaceovom razvoju determinante, važi

$$\sum_{j=1}^{r+1} a_{ij}(ad_j) = a\,(\sum_{j=1}^{r+1} a_{ij} d_j) = 0.$$

Pretpostavimo, sada, da je $i \geq r+1$. Važi da je

$$\sum_{j=1}^{r+1} a_{ij}(ad_j) = a \det \begin{bmatrix} a_{11} & \cdots & a_{1r+1} \\ \vdots & & \vdots \\ a_{r1} & \cdots & a_{rr+1} \\ a_{i\,1} & \cdots & a_{ir+1} \end{bmatrix} \in aI_{r+1}(A) = 0.$$

U svakom slučaju je $A\xi = 0$, tj $\xi \in R^n$ je netrivijalno rešenje sistema $AX = 0$.

■

Posledica 5: Svaki homogeni sistem linearnih jednačina ima netrivijalno rešenje ako je broj jednačina tog sistema manji od broja nepoznatih.

Dokaz: Neka je $AX = 0$ matrični zapis sistema linearnih jednačina u kome je broj jednačina manji od broja napoznatih. Ako je matrica koeficijenata $A \in M_{m\times n}(R)$, to znači da je $m < n$. Na osnovu tvrđenja 3(1) o rangu matrice, važi da je $r(A) \leq \min\{m,n\} = m < n$, pa prema prethodnoj teoremi, sistem $AX = 0$ ima netrivijalno rešenje.

■

Pored upravo navedene posledice, postoji još niz često primenjivanih tvrđenja čiji dokazi direktno slede iz McCoyove teoreme. Ovu teoremu, takođe, možemo primeniti u razmatranju baza konačno generisanog slobodnog R-modula. Sledeća teorema nam daje uslove za definiciju ranga slobodnog R-modula.

Teorema 7. Neka je M konačno generisani modul nad komutativnim prstenom R. Neka je $\{m_1, ..., m_k\}$ skup elemenata modula M koji su linearno nezavisni nad R i neka je $\{p_1, ..., p_n\}$ skup generatora modula M. Tada je $k \leq n$. Posebno, ako je $k = n$, onda je skup $\{p_1, ..., p_n\}$ baza R-modula M.

Dokaz: Kako je skup $\{p_1, ..., p_n\}$ jedna generatrisa modula M, znači da postoje skalari $a_{ij} \in R$ takvi da je $m_j = \sum_{i=1}^{n} a_{ij} p_i$, za $j = 1, ..., k$. Zapišimo elemente a_{ij} kao matricu $A = (a_{ij}) \in M_{n\times k}(R)$.
Ako je $k >$ n , na osnovu prethodne posledice sledi da sistem $AX = 0$ ima netrivijalno rešenje, $\xi = (r_1, ..., r_k)^T \in R^k$. Ali tada je

$$\sum_{j=1}^{k} r_j m_j = \sum_{j=1}^{k} r_j \left(\sum_{i=1}^{n} a_{ij} p_i \right) = \sum_{i=1}^{n} \left(\sum_{j=1}^{k} a_{ij} r_j \right) p_i = \sum_{i=1}^{n} (0)\, p_i = 0 \qquad (*)$$

Kako su međutim, elementi $\{m_1, ..., m_k\}$ linearno nezavisni, iz prethodne jednakosti sledi da je $r_1 = ... = r_k = 0$, a to je nemoguće pošto je rešenje ξ netrivijalno, što znači da bi bar jedna od komponenata $r_1, ..., r_k$ morala biti različita od nule.
Dakle, važi da je $k \leq n$ i prvi deo teoreme smo ovim dokazali.
Neka je sada $k = n$. Drugim rečima, pretpostavimo da modul M sadrži n elemenata $m_1, ..., m_n$ koji su linearno nezavisni nad prstenom R i da, takođe, sadrži n elemenata $p_1, ..., p_n$ koji su generatori tog modula. Dokazaćemo da su, u tom slučaju, i elementi $p_1, ..., p_n$ linearno nezavisni nad prstenom R i da time čine i jednu bazu R-modula M.
Neka je, ponovo, $m_j = \sum_{i=1}^{n} a_{ij} p_i$, sada za $j = 1, ...,n$ i neka je $A = (a_{ij}) \in M_n(R)$.
Iz jednakosti $(*)$ sledi da homogeni sistem $AX = 0$ neće imati netrivijalno rešenje, pa na osnovu McCoyove teoreme sledi da je $r(A) = n$.
Pređimo sada na potpuni prsten razlomaka $Q(R)$ prstena R, gde je

$$Q(R) = \{x/y \mid x,y \in R \text{ i element } y \text{ je regularan}\}.$$

Prsten R se sada poklapa sa potprstenom $\{x/1 \mid x \in R\} \subseteq Q(R)$, pa je i $A \in M_n(R) \subseteq M_n(Q(R))$.
Kako je $r(A) = n$, na osnovu tvrđenja 3(5), o rangu matrice, sledi da je detA regularan element u prstenu R, tj. $\det A \in U(Q(R))$, što prema posledici teoreme 3, o Laplaceovom razvoju determinante, znači da je matrica A inverzibilna u $M_n(Q(R))$. Označimo inverznu matricu matrice A sa $B = (b_{ij}) \in M_n(Q(R))$.
Pretpostavimo da je $y_1p_1 + y_2p_2 + ... + y_np_n = 0$ za neki $\xi = (y_1, ..., y_n)^T \in R^n$.
Neka je $c_j = \sum_{k=1}^{n} y_k b_{jk}$ za $j = 1, ..., n$.
Tada je $(c_1, ..., c_n)^T = B\xi \in (Q(R))^n$. Pošto je $AB = E$ u $M_n(Q(R))$, imamo da je

$$\sum_{j=1}^{n} c_j m_j = \sum_{j=1}^{n} c_j \left(\sum_{i=1}^{n} a_{ij} p_i \right) = \sum_{i=1}^{n} \left(\sum_{j=1}^{n} a_{ij} c_j \right) p_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{n} a_{ij} \left(\sum_{k=1}^{n} y_k b_{jk} \right) \right) p_i =$$

$$= \sum_{i=1}^{n} \left(\sum_{k=1}^{n} y_k \left(\sum_{j=1}^{n} a_{ij} b_{jk} \right) \right) p_i = \sum_{i=1}^{n} \left(\sum_{k=1}^{n} y_k \delta_{ik} \right) p_i = \sum_{i=1}^{n} y_i p_i = 0$$

Svaki konačan broj elemenata iz $Q(R)$ ima zajednički imenilac, pa postoji regularni element $x \in R$ takav da su $xc_1, ..., xc_n \in R$. Iz prethodne jednakosti sledi da je

$$\sum_{j=1}^{n} (xc_j)\, m_j = 0$$

pa kako su $m_1, ..., m_n$ linearno nezavisni nad prstenom R, možemo zaključiti da je $xc_1 = ... = xc_n = 0$. Element $x \in R$ je regularan, pa time i inverzibilan u $Q(R)$. Otuda zaključujemo da je $c_1 = ... = c_n = 0$. Pošto je, opet, matrica B inverzibilna, imamo da je $\xi = 0$. Dakle, $y_1 = ... = y_n = 0$, pa sledi da su generatori $p_1, ..., p_n$ linearno nezavisni nad prstenom R, tj. da je skup $\{p_1, ..., p_n\}$ jedna baza R-modula M.

■

Posledica 6: Ako su R-moduli R^n i R^m izomorfni, $R^n \cong R^m$, onda je $n = m$.

Dokaz: Neka je η: $R^n \to R^m$ izomorfizam R-modula R^n u modul R^m i neka je $\varepsilon = \{\varepsilon_1, ..., \varepsilon_n\}$ kanonska baza modula R^n. Dakle $\varepsilon_1 = (1, 0, ..., 0)^T$, $\varepsilon_2 = (0, 1, ..., 0)^T$, ..., $\varepsilon_n = (0, 0, ..., 1)^T$ u modulu R^n. Pošto je η izomorfizam, slike $\eta(\varepsilon_1)$, ..., $\eta(\varepsilon_n)$ su takođe linearno nezavisne u modulu R^m. Kanonska baza modula R^m sadrži m vektora, pa na osnovu teoreme 7 sledi da je $n \le m$. Ako zamenimo uloge modula R^n i R^m u ovom dobijamo da je i $m \le n$, pa je otuda $n = m$.

■

Prema tome, ako je M konačno generisan slobodan modul nad komutativnim prstenom R, onda sve njegove baze imaju isti broj elemenata. Ovo je analogno slučaju konačno-dimenzionog vektorskog prostora V nad poljem F, gde takođe važi da sve njegove generatrise imaju isti broj elemenata i taj broj se naziva dimenzijom vektorskog prostora V, $dim(V)$. Sada, broj elemenata baze konačno generisanog slobodnog R-modula M nazivamo **rangom** tog modula, u oznaci $r(M)$. Tako je, na primer, $r(R^n) = n$ dok je $r(M_{m\times n}(R)) = mn$. Ako bi prsten R bio i polje, onda bi dimenzija konačno-dimenzionog vektorskog prostora V nad tim poljem R bila upravo jednaka ovako definisanom rangu, $dim(V) = r(V)$.

Posledica 7: Neka su matrice $P, Q \in M_{m\times n}(R)$ takve da su prostori kolona tih matrica jednaki u modulu R^m, $CS(P) = CS(Q)$. Ako su kolone matrice P linearno nezavisne u R^m, onda postoji inverzibilna matrica $S \in GL(n,R)$, takva da je $P = QS$.

Dokaz: Neka su $P = (\delta_1 \mid \delta_2 \mid ... \mid \delta_n)$ i $Q = (\lambda_1 \mid \lambda_2 \mid ... \mid \lambda_n)$ particije po kolonama matrica P i Q. Tada je $R\delta_1 + R\delta_2 + ... + R\delta_n = CS(P) = CS(Q) = R\lambda_1 + R\lambda_2 + ... + R\lambda_n$. Kako su kolone $\delta_1, \delta_2, ..., \delta_n$ linearno nezavisne, skup $\{\delta_1, \delta_2, ..., \delta_n\}$ je baza R-modula $CS(P)$. To znači da je, na osnovu teoreme 7, i skup $\{\lambda_1, \lambda_2, ..., \lambda_n\}$ jedna baza modula $CS(P)$. Neka je $\delta_i = \sum_{j=1}^{n} v_{ij}\lambda_j$ za $i = 1, ..., n$, i neka je $\lambda_i = \sum_{j=1}^{n} t_{ij}\delta_j$, takođe za $i = 1, ..., n$, gde su v_{ij} i t_{ij} skalari iz komutativnog prstena R. Neka su $V = (v_{ij})$ i $T = (t_{ij})$ matrice iz $M_n(R)$.

Kako je

$$\delta_i = \sum_{j=1}^{n} v_{ij}\lambda_j = \sum_{j=1}^{n} v_{ij}\left(\sum_{k=1}^{n} t_{jk}\delta_k\right) = \sum_{k=1}^{n}\left(\sum_{j=1}^{n} v_{ij}t_{jk}\right)\delta_k ,$$

možemo zaključiti da je $\sum_{j=1}^{n} v_{ij}t_{jk} = \delta_{ik}$, pa je zbog toga $VT = E$.

Posebno, $V \in GL(n, R)$ i $TV = E$.

Neka je $S = V^T$. Tada je $S \in GL(n, R)$, pa na osnovu primera 14 i 15, o blok-množenju matrica, sledi da je

$$QS = \left[\, QS_{\downarrow 1} \,\middle|\, QS_{\downarrow 2} \,\middle|\, \cdots \,\middle|\, QS_{\downarrow n} \,\right] = \left[\, \sum_{j=1}^{n} [S]_{j1}\lambda_j \,\middle|\, \cdots \,\middle|\, \sum_{j=1}^{n} [S]_{jn}\lambda_j \,\right] =$$

$$= \left[\, \sum_{j=1}^{n} v_{j1}\lambda_j \,\middle|\, \cdots \,\middle|\, \sum_{j=1}^{n} v_{jn}\lambda_j \,\right] = \left(\, \delta_1 \mid \delta_2 \mid \cdots \mid \delta_n \,\right) = P$$

■

Pretpostavka da su kolone matrice P linearno nezavisne u R^m je ključna u tvrđenju prethodne posledice i ne može se izostaviti čak ni u slučaju 1×1 matrica tj. skalara iz prstena R. Neka su, naime, dati skalari $a,b\in R$ i neka je element a regularan u prstenu R. Uvedimo oznake za matrice, $P=(a)$ i $Q=(b)$. Tada su kolone matrice P linearno nezavisne u prstenu R. Pretpostavimo da su prostori kolona tih matrica jednaki, $CS(P) = CS(Q)$, što ustvari znači da je $Ra = Rb$. Sada, na osnovu posledice 7, sledi da postoji inverzibilan element $u\in U(R)$, takav da je $a = bu$.
Dakle, ako je $Ra = Rb$ i ako je pri tom element a regularan, onda su a i b pridruženi elementi u prstenu R, $a\sim b$.

Posledica 7 nas, dalje, dovodi do sledećeg tvrđenja, koje daje interesantnu karakterizaciju inverzibilnih matrica u modulu $M_n(R)$.

Posledica 8: Neka je $P = (\delta_1 \mid \delta_2 \mid ... \mid \delta_n)\in M_n(R)$. Matrica P je inverzibilna ako i samo ako je skup njenih kolona $\{ \delta_1 \mid \delta_2 \mid ... \mid \delta_n \}$ jedna baza R-modula R^n .

Dokaz: ($\Rightarrow$) Pretpostavimo da je je skup $\{ \delta_1 \mid \delta_2 \mid ... \mid \delta_n \}$ jedna baza R-modula R^n . Kolone jedinične matrice E čine kanonsku bazu ovog prostora, $\varepsilon_1= (1, 0, ..., 0)^T$,..., $\varepsilon_n=(0, 0, ..., 1)^T$. Stoga, na osnovu posledice 7, važi $P = ES$, za neku inverzibilnu matricu $S\in GL(n, R)$, što posebno znači da je i $P\in GL(n, R)$.

($\Leftarrow$) Obratno, pretpostavimo da je matrica P inverzibilna, $P = (\delta_1 \mid \delta_2 \mid ... \mid \delta_n) \in GL(n, R)$. Tada jednačina $PX = \lambda$ ima jedinstveno rešenje $P^{-1}\lambda = (y_1, ..., y_n)^T$ za svaki $\lambda\in R^n$. Otuda je $y_1\delta_1 + ... + y_n\delta_n = \lambda$. Posebno, skup $\{\delta_1, \delta_2, ..., \delta_n\}$ je generatrisa R-modula R^n. Pretpostavimo da je $z_1\delta_1 + ... + z_n\delta_n = 0$ u R^n . Neka je $\xi = (z_1, ..., z_n)^T \in R^n$. Tada važi da je $P\xi = 0$ i $\xi = P^{-1}(P\xi) = P^{-1}\boldsymbol{O} = \boldsymbol{O}$. Dakle, $z_1 = z_2 = ... = z_n = 0$, pa su kolone $\delta_1, \delta_2, ..., \delta_n$ linearno nezavisne nad prstenom R. Otuda je skup $\{\delta_1, \delta_2, ..., \delta_n\}$ jedna baza R-modula R^n.

■

Razmotrimo sada rešavanje **nehomogenog** sistema od m jednačina sa n nepoznatih

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases}$$

nad komutativnim prstenom R.
Ovaj sistem se, kao što smo rekli, može posmatrati i u ekvivalentnom obliku, kao matrična jednačina $AX=B$ sa matricom koeficijenata $A=[a_{ij}]\in M_{m\times n}(R)$, kolonom nepoznatih $X=[x_1,..., x_n]^T$ i kolonom $B = [b_1, ..., b_m]^T$ slobodnih članova od kojih je bar jedan različit od nule, $b_i \neq 0$ za $i = 1,...,m$.

Za određivanje jedinstvenog rešenja sistema $AX = B$ u slučaju kada je broj jednačina sistema jednak broju nepoznatih, često je se oslanjamo na poznato Cramerovo[9] pravilo. Rešenje se određuje preko determinante matrice koeficijenata A i tzv. karakterističnih determinanti koje se dobijaju zamenom odgovarajuće kolone matrice A kolonom slobodnih članova B.

[9] Gabriel Cramer (1704 – 1752.god.), švajcarski matematičar

Teorema 8. (Cramerovo pravilo)

Neka je $A \in M_n(R)$ matrica sa inverzibilnom determinantom u prstenu R, $\det A \in U(R)$. Tada jednačina $AX=B$ ima jedinstveno rešenje $\xi=(y_1, ..., y_n)^T$ za svako $B=[b_1, ..., b_n]^T \in R^n$, pri čemu je

$$y_j = (\det A)^{-1} \det \begin{bmatrix} a_{11} & \cdots & a_{1\,j-1} & b_1 & a_{1\,j+1} & \cdots & a_{1n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & \cdots & a_{n\,j-1} & b_n & a_{n\,j+1} & \cdots & a_{nn} \end{bmatrix}, \quad \text{za sve} \quad j = 1,...,n\,.$$

Dokaz: Neka je $\xi = (y_1, ..., y_n)^T \in R^n$ n-torka čije su komponente y_j definisane na navedeni način. Na osnovu teoreme 3, o Laplaceovom razvoju determinante, za svaku od komponenata y_j važi da je

$$\det A \cdot y_j = \det \begin{bmatrix} a_{11} & \cdots & a_{1\,j-1} & b_1 & a_{1\,j+1} & \cdots & a_{1n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & \cdots & a_{n\,j-1} & b_n & a_{n\,j+1} & \cdots & a_{nn} \end{bmatrix} = \sum_{i=1}^{n} b_i A_{ij}$$

gde je Aij kofaktor (i,j)-te komponente matrice A. Dakle, imamo da važi

$$\det A \cdot \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} \sum_{i=1}^{n} A_{i1} b_i \\ \vdots \\ \sum_{i=1}^{n} A_{in} b_i \end{bmatrix} = \operatorname{adj} A \cdot B$$

Kako je $\det A \cdot E_n = \operatorname{adj} A \cdot A$, na osnovu prethodne jednakosti sledi da je $\operatorname{adj} A \cdot [A\xi] = \operatorname{adj} A \cdot B$, a pošto je adjungovana matrica $\operatorname{adj} A$ inverzibilna, sa inverzom $(\det A)^{-1} \cdot A$, sledi da je $A\xi = B$.
Dokažimo sada da je ovako određeno rešenje $\xi \in R^n$ jedinstveno.
Pretpostavimo da je i n-torka $\xi' \in R^n$ rešenje jednačine $AX = B$. Tada je $A\xi' = A\xi = B$, pa otuda sledi da je $A(\xi - \xi') = 0$, a kako je matrica A inverzibilna, to znači da je $\xi - \xi' = 0$, tj. $\xi = \xi'$. Dakle, rešenje $\xi \in R^n$ je jedinstveno rešenje jednačine $AX = B$.

■

Dakle, ako je matrica $A \in M_n(R)$ inverzibilna, sistem $AX = B$, od n jednačina sa n nepoznatih, će imati jedinstveno rešenje za svaku kolonu slobodnih članova $B \in R^n$. Sama formula za određivanje tog rešenja po Cramerovom pravilu je, međutim, dosta nepodesna za praktičnu primenu u slučaju sistema sa većim brojem jednačina i nepoznatih tj. kada je potrebno izračunavati determinante većeg formata, pa se tada koristi Gausov algoritam ili neki drugi metod.

Primer 29. Neka je $R = \mathbb{Z}_4$ prsten ostataka po modulu 4. Odredimo sva rešenja sistema jednačina $AX = B$ gde je

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 1 & 2 \\ 1 & 0 & 2 \end{bmatrix} \in M_3(R) \quad \text{i} \quad B = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} \in R^3$$

Kako je, najpre, $\det A = 3 \in U(R)$, ovaj sistem jednačina će, prema prethodnoj teoremi imati jedinstveno rešenje $\xi = (y_1, y_2, y_3)^T$, za koje važi $y_i = (\det A)^{-1} \Delta_{yi}$, za $i = 1, 2, 3$. Kako su karakteristične determinante

$$\Delta y_1 = \begin{vmatrix} 1 & 1 & 1 \\ 2 & 1 & 2 \\ 3 & 0 & 2 \end{vmatrix} = 1, \quad \Delta y_2 = \begin{vmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 1 & 3 & 2 \end{vmatrix} = 0, \quad \Delta y_3 = \begin{vmatrix} 1 & 1 & 1 \\ 2 & 1 & 2 \\ 1 & 0 & 3 \end{vmatrix} = 2,$$

to je rešenje sistema $\xi = (3, 0, 2)$ u prstenu $\mathbb{Z}_4$.

Za sistem linearnih jednačina kažemo da je **nemoguć (nesaglasan)** ako nema rešenja, odnosno da je **neodređen** ako ima više rešenja. Cramerovo pravilo može utvrditi da li je sistem jednačina nemoguć ili neodređen u slučaju kada rešavanje sistema posmatramo nad poljem. Naime, u oba slučaja matrica koeficijenata sistema nije inverzibilna tj. njena determinanta je jednaka nuli, pa ukoliko je bar jedna od karakterističnih determinanti različita od nule sistem je nemoguć, a ako su sve karakteristične determinante sistema jednake nuli sistem je neodređen i zahteva detaljnija razmatranja za koja nam Cramerovo pravilo ne obezbeđuje odgovor.

Ako, međutim, rešavanje sistema linearnih jednačina posmatramo nad komutativnim prstenom, videćemo da se u slučaju kada determinanta matrice sistema nije inverzibilna ipak može dogoditi da sistem jednačina ima jedinstveno rešenje, ali takođe i da može imati više rešenja, ili pak biti nemoguć.

Razmotrimo sledeće primere.

Primer 30. Neka je $R = \mathbb{Z}_{21}$ prsten ostataka po modulu 21. Posmatrajmo sistem jednačina $AX = B$ gde je

$$A = \begin{bmatrix} 3 & 2 & 2 \\ 2 & 3 & 2 \\ 2 & 2 & 3 \end{bmatrix} \in M_3(R) \quad \text{i} \quad B = \begin{bmatrix} 6 \\ 4 \\ 4 \end{bmatrix} \in R^3$$

Determinanta $\Delta = \det A = 7$ nije inverzibilna u prstenu $R = \mathbb{Z}_{21}$, odnosno matrica A nije inverzibilna u $M_3(R)$, dok su karakteristične determinante $\Delta_{x_1} = 14$ i $\Delta_{x_2} = \Delta_{x_3} = 0$, pa za rešenja sistema važi

$$\Delta \cdot x_1 = 14, \quad \Delta \cdot x_2 = 0, \quad \Delta \cdot x_3 = 0,$$

odnosno $$7 \cdot x_1 = 14, \quad 7 \cdot x_2 = 0, \quad 7 \cdot x_3 = 0.$$

Rešenja prve jednačine su, na primer, $x_1 = 2; 5; 8;$ itd., dok rešenja druge i treće mogu biti 3; 6; 9; itd. Dakle, ovaj sistem jednačina ima više rešenja u prstenu $\mathbb{Z}_{21}$.

Primer 31. Uzmimo da je u prethodnom primeru kolona slobodnih članova

$$B = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \in R^3 .$$

Ponovo je $\Delta = \det A = 7$, ali karakteristične determinante su $\Delta_{x_1} = 5$ i $\Delta_{x_2} = \Delta_{x_3} = -2 = 19$ u prstenu $\mathbb{Z}_{21}$, pa važi

$$\Delta \cdot x_1 = 5, \quad \Delta \cdot x_2 = 19, \quad \Delta \cdot x_3 = 19,$$

odnosno $$7 \cdot x_1 = 5, \quad 7 \cdot x_2 = 19, \quad 7 \cdot x_3 = 19.$$

Ove jednačine nemaju rešenja u prstenu $\mathbb{Z}_{21}$, odnosno sistem jednačina $AX = B$ sada nema rešenja.

Primer 32: Ukoliko sada isti sistem razmotrimo nad prstenom celih brojeva, videćemo da on ima jedinstveno rešenje. Rešimo, dakle, sistem jednačina $AX = B$ gde je

$$A=\begin{bmatrix}3 & 2 & 2\\ 2 & 3 & 2\\ 2 & 2 & 3\end{bmatrix}\in M_3(R) \quad \text{i} \quad B=\begin{bmatrix}6\\ 4\\ 4\end{bmatrix}\in R^3$$

nad prstenom $R=\mathbb{Z}$.

Determinanta $\Delta=\det A=7$ nije inverzibilna u prstenu celih brojeva, a kako su karakteristične determinante $\Delta_{x_1}= 14$ i $\Delta_{x_2}= \Delta_{x_3}= 0$, za rešenja sistema važi

$$\Delta\cdot x_1 = 14, \quad \Delta\cdot x_2 = 0, \quad \Delta\cdot x_3 = 0,$$

odnosno $$7\cdot x_1 =14, \quad 7\cdot x_2 = 0, \quad 7\cdot x_3 = 0,$$

pa je $\xi = (2, 0, 0)$ rešenje sistema u prstenu $\mathbb{Z}$.

Dakle, ukoliko sistem linearnih jednačina rešavamo nad komutativnim prstenom, u slučaju kada determinanta matrice sistema nije inverzibilna, a pri tom deli sve karakteristične determinante, sistem može imati jedno ili više rešenja. Ukoliko pak, determinanta matrice sistema nije inverzibilna, a pri tome bar jedna od karakterističnih determinanti nije deljiva njome, sistem jednačina neće imati rešenja tj. biće nemoguć.

Naredna teorema daje potreban uslov da sistem od m jednačina sa n nepoznatih $AX = B$, za svaku matricu $A\in M_{m\times n}(R)$ i svaku kolonu $B\in R^m$, ima rešenje.

Teorema 9. Neka je matrica $A\in M_{m\times n}(R)$ takva da sistem jednačina $AX = B$ ima rešenje.
Tada je $I_t(A\,|\,B) = I_t(A)$ za svako $t\in\mathbb{Z}$.

Dokaz: Ako je $m > n$, možemo u dati sistem jednačina $AX = B$ uvesti nove promenljive $x_{n+1}, \dots, x_m$ sa koeficijentima nula i tako preći na sistem $A'X' = B$ gde je

$$\underbrace{\begin{bmatrix}a_{11} & a_{12} & \cdots & a_{1n} & 0 & \cdots & 0\\ \vdots & \vdots & & \vdots & \vdots & & \vdots\\ a_{m1} & a_{m2} & \cdots & a_{mn} & 0 & \cdots & 0\end{bmatrix}}_{A'}\underbrace{\begin{bmatrix}x_1\\ \vdots\\ x_m\end{bmatrix}}_{X'}=\underbrace{\begin{bmatrix}b_1\\ \vdots\\ b_m\end{bmatrix}}_{B}.$$

Tada je $\xi = (y_1, \dots, y_n)^{\mathrm{T}}\in R^n$ rešenje sistema $AX = B$ ako i samo ako je $\xi' = (y_1, \dots, y_n, 0,\dots, 0)^{\mathrm{T}}\in R^m$ rešenje sistema $A'X' = B$. Prema primeru 25, o rangu matrice, važi da je $I_t(A\,|\,\boldsymbol{O}) = I_t(A)$ za svaki $t\in\mathbb{Z}$, tj. važi jednakost ideala $I_t(A) = I_t(A')$, iz čega dalje sledi da je $I_t(A\,|\,B) = I_t(A'\,|\,B)$, za sve $t\in\mathbb{Z}$. Dakle, ako je $I_t(A'\,|\,B) = I_t(A')$, za sve $t\in\mathbb{Z}$, onda je i $I_t(A\,|\,B) = I_t(A)$, za sve $t\in\mathbb{Z}$. Poenta ovoga je da zbog mogućnosti prelaska na sistem $A'X' = B$ ako je potrebno, bez gubitka na opštosti, uvek možemo pretpostavljati da važi $m \le n$.
Pošto i matrica A i proširena matrica $A\,|\,B$ imaju po m vrsta, u slučaju da je $t > \min\{m, n\}$ važi da $I_t(A) = I_t(A\,|\,B) = \{0\}$. Dakle, možemo pretpostaviti da je $1\le t \le m = \min\{m, n\}$. Iz same definicije ideala sledi da je $I_t(A) \subseteq I_t(A\,|\,B)$ za bilo koje t, pa je potrebno samo dokazati da važi i $I_t(A\,|\,B)\subseteq I_t(A)$. Očigledno je, najpre, da je svaki minor reda t matrice $A\,|\,B$ koji ne uključuje kolonu B, sadržan u idealu $I_t(A)$. Stoga ćemo razmatrati samo one minore reda t matrice $A\,|\,B$ koji sadrže kolonu B. Takvi minori su oblika $\Delta(i_1, \dots, i_t; j_1, \dots, j_{t-1}, n+1)$, gde su indeksi
$1 \le i_1 \le \dots \le i_t \le m$ i $1 \le j_1 \le \dots \le j_{t-1} \le m$. Želimo da pokažemo da

$$\Delta(i_1, \dots, i_t; j_1, \dots, j_{t-1}, n+1)\in I_t(A).$$

Fiksirajmo indekse $1 \le i_1 \le \ldots \le i_t \le m$ i $1 \le j_1 \le \ldots \le j_{t-1} \le m$, i razmotrimo minor $\Delta(i_1, \ldots , i_t ; j_1, \ldots , j_{t-1}, n+1) \in I_t(A \,|\, B)$. Neka je $\xi = (x_1, \ldots, x_n)^T \in R^n$ rešenje sistema $AX = B$. Prema primeru 14, o blok-množenju matrica, $A\xi = B$ je proizvod oblika

$$x_1 A_{\downarrow 1} + x_2 A_{\downarrow 2} + \ldots + x_n A_{\downarrow n} = B$$

odnosno, važi da je

$$\Delta(i_1, \ldots , i_t ; j_1, \ldots , j_{t-1}, n+1) = \det \left[\begin{array}{ccc|c} a_{i_1 j_1} & \cdots & a_{i_1 j_{t-1}} & x_1 a_{i_1 1} + \cdots + x_n a_{i_1 n} \\ a_{i_2 j_1} & \cdots & a_{i_2 1 j_{t-1}} & x_1 a_{i_2 1} + \cdots + x_n a_{i_2 n} \\ \vdots & & \vdots & \vdots \\ a_{i_t j_1} & \cdots & a_{i_t j_{t-1}} & x_1 a_{i_t 1} + \cdots + x_n a_{i_t n} \end{array}\right] =$$

$$= \sum_{k=1}^{n} x_k \det \left[\begin{array}{ccc} a_{i_1 j_1} & \cdots & a_{i_1 j_{t-1}}, a_{i_1 k} \\ a_{i_2 j_1} & \cdots & a_{i_2 1 j_{t-1}}, a_{i_2 k} \\ \vdots & & \vdots \\ a_{i_t j_1} & \cdots & a_{i_t j_{t-1}},, a_{i_t k} \end{array}\right] \in I_t(A)$$

■

Dakle, teorema 9 daje potreban uslov da sistem od m jednačina sa n nepoznatih, $AX = B$ ima rešenje za svaku matricu $A \in M_{m\times n}(R)$ i svaku kolonu $B \in R^m$. Naravno, ako su ideali generisani minorima reda t matrica $A \,|\, B$ i A jednaki, $I_t(A \,|\, B) = I_t(A)$, za svako $t \in \mathbb{Z}$, onda su i rangovi tih matrica jednaki, $r(A \,|\, B) = r(A)$. Ukoliko je R polje, tada možemo zaključiti da je $B \in \mathrm{CS}(A)$, što povlači da sistem $AX = B$ ima rešenje, drugim rečima, u slučaju kada je R polje uslov da je $I_t(A \,|\, B) = I_t(A)$, za svako $t \in \mathbb{Z}$, je i dovoljan, dok u opštem slučaju, kada je R komutativan prsten to ne mora biti.

Naredna teorema, međutim, daje dovoljan uslov da sistem jednačina $AX = B$ ima rešenje. Pretpostavićemo da je $B \neq 0$ tj. da je sistem nehomogeni. Takođe, kao što je istaknuto na početku dokaza teoreme 9, uvek možemo napraviti i pretpostavku da je $m \le n$, tj. da broj jednačina nije veći od broja nepoznatih u sistemu. U ovom slučaju ćemo sa $I_m(A \,|\, B)^*$ označavati ideal u prstenu R koji je generisan svim minorima reda m proširene matrice $A \,|\, B$ koji sadrže kolonu B. Dakle, $I_m(A \,|\, B)^*$ je ideal u R koji generiše skup minora oblika

$$\{ \Delta(1, \ldots , m ; j_1, \ldots , j_{m-1}, n+1) \,|\, 1 \le j_1 \le \ldots \le j_{m-1} \le n \}.$$

Teorema 10. Neka je matrica $A \in M_{m\times n}(R)$ takva da je $m \le n$ i da je rang $r(A) = m$ i neka je kolona $B \in R^m$. Ako postoji ideal U u prstenu R i regularan element $z \in R$ takav da je $UI_m(A \,|\, B)^* \subseteq Rz \subseteq UI_m(A)$, onda sistem jednačina $AX = B$ ima rešenje.

Dokaz: Kako je $r(A) = m$, to prema definiciji ranga, znači da je $Ann_R(I_m(A)) = \{0\}$, odnosno da je $I_m(A) \neq \{0\}$, tj. da postoji bar jedan ne-nula minor reda m matrice A. Pretpostavimo da je $\Delta(1, \ldots , m ; j_1, \ldots , j_m)$ taj ne-nula minor matrice A, gde je $1 \le j_1 \le \ldots \le j_m \le n$. Posmatrajmo sledeću $m\times m$ podmatricu matrice A

$$\overline{A} = \left[\begin{array}{ccc} a_{1 j_1} & \cdots & a_{1 j_m} \\ \vdots & & \vdots \\ a_{m j_1} & \cdots & a_{m j_m} \end{array}\right]$$

Determinanta matrice $\overline{A}$ je tada upravo $\det \overline{A} = \Delta \neq 0$ i važi da je

$$\Delta \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} = \det \overline{A} \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} = \overline{A}\, \mathrm{adj} \overline{A} \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} \qquad (1)$$

Kako je

$$\mathrm{adj}\ \overline{A} \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} = \begin{bmatrix} \sum_{j=1}^{m} b_j \overline{A}_{j1} \\ \vdots \\ \sum_{j=1}^{m} b_j \overline{A}_{jm} \end{bmatrix} \qquad (2)$$

gde su $\overline{A}_{ji}$ kofaktori matrice $\overline{A}$. Ako uvedemo oznaku

$$\begin{bmatrix} c_1 \\ \vdots \\ c_m \end{bmatrix} = \begin{bmatrix} \sum_{j=1}^{m} b_j \overline{A}_{j1} \\ \vdots \\ \sum_{j=1}^{m} b_j \overline{A}_{jm} \end{bmatrix} \in R^m$$

onda važi da je

$$c_i = \sum_{j=1}^{m} b_j \overline{A}_{j\,i} = \det \begin{bmatrix} a_{1j_1} & \cdots & b_1 & \cdots & a_{1j_m} \\ \vdots & & & & \vdots \\ a_{mj_1} & \cdots & b_m & \cdots & a_{mj_m} \end{bmatrix} \in I_m \left(A \mid B \right)^*, \text{ za sve } i = 1,\ldots,m\,.$$

Sada, na osnovu jednakosti (1) i (2) sledi da je

$$\Delta \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} = \begin{bmatrix} a_{1j_1} & \cdots & a_{1j_m} \\ \vdots & & \vdots \\ a_{mj_1} & \cdots & a_{mj_m} \end{bmatrix} \begin{bmatrix} c_1 \\ \vdots \\ c_m \end{bmatrix},$$

drugim rečima, da je

$$\Delta\, b_i = \sum_{u=1}^{m} a_{i\,j_u} c_u\,, \text{ za sve } i = 1, \ldots, m.$$

Uvedimo oznake $y_1, \ldots, y_n$ za skalare $y_v \in I_m(A/B)^*$, za sve $v = 1, .., n$, na sledeći način

$$y_v = \begin{cases} 0\,, \text{ ako je } v \in \{1,\ldots,n\} \setminus \{j_1,\ldots,j_m\} \\ c_i\,, \text{ako je } v = j_i \text{ za } i = 1,\ldots,m \end{cases}$$

Primetimo da je tada takođe važi i

$$\sum_{v=1}^{n} a_{iv}\, y_v = a_{i\,j_1} y_1 + \ldots + a_{i\,j_m} y_m = a_{i\,j_1} c_1 + \ldots + a_{i\,j_m} c_m = \Delta b_i\,, \text{ za sve } i = 1,\ldots, m\,.$$

Sada smo upravo pokazali da je $\Delta b_i = \sum_{v=1}^{n} a_{iv} y_v$, za sve $i = 1, \ldots, m$,

gde su skalari $y_1, \ldots, y_n \in I_m(A/B)^*$. Ovo se sumiranje može izvršiti za svaki ne-nula minor reda m matrice A. Uvedimo oznake $\Delta_1, \ldots, \Delta_p$ za takve, ne-nula minore reda m matrice A. Tada za svaki $k = 1, \ldots, p$ postoje skalari $\{ y_{kv} \in R \mid v = 1,\ldots,n \} \subseteq I_m(A/B)^*$ takvi da je

$$\Delta_k b_i = \sum_{v=1}^{n} a_{iv} y_{kv}, \text{ za sve } i = 1,\ldots, m\,. \qquad (3)$$

Kako je po pretpostavci $UI_m(A\,|\,B)^* \subseteq Rz \subseteq UI_m(A)$, i kako minori $\Delta_1, ..., \Delta_p$ generišu ideal $I_m(A)$, to sledi da je

$$z = \sum_{k=1}^{p} q_k \Delta_k, \text{ za neke } q_1, ..., q_p \in U .$$

Sada, na osnovu jednakosti (3), sledi da

$$\sum_{k=1}^{p}\sum_{v=1}^{n} a_{iv} q_k y_{kv} = \sum_{k=1}^{p} q_k \left(\sum_{v=1}^{n} a_{iv} y_{kv}\right) = \sum_{k=1}^{p} q_k \Delta_k b_i = z b_i, \text{ za sve } i = 1, ..., m$$

pa je stoga

$$\sum_{v=1}^{n} a_{iv} \left(\sum_{k=1}^{p} q_k y_{kv}\right) = z b_i, \text{ za sve } i = 1, ..., m . \qquad (4)$$

Kako je

$$\sum_{k=1}^{p} q_k y_{kv} \in UI_m(A\,|\,B)^* \subseteq Rz \quad \text{za svaki } v = 1, ..., n ,$$

to važi da je $\sum_{k=1}^{p} q_k y_{kv} = r_v z$, za neki $r_v \in R$. z jednakosti (4) sada sledi da je

$$z \cdot \left(\sum_{v=1}^{n} a_{iv} r_v\right) = z b_i \quad \text{za sve} \quad i = 1, ..., m.$$

Pošto je element z regularan u prstenu R, to znači da je

$$\sum_{v=1}^{n} a_{iv} r_v = b_i , \text{ za sve } i = 1, ..., m$$

pa je otuda $\xi = (r_1, ..., r_n)^T \in R^n$ rešenje sistema jednačina $AX = B$.

■

Pretpostavimo da je $I_m(A) = R$. Tada je $r(A) = m$, pa za svaku kolonu $B \in R^m$ važi da je $RI_m(A\,|\,B)^* \subseteq R \cdot 1 \subseteq RI_m(A)$, a kako je 1 regularan element prstena R, to na osnovu teoreme 10 sledi da sistem $AX = B$ ima rešenje. Time smo dokazali sledeće tvrđenje.

Posledica 9. Neka je $A \in M_{m\times n}(R)$ matrica takva da je $I_m(A) = R$. Tada za svaku kolonu $B \in R^m$ sistem jednačina $AX = B$ ima rešenje.

■

Tvrđenja u ovom poglavlju se mogu primeniti na razmatranja koja se odnose na linearna preslikavanjima među slobodnim R-modulima.

Neka je $A \in M_{m\times n}(R)$. Matrica A indukuje jedan homomorfizam R-modula R^n u modul R^m, $\mu_A: R^n \to R^m$, dat sa $\mu_A(\xi) = A\xi$. McCoyova teorema 6 i upravo dokazana posledica 9 nas dovode do sledeće teoreme.

Teorema 11. Neka je $A \in M_{m\times n}(R)$ i neka je μ_A: $R^n \to R^m$ homomorfizam R-modula dat sa $\mu_A(\xi) = A\xi$. Tada važe sledeća tvrđenja:

1) Neka je $n \geq m$. Preslikavanje μ_A je surjektivno ako i samo ako je ideal $I_m(A) = R$.
2) Neka je $n \leq m$. Preslikavanje μ_A je injektivno ako i samo ako je $Ann_R(I_n(A)) = \{0\}$.

Dokaz: Najpre, ako je $n < m$, preslikavanje μ_A ne može biti surjektivno prema teoremi 7. Ako je, s druge strane, $n > m$, preslikavanje μ_A iz istog razloga ne može biti injektivno. Razmotrimo zato tvrđenja 1 i 2.

1) Pretpostavimo da je $n \geq m$. Ako je $I_m(A) = R$ onda na osnovu posledice 9 sledi da sistem jednačina $AX = B$ ima rešenje za svako $B \in R^m$. Ovo upravo znači da je preslikavanje μ_A surjektivno, tj. da je modul R^m slika homomorfizma μ_A.
Pretpostavimo obratno, da je preslikavanje μ_A surjektivno. Označimo sa $\varepsilon = \{\varepsilon_1, ..., \varepsilon_m\}$ kanonsku bazu modula R^m, gde je $\varepsilon_1 = (1, 0, ..., 0)^T$, $\varepsilon_2 = (0, 1, ..., 0)^T$, ..., $\varepsilon_m = (0, 0, ..., 1)^T$. Tada sistem jednačina $AX = \varepsilon_1$ ima rešenje jer je μ_A surjektivno. Naime, prema teoremi 9 sledi da je $I_m(A) = I_m(A \mid \varepsilon_1)$. Jednačina $AX = \varepsilon_2$ takođe ima rešenje $\xi \in R^n$ jer je μ_A surjektivno. Tada možemo zapisati da je $(A \mid \varepsilon_1)Y = \varepsilon_2$ za matricu $Y = \begin{pmatrix} \xi \\ \boldsymbol{O} \end{pmatrix}$. To konkretno znači da jednačina $(A \mid \varepsilon_1)X = \varepsilon_2$ ima rešenje, što opet prema teoremi 9 znači da je $I_m(A \mid \varepsilon_1) = I_m(A \mid \varepsilon_1 \mid \varepsilon_2)$. Nastavimo li dalje na isti način, dolazimo do zaključka da je
$$I_m(A) = I_m(A \mid \varepsilon_1) = I_m(A \mid \varepsilon_1 \mid ... \mid \varepsilon_m) = R.$$

2) Preslikavanje μ_A neće biti injektivno onda i samo onda kada sistem jednačina $AX = 0$ ima netrivijalno rešenje $\xi \in R^n$. Prema McCoyovoj teoremi, homogeni sistem $AX = 0$ ima netrivijalno rešenje onda i samo onda kada je rang matrice koeficijenata $r(A) < n$, što po definiciji znači da je anulator $Ann_R(I_n(A)) \neq \{0\}$.

■

Literatura

1. William C. Brown, *Matrices over commutative rings*, Marcel Dekker, Inc., Michigan State University, 1993.
2. Gojko Kalajdžić, *Linearna algebra*, MAM Vesta, Matematički fakultet, Beograd, 1998.
3. Gojko Kalajdžić, *Algebra*, MAM Vesta, Matematički fakultet, Beograd, 1998.
4. Joseph J. Rotman, *Advanced Modern Algebra*, Pearson Education, Inc., American Mathematical Society, 2002
5. Đuro Kurepa, *Viša algebra II*, Beograd, 1971
6. http://www.mathreference.com
7. http://en.wikipedia.org
8. http://books.google.com
9. http://www.springerlink.com