Математички факултет
Универзитет у Београду

Мастер рад

Матрице над $\mathbb{Z}_n$

Студент: Кристина Поповић 1125/2016
Ментор: проф. др Зоран Петровић

Београд,
2019.

Чланови комисије:
1. проф. др Зоран Петровић
2. проф. др Александар Липковски
3. др Марко Радовановић

Садржај

Глава 1

Увод

Прво поглавље представља основне елементе потребне за заснивање матрица над $\mathbb{Z}_n$. Алгебарски појмови попут прстена и поља, инвертибилних елемената, регуларних елемената, делитеља нуле, нилпотентних елемената, идемпотентних елемената, идеала, као и везе између истих, стварају базу над којом ће теорија матрица имати пуног смисла.

У другом поглављу изложена су основна својства матрица, са акцентом на оне које припадају комутативном прстену са јединицом $\mathbb{Z}_n$. Аналогно прстену $\mathbb{Z}_n$, и у скупу матрица $M_{m\times k}(\mathbb{Z}_n)$, обрађене су инвертибилне матрице, нилпотентне матрице,...

У наредном поглављу описане су детерминанте, њихова својства, али и веза између детерминанте матрице над прстеном $\mathbb{Z}_n$, као и елемената датог прстена $\mathbb{Z}_n$.

У поглављу о рангу матрице дате су теореме које помажу да се одреди ранг матрице из $M_{m\times k}(\mathbb{Z}_n)$, који се разликује од ранга матрице над пољем (рађено на часовима Линеарне алгебре). Лакоћа одређивања ранга заснива се на појму анулатора идеала неке матрице.

С обзиром да су елементи прстена $\mathbb{Z}_n$, елементи добијени као остаци при дељењу са n, неизоставне су и конгруенције и Кинеска теорема о остацима, док је решавање система једначина у прстену $\mathbb{Z}_n$ природни наставак теме.

Идеја овог рада јесте представити што већи број примера, и помоћу њих створити што јаснију слику о повезаности свих алгебарских појмова који се у раду обрађују.

Велику захвалност дугујем свом ментору за све смернице и идеје, као и за сву помоћ коју ми је указао у току израде рада.

Глава 2

$\mathbb{Z}_n$

2.1 Прстени $\mathbb{Z}_n$

На самом почетку дефинисаћемо алгебарску структуру прстен, а онда прећи на конкретно објашњавање прстена $\mathbb{Z}_n$.

Дефиниција 1. Алгебарска структура која подразумева постојање скупа S и на њему дефинисане операције $+$ и $\cdot$ тако да важи:

- $(S, +)$ је Абелова група,
- $(S, \cdot)$ је моноид,
- за $x, y, z \in S$, $x \cdot (y + z) = x \cdot y + x \cdot z$ и $(y + z) \cdot x = y \cdot x + z \cdot x$
  закон дистрибутивности множења у односу на сабирање,

назива се прстен. Неутрал за сабирање (операцију $+$ у прстену) у прстену S означавамо са 0 и зовемо нулом прстена S, док неутрал за множење (операцију $\cdot$ у прстену) означавамо са 1 и зовемо јединицом прстена S. Ако притом важи и $0 \neq 1$, такав прстен зовемо прстен са јединицом. Дати услов нам користи да тривијални нула прстен $\{0\}$ не зовемо прстен са јединицом.

Дефиниција 2. Прстен у коме важи $\forall(a, b)\ a \cdot b = b \cdot a$ назива се комутативни прстен.

Пример 1. $(\mathbb{Z}, +, \cdot)$ је прстен на основу следећих чињеница:

- $(\mathbb{Z}, +)$ је Абелова група у којој је неутрал елемент 0, а за елемент $x \in \mathbb{Z}$ инверз је $-x \in \mathbb{Z}$.
- $(\mathbb{Z}, \cdot)$ је моноид у коме је неутрал елемент 1.
- За $x, y, z \in \mathbb{Z}$ важи $x \cdot (y + z) = x \cdot y + x \cdot z$ и $(y + z) \cdot x = y \cdot x + z \cdot x$.

Пример 2. Нека је $n \geq 2$. Скуп

$$\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$$

је скуп свих остатака при дељењу бројем n.

Свака од алгебарских структура $(\mathbb{Z}_n, +_n)$ је Абелова група, $(\mathbb{Z}_n, \cdot_n)$ моноид и важи закон дистрибутивности, па је самим тим $(\mathbb{Z}_n, +_n, \cdot_n)$ и прстен.

Дефиниција 3. Елемент a је инвертибилан у прстену S ако постоји $b \in S$ тако да је $a \cdot b = b \cdot a = 1$. Елемент b је јединствено одређен и означава се са a^{-1}. Скуп свих инвертибилних елемената прстена S означава се са $U(S)$.

Дефиниција 4. Елемент a прстена S је леви (десни) делитељ нуле уколико постоји елемент $b \neq 0$ за који је $a \cdot b = 0$ ($b \cdot a = 0$). Уколико је и $a \neq 0$, онда је a прави делитељ нуле. Скуп свих левих (десних) делитеља нуле прстена S означава се са $Z_L(S)$ ($Z_D(S)$). Ако је прстен комутативан онда говоримо само о делитељима нуле, и такав скуп се означава са $Z(S)$.

Пример 3. У прстену $\mathbb{Z}_{12}$ скуп инвертибилних елемената је $U(\mathbb{Z}_{12}) = \{1, 5, 7, 11\}$ јер је:

$$1 \cdot 1 \equiv 1 \pmod{12}$$

$$5 \cdot 5 \equiv 1 \pmod{12}$$

$$7 \cdot 7 \equiv 1 \pmod{12}$$

$$11 \cdot 11 \equiv 1 \pmod{12}$$

У истом прстену, делитељи нуле припадају скупу $Z(\mathbb{Z}_{12}) = \{0, 2, 3, 4, 6, 8, 9, 10\}$ јер је:

$$0 \cdot 2 \equiv 0 \pmod{12}$$

$$2 \cdot 6 \equiv 0 \pmod{12}$$

$$3 \cdot 4 \equiv 0 \pmod{12}$$

$$4 \cdot 3 \equiv 0 \pmod{12}$$

$$6 \cdot 2 \equiv 0 \pmod{12}$$

$$8 \cdot 3 \equiv 0 \pmod{12}$$

$$9 \cdot 4 \equiv 0 \pmod{12}$$

$$10 \cdot 6 \equiv 0 \pmod{12}$$

Пример 4. У прстену $(\mathbb{Z}_6, +_6, \cdot_6)$ важи $2 \cdot 3 = 0$ и $2, 3 \neq 0$, па су бројеви 2 и 3 прави делитељи нуле.

Напомена 1. У прстену $\mathbb{Z}_n$ важи

$$\mathbb{Z}_n = U(\mathbb{Z}_n) \sqcup Z(\mathbb{Z}_n).$$

Дефиниција 5. Елемент a прстена S је регуларан слева (здесна) уколико за све $x, y \in S$ важи: ако је $a \cdot x = a \cdot y$ ($x \cdot a = y \cdot a$), онда је $x = y$.

Напомена 2. Сваки инвертибилан елемент истовремено је и регуларан. Међутим, није сваки регуларан уједно и инвертибилан. Пример за то је прстен $\mathbb{Z}$ у коме је сваки различит од нуле регуларан, али само 1 и -1 јесу инвертибилни.

Дефиниција 6. Елемент a прстена $\mathbb{Z}_n$ је нилпотентан ако постоји $k \in \mathbb{N},\ k > 1$ тако да важи $a^k = 0$. Скуп свих нилпотентних елемената прстена $\mathbb{Z}_n$ означава се са $\mathrm{Nil}(\mathbb{Z}_n)$.

Пример 5. Одредимо нилпотентне елементе у прстену $\mathbb{Z}_6$. Јединице овог прстена су 1 и 5. Елемент 0 јесте нилпотентан. Елемент 2 није јер је модул сваког његовог степена једнак броју 2 или броју 4. Елемент 3 није јер је модул сваког његовог степена 3. Ни елемент 4 није нилпотентан јер је модул степена као и код броја 2 једнак броју 2 или броју 4. Дакле, $\mathrm{Nil}(\mathbb{Z}_n) = \{0\}$.

Постоји наравно, и *лакши* начин за одређивање нилпотентних елемената, и њега ћемо представити у делу који говори о *идеалима*.

Дефиниција 7. Елемент a прстена $\mathbb{Z}_n$ је идемпотентан ако важи $a \cdot a = a$. Скуп свих идемпотентних елемената прстена $\mathbb{Z}_n$ означава се са $\mathrm{Idem}(\mathbb{Z}_n)$.

Напомена 3. Тривијални идемпотентни елементи у сваком $\mathbb{Z}_n$ прстену су 0 и 1 .

Пример 6. Идемпотентни елементи у прстену $\mathbb{Z}_6$ су $\mathrm{Idem}(\mathbb{Z}_6) = \{0, 1, 3, 4\}$ јер је $3 \cdot 3 \equiv 3 \pmod 6,\ 4 \cdot 4 \equiv 3 \pmod 6$.

2.2 Поља $\mathbb{Z}_n$

Као што смо видели у претходном делу, $\mathbb{Z}_n$ је пример прстена. Међутим, уколико бисмо се бавили питањем постојања инверзног елемента у сваком од поменутих прстена, видели бисмо да се ситуација разликује.

Пример 7.

У $\mathbb{Z}_2 = \{0, 1\}$, за елемент 1, инверз је 1, тј. $1 \cdot 1 = 1$.

У $\mathbb{Z}_3 = \{0, 1, 2\}$, за елемент 1 инверз је 1, тј. $1 \cdot 1 = 1$, за елемент 2 инверз је 2, тј. $2 \cdot 2 = 1$.

У $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, елемент 2 нема инверз, што можемо проверити јер је $2 \cdot 1 \neq 1,\ 2 \cdot 2 \neq 1,\ 2 \cdot 3 \neq 1$.

За прстен $\mathbb{Z}_6$ можемо искористити Кејлијеву таблицу.

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Из таблице закључујемо да једино елементи 1 и 5 имају инверзне елементе у $\mathbb{Z}_6$.

Другим речима, с обзиром да у $\mathbb{Z}_4,\ \mathbb{Z}_6$ немају сви елементи инверзе, и сами $(\mathbb{Z}_4, \cdot_4),\ (\mathbb{Z}_6, \cdot_6)$ су највише моноиди, а $(\mathbb{Z}_4, +_4, \cdot_4),\ (\mathbb{Z}_6, +_6, \cdot_6)$ прстени.

Дефиниција 8. Поље је комутативни прстен са јединицом у коме сваки ненула елемент има инверз.

Теорема 1. За елементе поља a и b важи:

$$a \cdot b = 0 \Rightarrow a = 0 \vee b = 0.$$

Доказ. Претпоставимо да је $a \cdot b = 0$. Ако $a \neq 0$, тада a има инверз a^{-1} па је

$$a \cdot b = 0 \Rightarrow a^{-1}ab = a^{-1} \cdot 0 \Rightarrow 1 \cdot b = 0 \Rightarrow b = 0.$$

□

Пример 8. Приметимо да претходна теорема не важи у општем случају у прстену. Рецимо, у $\mathbb{Z}_4$ важи $2 \cdot 2 = 0$, али $2 \neq 0$.

У пољу такође важи закон "скраћивања":

Теорема 2. За елементе поља $a, b, c,\ a \neq 0$ важи:

$$a \cdot b = a \cdot c \Rightarrow b = c.$$

Доказ. Претпоставимо да је $a \neq 0$. Тада је

$$a \cdot b = a \cdot c \Rightarrow a^{-1}ab = a^{-1} \cdot a \cdot c \Rightarrow 1 \cdot b = 1 \cdot c \Rightarrow b = c.$$

□

Пример 9. Претходна теорема не важи у општем случају у прстену. На пример, у $\mathbb{Z}_4$ важи $2 \cdot 2 = 2 \cdot 0$, али $2 \neq 0$.

Следећа теорема покрива случај када сваки ненула елемент има инверз, као што је нпр. у $\mathbb{Z}_2$ и $\mathbb{Z}_3$.

Теорема 3. Прстен $(\mathbb{Z}_n, +_n, \cdot_n)$ је поље ако и само ако је n прост број.

Доказ. Претпоставимо да је p прост број. Како бисмо доказали да је $\mathbb{Z}_p$ поље, узмимо $m \in \{0, 1, ..., p-1\}$ и претпоставимо да m нема инверз у $\mathbb{Z}_p$.

Тада ниједан од бројева p облика

$$0 \cdot m, 1 \cdot m, 2 \cdot m, ..., (p-1) \cdot m$$

не може бити једнак 1, тако да се међу задатим бројевима налазе бар два који су једнаки у $\mathbb{Z}_p$. Дакле, важи

$$i \cdot m \equiv j \cdot m \pmod{p} \vee (i-j) \cdot m \equiv 0 \pmod{p}$$

за неке $i, j,\ 0 < i - j < p$. Како је p прост, један од бројева $i - j$ или m мора имати као фактор p, па је једина могућност $m = 0$.

Из овога следи да је 0 једини елемент који нема инверз, па је $\mathbb{Z}_p$ дакле поље.

Да бисмо комплетирали доказ, покажимо да ако n није прост, тада $\mathbb{Z}_n$ није поље.

Ако је $n \geq 2$ и није прост, тада је $n = qr$ за неке $q, r \geq 2$. Тада имамо два ненула елемента q и r чији је производ нула у $\mathbb{Z}_n$. Како то није могуће у пољу , одатле следи да $\mathbb{Z}_n$ није поље. □

2.3 Идеали у $\mathbb{Z}_n$

Дефиниција 9. Нека је $\mathbb{Z}_n$ прстен и I непразан подскуп од $\mathbb{Z}_n$. Тада је I идеал у $\mathbb{Z}_n$ уколико:

1. за све $x, y \in I : x +_n y \in I$;
2. за све $a \in \mathbb{Z}_n$ и $x \in I : a \cdot_n x \in I$.

Ознака $I \lhd \mathbb{Z}_n$ означава да је I идеал у $\mathbb{Z}_n$.

Пример 10. Нека је $\mathbb{Z}_n$ прстен и $I \lhd \mathbb{Z}_n$. Идеали $I = \{0\}$ и $I = Z_n$ зову се тривијални идеали. У случају да је $I \neq Z_n$ идеал је прави, а ако је $I \neq \{0\}$ онда је ненула.

Пример 11. Нека је $\mathbb{Z}_n$ поље и $I \lhd \mathbb{Z}_n$. Тада је $I = \{0\}$ или $I = \mathbb{Z}_n$.

Претпоставимо да је I идеал у $\mathbb{Z}_n$ и да је $I \neq \{0\}$. То значи да идеал I садржи неки елемент $x \neq 0$. Уколико је a ма који елемент из $\mathbb{Z}_n$, одатле следи да и a припада идеалу I. Како је I идеал и $x \neq 0$, тада постоји x^{-1}, па и $(ax^{-1}) \cdot x$ мора припадати идеалу I, а јасно је да је тај елемент једнак елементу a.

Са идеалима се могу вршити операције сабирања и множења као и са елементима.

Дефиниција 10. Нека су I и J идеали прстена $\mathbb{Z}_n$.

1. $I + J := \{x +_n y : x \in I, y \in J\}$;
2. $I \cdot J := \{x_1y_1 +_n \cdots +_n x_ny_n : x_i \in I$ за све $i = 1, ..., n, y_j \in J$ за све $j = 1, ..., n$ и све $n \geqslant 1\}$.

Дефиниција 11. Ако је A комутативан прстен и $a \in A$ произвољан елемент, онда је

$$\langle a \rangle := \{r \cdot a \ : \ r \in A\},$$

идеал. Овај идеал се назива **главни идеал** генерисан елементом a.

Прстен у коме је сваки идеал главни назива се главноидеалски прстен.

Напомена 4. Сваки идеал у $\mathbb{Z}$ је облика $\langle m \rangle$ за неки природан број m.

Напомена 5. Идеал $\langle m \rangle$ означава се и са $m\mathbb{Z}$ (скуп свих целобројних умножака броја m).

Пример 12. Неки од идеала у $\mathbb{Z}$ су: $\langle 0 \rangle = \{0\}$, $\langle 1 \rangle = \langle -1 \rangle = \mathbb{Z}$, $\langle 2 \rangle = \langle -2 \rangle = 2\mathbb{Z}$

Дефиниција 12. Нека су $(A, +, \cdot)$ и $(B, +', \cdot')$ два комутативна прстена са јединицом. Функција $f : A \to B$ је хомоморфизам прстена уколико је $f(1_A) = 1_B$ и уколико за све $x, y \in A$ важи:

$$f(x + y) = f(x) +' f(y) \text{ и } f(x \cdot y) = f(x) \cdot' f(y).$$

Дефиниција 13. Нека је $f : A \to B$ хомоморфизам комутативних прстена са јединицом. Језгро хомоморфизма f, у ознаци $\mathrm{Ker}(f)$ дефинише се са:

$$\mathrm{Ker}(f) = \{x \in A : f(x) = 0_B\}.$$

Дефиниција 14. Слика хомоморфизма $f : A \to B$, у ознаци $\mathrm{Im}(f)$, дефинише се са:

$$\mathrm{Im}(f) = \{y \in B : (\exists x \in A)\ y = f(x)\}.$$

Теорема 4.

1. Прстен $\mathbb{Z}$ је главноидеалски.
2. Хомоморфна слика главноидеалског прстена је такође главноидеалски прстен.

3. $\mathbb{Z}_n$ је главноидеалски прстен за свако $n > 0$.

Доказ.

1. Нека је $I \subseteq \mathbb{Z}$ идеал у $\mathbb{Z}$. Тада је $\langle 1\rangle = \mathbb{Z}$ и $\langle 0\rangle = \{0\}$, па можемо претпоставити да је I прави идеал. Како је I прави идеал, тада он садржи бар један позитиван цео број. Нека је $a \in I$ најмањи позитиван цео број у I, и тврдимо да је $I = \langle a\rangle$.

   Како је $a \in I$, довољно је показати да $I \subseteq \langle a\rangle$. Нека је $x \in I - \{0\}$. Можемо наћи целе бројеве q и r тако да је $x = qa + r$ и $0 \leqslant r < a$. Како је $a \in I$ и I идеал, онда $qa \in I$ и $r = x - qa \in I$. Дакле, за одабрано a је $r = 0$. Стога $\forall x \in I$, $x = qa$ за неко $q \in \mathbb{Z}$. Тако је $I \subseteq \langle a\rangle$.

2. Нека су $R, R^{'}$ комутативни прстени, тако да је R главноидеалски, и $f : R \to R^{'}$ прстен хомоморфизма тако да $R^{'} = f(R)$. Тада је и $R^{'}$ главноидеалски прстен.

   Нека је $I^{'}$ идеал у $R^{'}$. Тада је $I = f^{-1}(I^{'})$ идеал у R, и $\exists a \in R$ тако да је $I = \langle a\rangle$. Знамо да је $I = f(f^{-1}(I^{'})) = f(\langle a\rangle)$.

   Треба доказати $\langle f(a)\rangle = f(\langle a\rangle)$.

   $\langle f(a)\rangle = \{r^{'}f(a) : r^{'} \in R^{'}\} \overset{f \text{ је „на”}}{=} \{f(r)f(a) : r \in R\} = \{f(ra) : r \in R\} = f(\langle a\rangle)$.

3. Како је $\mathbb{Z}$ главноидеалски прстен и канонски хомоморфизам $f : \mathbb{Z} \to \mathbb{Z}_n$ тј. $f(m) = \overline{m} \in \mathbb{Z}_n$ епиморфизам, из тачке 2 следи да је $\mathbb{Z}_n$ главноидеалски прстен. □

Пример 13. За прстен $\mathbb{Z}_n$ и елемент $u \in U(\mathbb{Z}_n)$, важи $\langle u\rangle = Z_n$.

Пример 14. Идеали у $\mathbb{Z}_8$ су $\langle 0\rangle = 0$, $\langle 1\rangle = \{0,1,2,3,4,5,6,7\} = \mathbb{Z}_8$, $\langle 2\rangle = \{0,2,4,6\}$, $\langle 3\rangle = \{0,1,2,3,4,5,6,7\} = \mathbb{Z}_8$, $\langle 4\rangle = \{0,4\}$, $\langle 5\rangle = \{0,1,2,3,4,5,6,7\} = \mathbb{Z}_8$, $\langle 6\rangle = \{0,2,4,6\}$, $\langle 7\rangle = \{0,1,2,3,4,5,6,7\} = \mathbb{Z}_8$.

Пример 15. Идеали у $\mathbb{Z}_5$ су $\langle 0\rangle = 0$, $\langle 1\rangle = \{0,1,2,3,4,5\} = \mathbb{Z}_5$, $\langle 2\rangle = \{0,2,4,1,3\} = \mathbb{Z}_5$, $\langle 3\rangle = \{0,3,1,4,2\} = \mathbb{Z}_5$, $\langle 4\rangle = \{0,4,3,2,1\} = \mathbb{Z}_5$.

Као што смо показали у једном од претходних тврђења, како је $\mathbb{Z}_5$ поље, једини идеали су $I = \{0\}$ и $I = Z_5$.

Пример 16. У прстену $\mathbb{Z}_{12}$ сваки елемент је или делитељ нуле или инвертибилан. Приметимо да сваки инвертибилни генерише цео прстен, док делитељи нуле генеришу остале идеале. Елемент из овог прстена је делитељ нуле ако и само ако га дели број 2 или број 3.

Како је $5 \in U(\mathbb{Z}_{12})$ и $10 = 5 \cdot_{12} 2$, и број 5 инвертибилан у прстену $\mathbb{Z}_{12}$, тада следи да је $\langle 10\rangle = \langle 2\rangle$. На исти начин је и $\langle 8\rangle = \langle 4\rangle$ јер је $8 = 4 \cdot_{12} 5$, као и $\langle 9\rangle = \langle 3\rangle$ због $9 = 11 \cdot_{12} 3$, итд.

Са друге стране, $\langle 2\rangle \neq \langle 4\rangle$. Ако претпоставимо да је $m \in \mathbb{Z}_{12}$ и $2 = 4 \cdot_{12} m$, тада би постојао цео број q тако да је $2 = 4m + 12q$. Дељењем са 2 добија се једнакост $1 = 2m + 6q$ за коју не постоје цели бројеви m и q за које ће иста бити тачна. Међутим, с обзиром да је $4 = 2m + 12q$ и после дељења са 2, $2 = m + 6q$, постоје цели бројеви m и q за које је задовољена једнакост, па важи $\langle 4\rangle \subset \langle 2\rangle$. На исти начин, важи $\langle 6\rangle \subset \langle 3\rangle$ јер постоје m и q за које је $6 = 3m + 12q$ тачно. Провером осталих случајева уверавамо се да су различити идеали прстена $\mathbb{Z}_{12}$ заправо

$$\langle 0\rangle, \langle 2\rangle, \langle 3\rangle, \langle 4\rangle, \langle 6\rangle, Z_{12}.$$

Када су у питању нилпотентни елементи прстена $\mathbb{Z}_{12}$, постоји једна важна особина која их повезује са идеалима. Наиме, скуп свих нилпотентних елемената прстена $\mathbb{Z}_n$ јесте један идеал, чији је генератор производ свих различитих простих фактора броја n.

Пример 17. Одредити све нилпотентне елементе прстена:

- $\mathbb{Z}_8$

  Број 8 се може факторисати као $8 = 2^3$, па ће број 2 бити генератор свих нилпотентних елемената. Дакле,

  $$I = \langle 2\rangle = \{0, 2, 4, 6\} = \mathrm{Nil}(\mathbb{Z}_8).$$

- $\mathbb{Z}_{12}$

  Број 12 се може факторисати као $12 = 2^2 \cdot 3$, па је НЗД$(2, 3) = 1$, па ће број 6 бити генератор свих нилпотентних елемената. Дакле,

  $$I = \langle 6\rangle = \{0, 6\} = \mathrm{Nil}(\mathbb{Z}_{12}).$$

- $\mathbb{Z}_{20}$

  Број 20 се може факторисати као $20 = 2^2 \cdot 5$, па је НЗД$(2, 5) = 1$, па ће број 10 бити генератор свих нилпотентних елемената. Дакле,

  $$I = \langle 10\rangle = \{0, 10\} = \mathrm{Nil}(\mathbb{Z}_{20}).$$

- $\mathbb{Z}_{30}$

  Број 30 се може факторисати као $30 = 2 \cdot 3 \cdot 5$, па је НЗД$(2, 3, 5) = 1$, па ће број 30 бити генератор свих нилпотентних елемената. Дакле,

  $$I = \langle 30\rangle = \{0\} = \mathrm{Nil}(\mathbb{Z}_{30}).$$

- $\mathbb{Z}_{36}$

  Број 36 се може факторисати као $36 = 2^2 \cdot 3^2$, па је НЗД$(2, 3) = 1$, па ће број 6 бити генератор свих нилпотентних елемената. Дакле,

  $$I = \langle 6\rangle = \{0, 6, 12, 18, 24, 30\} = \mathrm{Nil}(\mathbb{Z}_{36}).$$

Глава 3

Матрице

Дефиниција 15. Матрица A формата $m \times k$ над $\mathbb{Z}_n$ је функција која пресликава Декартов производ $\{1, 2, ..., m\} \times \{1, 2, ..., k\}$ у $\mathbb{Z}_n$.

Уређени пар (i, j) пресликава се у елемент матрице a_{ij}. Матрица A има m врста и k колона, па елемент a_{ij} припада i-тој врсти и j-тој колони. Матрица $A \in M_{m\times k}(\mathbb{Z}_n)$ представља се као:

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mk} \end{bmatrix}$$

или

$$A = [a_{ij}]_{m\times k}$$

где $M_{m\times k}(\mathbb{Z}_n)$ означава скуп свих матрица формата $m \times k$.

Дефиниција 16. Матрица у којој је број колона и број врста једнак, тј. $m = k$ назива се квадратном матрицом реда k.

Скуп свих квадратних матрица k-тог реда означавамо са $M_k(\mathbb{Z}_n)$.

Дефиниција 17. Матрица чији су сви елементи једнаки нули назива се нула матрица.

Дефиниција 18. Под главном дијагоналом квадратне матрице подразумевамо уређену k-торку $(a_{11}, a_{22}, ..., a_{kk})$.

Дефиниција 19. За квадратну матрицу кажемо да је дијагонална ако су сви њени елементи ван главне дијагонале једнаки 0.

$$D = \begin{bmatrix} d_1 & & & 0 \\ & d_2 & & \\ & & \ddots & \\ 0 & & & d_n \end{bmatrix}$$

Међутим, дијагонална матрица не мора бити квадратна.

Дефиниција 20. Нека је $D \in M_{m\times k}(\mathbb{Z}_n)$. D је дијагонална матрица ако је $d_{ij} = 0$ за свако $i \neq j$.

Нека је $r = \min\{m, k\}$. За дијагоналну матрицу формата $m \times k$ користићемо нотацију $D = \text{diag}(d_1, \ldots, d_r)$, где је $d_{ii} = d_i$ за $i = 1, \ldots, r$. Такође, за приказ $\text{diag}(d_1, \ldots, d_r)$ постоје две форме у зависности од m и k.

Ако је $m \leq k$, тада $\text{diag}(d_1, \ldots, d_r)$ има следећу форму:

$$\text{diag}(d_1, \ldots, d_r) = \begin{bmatrix} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & d_r & 0 & \cdots & 0 \end{bmatrix}$$

Ако је $m \geq k$, тада $\text{diag}(d_1, \ldots, d_r)$ има форму

$$\text{diag}(d_1, \ldots, d_r) = \begin{bmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & d_r \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}.$$

Ако су сви елементи дијагоналне квадратне матрице једнаки онда се таква дијагонална матрица назива скаларном матрицом.

Дефиниција 21. Скаларна (дијагонална) матрица чији су сви елементи на главној дијагонали једнаки 1, а сви остали елементи 0, назива се јединичном матрицом.

$$I = \begin{bmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{bmatrix}$$

Дефиниција 22. Матрица $1 \times k$

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1k} \end{bmatrix}$$

је матрица врста, а матрица $m \times 1$

$$\begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{bmatrix}$$

је матрица колона. Ове врсте матрица се зову и вектори.

Дефиниција 23. Матрица

$$\begin{bmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

је доња троугаона матрица, а

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{bmatrix}$$

је горња троугаона матрица.

Дефиниција 24. Две матрице истог типа $A = [a_{ij}]_{m\times k}$ и $B = [b_{ij}]_{m\times k}$ над $M_{m\times k}(\mathbb{Z}_n)$ сабирају се тако што им се саберу одговарајући елементи

$$A + B = [a_{ij}]_{m\times k} + [b_{ij}]_{m\times k} = [a_{ij} +_n b_{ij}]_{m\times k}.$$

Сабирање матрица је комутативно и асоцијативно

$$A + B = B + A$$

$$(A + B) + C = A + (B + C).$$

Неутрални елемент за сабирање матрица типа $m \times k$ је нула матрица типа $m \times k$.

Дефиниција 25. Матрица се множи скаларом α тако што се сваки елемент матрице помножи тим скаларом. Ако је $A = [a_{ij}]_{m\times k}$ онда је

$$\alpha \cdot A = [\alpha a_{ij}]_{m\times k}.$$

За множење матрице скаларом и сабирање матрица важи:

- $(\alpha + \beta)A = \alpha A + \beta A$,
- $\alpha(A + B) = \alpha A + \alpha B$,
- $\alpha(\beta A) = (\alpha\beta)A$,
- $1 \cdot A = A$.

Дефиниција 26. Матрице $A = [a_{ij}]_{m\times n}$ и $B = [b_{ij}]_{p\times q}$ могуће је множити само ако је број колона матрице A једнак броју врста матрице B. Добијена матрица ће имати број врста једнак броју врста прве матрице и број колона једнак броју колона друге матрице. Производ матрица A и B је матрица $C = [c_{ij}]_{m\times q}$, тј.

$$c_{ij} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj}; \quad i = 1, 2, ..., m; \ j = 1, 2, ..., q.$$

Пример 18. Да множење матрица није комутативно можемо се уверити из следећег:

$$A = \begin{bmatrix} 2 & 0 & 5 & -5 \\ 1 & 17 & 1 & 2 \\ 14 & -9 & 1 & 0 \end{bmatrix}, \ B = \begin{bmatrix} 1 & 2 \\ 7 & 8 \\ 8 & 51 \\ 3 & -11 \end{bmatrix}$$

У пољу $\mathbb{Z}_5$ важиће:

$$A \cdot B = \begin{bmatrix} 2 & 0 & 5 & -5 \\ 1 & 17 & 1 & 2 \\ 14 & -9 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \\ 7 & 8 \\ 8 & 51 \\ 3 & -11 \end{bmatrix} = \begin{bmatrix} 27 & 314 \\ 134 & 167 \\ -41 & 7 \end{bmatrix} = \begin{bmatrix} 2 & 4 \\ 4 & 2 \\ 4 & 2 \end{bmatrix}.$$

Док $B \cdot A$ није уопште дефинисано.

Пример 19. Нека су дате матрице:

$$A = \begin{bmatrix} 14 & 19 & 50 & -5 \\ 0 & 17 & 5 & 31 \\ 42 & -9 & 15 & 23 \\ 2 & 18 & 40 & 45 \end{bmatrix}, \quad B = \begin{bmatrix} 15 & 47 & 52 & 19 \\ 32 & 16 & 12 & 28 \\ -8 & 65 & 9 & 41 \\ 18 & -3 & 60 & 14 \end{bmatrix}.$$

Одредићемо вредност збира и производа датих матрица над прстеном $\mathbb{Z}_{15}$.

Вредност $A + B$ гласи:

$$\begin{bmatrix} 14 & 19 & 50 & -5 \\ 0 & 17 & 5 & 31 \\ 42 & -9 & 15 & 23 \\ 2 & 18 & 40 & 45 \end{bmatrix} + \begin{bmatrix} 15 & 47 & 52 & 19 \\ 32 & 16 & 12 & 28 \\ -8 & 65 & 9 & 41 \\ 18 & -3 & 60 & 14 \end{bmatrix} = \begin{bmatrix} 14 & 6 & 12 & 14 \\ 2 & 3 & 2 & 14 \\ 4 & 11 & 9 & 4 \\ 5 & 0 & 10 & 14 \end{bmatrix}.$$

Док вредност $A \cdot B$ гласи:

$$\begin{bmatrix} 14 & 19 & 50 & -5 \\ 0 & 17 & 5 & 31 \\ 42 & -9 & 15 & 23 \\ 2 & 18 & 40 & 45 \end{bmatrix} \cdot \begin{bmatrix} 15 & 47 & 52 & 19 \\ 32 & 16 & 12 & 28 \\ -8 & 65 & 9 & 41 \\ 18 & -3 & 60 & 14 \end{bmatrix} = \begin{bmatrix} 13 & 12 & 5 & 13 \\ 12 & 9 & 9 & 5 \\ 6 & 6 & 6 & 13 \\ 1 & 12 & 5 & 7 \end{bmatrix}.$$

Дефиниција 27. Квадратна матрица A је инвертибилна ако постоји матрица B тако да је $A \cdot B = B \cdot A = I$. Матрица B је јединствено одређена и означава се са A^{-1}.

Дефиниција 28. Матрица A је леви (десни) делитељ нуле уколико постоји матрица $B \neq 0$ за коју је $A \cdot B = 0$ ($B \cdot A = 0$). Уколико је и $A \neq 0$, онда је A прави делитељ нуле.

Пример 20. Нека су дате матрице $A, B \in M_2(\mathbb{Z}_7)$,

$$A = \begin{bmatrix} 2 & 6 \\ 6 & 4 \end{bmatrix}, B = \begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix}.$$

Њихов производ је $A \cdot B = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. Дате матрице A и B су прави делитељи нуле у посматраном прстену квадратних матрица реда 2 над $\mathbb{Z}_7$.

Дефиниција 29. k-ти степен квадратне матрице A је

$$A^k = \underbrace{A \cdot A \cdots A}_{k-\text{пута}}.$$

Нулти степен квадратне матрице је јединична матрица

$$A^0 = I.$$

Ако је A квадратна матрица а k и l су ненегативни цели бројеви, тада је

$$A^k \cdot A^l = A^{k+l}$$

$$(A^k)^l = A^{kl}.$$

Ако матрице A и B комутирају тада је

$$(A \cdot B)^k = A^k \cdot B^k.$$

Дефиниција 30. Матрица A је нилпотентна ако за неки позитивни цели број k важи $A^k = O$. Најмање такво k зовемо степен нилпотентности.

Пример 21. Ако је A матрица из $M_3(\mathbb{Z}_5)$

$$A = \begin{bmatrix} 1 & -3 & -4 \\ -1 & 3 & 4 \\ 1 & -3 & -4 \end{bmatrix}, \text{ тј. } A = \begin{bmatrix} 1 & 2 & 1 \\ 4 & 3 & 4 \\ 1 & 2 & 1 \end{bmatrix}$$

тада је

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

Дакле матрица A је нилпотентна.

Пример 22. Ако је A матрица из $M_3(\mathbb{Z}_5)$

$$A = \begin{bmatrix} 1 & 1 & 3 \\ 5 & 2 & 6 \\ -2 & -1 & -3 \end{bmatrix}, \text{ тј. } A = \begin{bmatrix} 1 & 1 & 3 \\ 0 & 2 & 1 \\ 3 & 4 & 2 \end{bmatrix}$$

тада је

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

Дакле матрица A је нилпотентна.

Пример 23. Посматрајмо матрице $A = \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}$ и $B = \begin{bmatrix} 0 & 0 \\ b & 0 \end{bmatrix}$, где су $a, b \in \mathbb{Z}_n$ и a, b нису нилпотентни елементи у $\mathbb{Z}_n$. Матрице су нилпотентне са степеном нилпотентности 2, али њихов збир $A + B = \begin{bmatrix} 0 & a \\ b & 0 \end{bmatrix}$, није нилпотентна матрица.

Дефиниција 31. За матрицу $A = [a_{ij}]_{m\times n}$, транспонована матрица $(A = [a_{ij}]_{m\times n})^T$ добија се када врсте и колоне дате матрице замене места.

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

$$A^T = \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{bmatrix}$$

За транспоноване матрице важи:

- $(A^T)^T = A$,
- $(\alpha A)^T = \alpha A^T$,
- $(A + B)^T = A^T + B^T$,
- $(A \cdot B)^T = B^T \cdot A^T$.

Глава 4

Детерминанте

Нека је A квадратна матрица реда 2:

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

дефинисаћемо њену детерминанту

$$\det A = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}$$

на следећи начин

$$\det A = a_{11}a_{22} - a_{12}a_{21}.$$

За квадратну матрицу A реда 3 одговарајућа детерминанта је

$$\det A = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \end{vmatrix} =$$

$$= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}$$

што представља и Сарусово правило које се користи само за израчунавање детерминанти трећег реда.

Приметимо да су сви сабирци облика $a_{1j_1}a_{2j_2}a_{3j_3}$, где $j_1j_2j_3$ представљају редом пермутације бројева 1,2 и 3:

123 231 312 321 132 213

Промена редоследа елемената у пермутацији у односу на основну пермутацију назива се инверзијом. На пример, у пермутацији 231 постоје две инверзије: 2 испред 1 и 3 испред 1. Пермутације са парним бројем инверзија зову се парним, а са непарним бројем инверзија непарним пермутацијама. Уочимо и да су сви сабирци за које $j_1j_2j_3$ чине парну пермутацију позитивни, док су негативни сабирци у којима су $j_1j_2j_3$ непарне пермутације.

Ако бисмо са k означили број инверзија у пермутацији $j_1j_2j_3$, онда сваки сабирак који чини детерминанту реда 3 можемо представити као

$$(-1)^k a_{1j_1}a_{2j_2}a_{3j_3}$$

па

$$\det A = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \sum_{j_1j_2j_3 \in S} (-1)^k a_{1j_1}a_{2j_2}a_{3j_3}$$

где је S скуп свих пермутација скупа $\{1, 2, 3\}$ којих има 3!.

Из наредне дефиниције можемо видети како се дефинише детерминанта реда n.

Дефиниција 32. За квадратну матрицу $A = [a_{ij}]_{n\times n}$ детерминанта гласи

$$\det A = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = \sum_{j_1j_2\cdots j_n \in S} (-1)^k a_{1j_1}a_{2j_2}\cdots a_{nj_n}$$

где S представља скуп свих пермутација скупа $\{1, 2, ..., n\}$ којих има укупно $n!$, а k је број инверзија у пермутацији $j_1j_2\cdots j_n$.

Дефиниција 33. Минор M_{ij} елемента a_{ij} је детерминанта $(n-1)$ реда која се добија из дате матрице (реда n) изостављањем i-те врсте и j-те колоне.

Пример 24. Нека је дата матрица $A \in M_3(\mathbb{Z})$

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}.$$

Минори дате матрице су:
$M_{11} = \begin{vmatrix} 5 & 6 \\ 8 & 9 \end{vmatrix} = -3,\ M_{12} = \begin{vmatrix} 4 & 6 \\ 7 & 9 \end{vmatrix} = -6,\ M_{13} = \begin{vmatrix} 4 & 5 \\ 7 & 8 \end{vmatrix} = -3,\ M_{21} = \begin{vmatrix} 2 & 3 \\ 8 & 9 \end{vmatrix} = -6,\ M_{22} = \begin{vmatrix} 1 & 3 \\ 7 & 9 \end{vmatrix} = -12,\ M_{23} = \begin{vmatrix} 1 & 2 \\ 7 & 8 \end{vmatrix} = -6,\ M_{31} = \begin{vmatrix} 2 & 3 \\ 5 & 6 \end{vmatrix} = -3,$
$M_{32} = \begin{vmatrix} 1 & 3 \\ 4 & 6 \end{vmatrix} = -6,\ M_{33} = \begin{vmatrix} 1 & 2 \\ 4 & 5 \end{vmatrix} = -3.$

Дефиниција 34. Кофактор A_{ij} елемента a_{ij} је $(-1)^{i+j}M_{ij}$.

Пример 25. Кофактори матрице из претходног примера су: $A_{11} = M_{11} = -3,\ A_{12} = -M_{12} = 6,\ A_{13} = M_{13} = -3,\ A_{21} = -M_{21} = 6,\ A_{22} = M_{22} = -12,\ A_{23} = -M_{23} = 6,\ A_{31} = M_{31} = -3,\ A_{32} = -M_{32} = 6,\ A_{33} = M_{33} = -3.$

За детерминанте важе следећа својства која наводимо без доказа [1]:

1. Детерминанта производа двеју матрица једнака је производу њихових детерминанти.
2. Ако две врсте(колоне) замене места, вредност детерминанте постаје супротног знака.
3. Детерминанта чија је једна врста(колона) нула, има вредност нула.
4. Ако су две врсте(колоне) пропорционалне, вредност детерминанте једнака је нули.
5. Ако једну врсту(колону) детерминанте помножимо скаларом k и добијену вредност додамо другој врсти(колони), вредност детерминанте се неће променити.
6. Множење детерминанте скаларом k јесте множење једне врсте или колоне датим скаларом.
7. Степен детерминанте једнак је детерминанти степена.

Лема 1. Ако је матрица A нилпотентна над пољем, тада је $\det A = 0$.

Доказ. Kako je $A^k = 0$ онда $(\det A)^k = \det(A^k) = \det 0 = 0$ тј. $(\det A)^k = 0$ па је $\det A = 0$. □

Дефиниција 35. Адјунгована матрица матрице A је:

$$\text{adj } A = [A_{ij}]^T = \begin{bmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & & \vdots \\ A_{n1} & \cdots & A_{nn} \end{bmatrix}^T = \begin{bmatrix} A_{11} & \cdots & A_{n1} \\ \vdots & & \vdots \\ A_{1n} & \cdots & A_{nn} \end{bmatrix}$$

где су A_{ij} кофактори елемената a_{ij}.

Теорема 5. Нека је i произвољна врста квадратне матрице $A \in M_m(\mathbb{Z}_n)$. Тада је:

$$\det A = \sum_{j=1}^{m} a_{ij} A_{ij}.$$

Израчунавање детерминанте на овај начин назива се *развијање* детерминанте по i-тој врсти.

Аналогно, ако је j произвољна колона квадратне матрице $A \in M_m(\mathbb{Z}_n)$, тада је:

$$\det A = \sum_{i=1}^{m} a_{ij} A_{ij}$$

што представља *развијање* детерминанте по j-тој колони.

Наведена теорема зове се **Лапласов**[2] **развој детерминанте** по вр-

[1] Докази су исти као и за матрице над пољем, што је рађено у курсу Линеарне алгебре.

[2] Пјер Лаплас, 1749-1827., француски математичар

сти (колони).

Лема 2. За квадратну матрицу $A \in M_m(\mathbb{Z}_n)$ важи

$$A \cdot \text{adj } A = (\text{adj } A) \cdot A = (\det A) \cdot I.$$

У шта се и сами можемо уверити

$$\begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mm} \end{bmatrix} \cdot \begin{bmatrix} A_{11} & \cdots & A_{m1} \\ \vdots & & \vdots \\ A_{1m} & \cdots & A_{mm} \end{bmatrix} = \sum_{j=1}^{m} a_{ij}A_{ij} = \begin{bmatrix} \det A & \cdots & 0 \\ \vdots & \det A & \vdots \\ 0 & \cdots & \det A \end{bmatrix}.$$

На овом месту, оправдано је питати се, да ли из дате једнакости можемо доћи до инверзне матрице матрице A. Помножимо за почетак дату једнакост инверзном матрицом A^{-1}

$$A^{-1} \cdot A \cdot \text{adj } A = A^{-1} \cdot \det A$$
$$\text{adj } A = A^{-1} \cdot \det A.$$

Затим ћемо обе стране једнакости помножити инверзом[3] елемента $\det A$, тј. помножићемо бројем $(\det A)^{-1}$.

$$A^{-1} = \text{adj } A \cdot (\det A)^{-1}$$

На овај начин дошли смо до закључка да ће инверзна матрица A^{-1} матрице $A \in M_m(\mathbb{Z}_n)$ бити облика $A^{-1} = (\det A)^{-1} \cdot \text{adj } A$, под условом да $\det A$ има инверз у $\mathbb{Z}_n$, о чему и говори наредна теорема.

Теорема 6. Матрица A је инвертибилна у $M_m(\mathbb{Z}_n)$ ако и само ако њена детерминанта има инверз у $\mathbb{Z}_n$.

Доказ. Теорему ћемо доказати доказујући сваки смер посебно.

$\Rightarrow$ Ако је матрица A инвертибилна у прстену $M_m(\mathbb{Z}_n)$, тада постоји матрица $B \in M_m(\mathbb{Z}_n)$ таква да важи $AB = BA = I$. Како је $1 = \det I = \det AB = \det A \cdot \det B$, то управо значи да је $\det A$ инвертибилни елемент у прстену $\mathbb{Z}_n$.

$\Leftarrow$ Ако је $\det A$ инвертибилан елемент у прстену $\mathbb{Z}_n$, множењем једнакости $A \cdot \text{adj } A = (\text{adj } A) \cdot A = (\det A) \cdot I$ инверзом елемента $\det A$, тј. $(\det A)^{-1}$ добијамо:

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

из чега следи да је матрица A инвертибилна у $M_m(\mathbb{Z}_n)$. □

Последица 1. У случају да $\det A$ није инвертибилни елемент у $\mathbb{Z}_n$, и сама матрица A неће имати инверзну матрицу.

[3] у случају да такав елемент у скупу $\mathbb{Z}_n$ заиста и постоји!

Напомена 6. Тврђење $A \cdot \text{adj } A = (\text{adj } A) \cdot A = (\det A) \cdot I$ остаје да важи чак и ако матрица A нема инверзну матрицу.

Из изложеног проистиче, да ће с обзиром да је нула једини елемент поља који нема инверз, услов $\det A \neq 0$ бити довољан за закључак да је задата матрица над пољем увек инвертибилна. Ако је у питању матрица над прстеном, услов $\det A \neq 0$ не гарантује постојање инверзне матрице, што следи из дефиниције прстена.

Пример 26. Нека је матрица $A \in M_3(\mathbb{Z}_{14})$,

$$A = \begin{bmatrix} 2 & 14 & 20 \\ -9 & 7 & 4 \\ 30 & 15 & -5 \end{bmatrix}, \text{ тј. } A = \begin{bmatrix} 2 & 0 & 6 \\ 5 & 7 & 4 \\ 2 & 1 & 9 \end{bmatrix}.$$

Одредимо детерминанту матрице A:

$$\det A = 2 \cdot \begin{vmatrix} 7 & 4 \\ 1 & 9 \end{vmatrix} - 0 \cdot \begin{vmatrix} 5 & 4 \\ 2 & 9 \end{vmatrix} + 6 \cdot \begin{vmatrix} 5 & 7 \\ 2 & 1 \end{vmatrix} = 8.$$

Вредност детерминанте није инвертибилан елемент у прстену $\mathbb{Z}_{14}$ јер не постоји такав елемент $x \in \mathbb{Z}_{14}$ за који важи $8 \cdot x = 1$. Управо из овог разлога, и сама матрица A нема инверз. Међутим, ова чињеница не значи да не важи:

$$(\text{adj } A) \cdot A = (\det A) \cdot I.$$

Уверимо се да претходно својство важи.

Одредимо кофакторе:

$$A_{11} = 59 \equiv_{14} 3,\ A_{12} = -37 \equiv_{14} 5,\ A_{13} = -9 \equiv_{14} 5$$
$$A_{21} = 6 \equiv_{14} 6,\ A_{22} = 6 \equiv_{14} 6,\ A_{23} = -2 \equiv_{14} 12,$$
$$A_{31} = -42 \equiv_{14} 0,\ A_{32} = 22 \equiv_{14} 8,\ A_{33} = 14 \equiv_{14} 0$$

Тада је матрица кофактора:

$$[A_{ij}] = \begin{bmatrix} 3 & 5 & 5 \\ 6 & 6 & 12 \\ 0 & 8 & 0 \end{bmatrix}$$

као и

$$\text{adj } A = \begin{bmatrix} 3 & 6 & 0 \\ 5 & 6 & 8 \\ 5 & 12 & 0 \end{bmatrix}$$

и провером се уверавамо да важи:

$$\begin{bmatrix} 3 & 6 & 0 \\ 5 & 6 & 8 \\ 5 & 12 & 0 \end{bmatrix} \cdot \begin{bmatrix} 2 & 0 & 6 \\ 5 & 7 & 4 \\ 2 & 1 & 9 \end{bmatrix} = 8 \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 8 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 8 \end{bmatrix} = \begin{bmatrix} 8 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 8 \end{bmatrix}$$

Пример 27. За дату матрицу $A \in M_3(\mathbb{Z}_6)$,

$$A = \begin{bmatrix} 9 & 8 & 14 \\ 6 & 19 & -1 \\ 7 & -1 & 2 \end{bmatrix}, \text{ тј. } A = \begin{bmatrix} 3 & 2 & 2 \\ 0 & 1 & 5 \\ 1 & 5 & 2 \end{bmatrix}$$

$$\det A = 3 \cdot \begin{vmatrix} 1 & 5 \\ 5 & 2 \end{vmatrix} - 0 \cdot \begin{vmatrix} 2 & 2 \\ 5 & 2 \end{vmatrix} + 1 \cdot \begin{vmatrix} 2 & 2 \\ 1 & 5 \end{vmatrix} = 5.$$

Инвертибилни елемент елемента 5 у прстену $\mathbb{Z}_6$ јесте број 5. У наставку одређујемо матрицу кофактора, адјунговану, а затим и инверзну матрицу матрице A:

$$[A_{ij}] = \begin{bmatrix} 1 & 5 & 5 \\ 0 & 4 & 5 \\ 2 & 3 & 3 \end{bmatrix}$$

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

односно

$$A^{-1} \cdot 5 = \begin{bmatrix} 1 & 0 & 2 \\ 5 & 4 & 3 \\ 5 & 5 & 3 \end{bmatrix} \quad / \cdot 5$$

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

$$A^{-1} = \begin{bmatrix} 5 & 0 & 10 \\ 25 & 20 & 15 \\ 25 & 25 & 15 \end{bmatrix} = \begin{bmatrix} 5 & 0 & 4 \\ 1 & 2 & 3 \\ 1 & 1 & 3 \end{bmatrix}.$$

Глава 5

Ранг матрице

Став 1. Ако је I идеал у прстену $\mathbb{Z}_n$, тада је

$$M_m(I) = \{A \in M_m(\mathbb{Z}_n) \mid a_{ij} \in I, \text{ за све } i, j = 1, \ldots, m\}$$

идеал у $M_m(\mathbb{Z}_n)$.

Дефиниција 36. Нека је $A \in M_{m\times k}(\mathbb{Z}_n)$. За свако $t = 1, \ldots, r = \min\{m, k\}$ идеал $I_t(A)$ прстена $\mathbb{Z}_n$ генерисан је свим минорима реда t из A.

На основу Лапласове теореме следи да сваки минор реда $t+1$ матрице A припада $I_t(A)$. На тај начин формира се ланац идеала у $\mathbb{Z}_n$:

$$I_r(A) \subseteq I_{r-1}(A) \subseteq \cdots \subseteq I_2(A) \subseteq I_1(A) \subseteq \mathbb{Z}_n.$$

Проширимо дефиницију идела $I_t(A)$ за све вредности $t \in \mathbb{Z}$ на следећи начин:

$$I_t(A) = \begin{cases} \langle 0\rangle, & t > \min\{m, k\} \\ \mathbb{Z}_n, & t \leq 0 \end{cases}$$

тако да важи

$$\langle 0\rangle = I_{r+1}(A) \subseteq I_r(A) \subseteq \cdots \subseteq I_1(A) \subseteq I_0(A) = \mathbb{Z}_n.$$

Дефиниција 37. Анулатор идеала $I_t(A)$ јесте

$$\mathrm{Ann}_{\mathbb{Z}_n}(I_t(A)) = \{r \mid a \cdot r = 0,\ a \in I_t(A)\}.$$

Приметимо да је

$$\langle 0\rangle = \mathrm{Ann}_{\mathbb{Z}_n}(\mathbb{Z}_n) \subseteq \mathrm{Ann}_{\mathbb{Z}_n}(I_1(A)) \subseteq \mathrm{Ann}_{\mathbb{Z}_n}(I_2(A)) \subseteq \cdots \subseteq \mathrm{Ann}_{\mathbb{Z}_n}(I_r(A)) \subseteq \mathrm{Ann}_{\mathbb{Z}_n}(\langle 0\rangle) = \mathbb{Z}_n$$

Анулатори нам помажу да дефинишемо ранг матрице A, у ознаци $\mathrm{rang}(A)$ над прстеном $\mathbb{Z}_n$.

Дефиниција 38. Нека је $A \in M_{m\times k}(\mathbb{Z}_n)$. Ранг матрице A над прстеном $\mathbb{Z}_n$ јесте

$$\operatorname{rang}(A) = \max\{t \mid \operatorname{Ann}_{\mathbb{Z}_n}(I_t(A)) = \langle 0\rangle\}$$

Теорема 7. Нека је $A \in M_{m\times k}(\mathbb{Z}_n)$. Тада важи:

1. $0 \leq \operatorname{rang}(A) \leq \min\{m, k\}$
2. $\operatorname{rang}(A) = 0$ ако и само ако $\operatorname{Ann}_{\mathbb{Z}_n}(I_1(A)) \neq \langle 0\rangle$
3. ако је $m = k$, тада је $\operatorname{rang}(A) < k$ ако и само ако $\det A \in Z(\mathbb{Z}_n)$.

Доказ. Како је $I_0(A) = \mathbb{Z}_n$ и $\operatorname{Ann}_{\mathbb{Z}_n}(\mathbb{Z}_n) = \langle 0\rangle$ важи да је $\operatorname{rang}(A) \geq 0$. Ако је $t > \min\{m, k\}$ тада је $I_t(A) = \langle 0\rangle$ и $\operatorname{Ann}_{\mathbb{Z}_n}(\langle 0\rangle) = \mathbb{Z}_n$. Дакле $\operatorname{rang}(A) \leq \min\{m, k\}$.

Својство **2** следи директно из дефиниције ранга матрице, за случај $t \leq 0$. Ако је $\operatorname{Ann}_{\mathbb{Z}_n}(I_1(A)) \neq \langle 0\rangle$, и како анулатори идеала образују растући ланац $\operatorname{Ann}_{\mathbb{Z}_n}(I_0(A)) \subseteq \operatorname{Ann}_{\mathbb{Z}_n}(I_1(A))$, при чему је $I_0(A) = \mathbb{Z}_n$ и $\operatorname{Ann}_{\mathbb{Z}_n}(\mathbb{Z}_n) = \langle 0\rangle$, следи да је $\operatorname{Ann}_{\mathbb{Z}_n}(I_t(A)) = \langle 0\rangle$ једино за $t = 0$ односно када је $\operatorname{rang}(A) = 0$.

Својство **3** такође следи директно из дефиниције ранга матрице, јер уколико је $\operatorname{rang}(A) < k$, значи да је анулатор $\operatorname{Ann}_{\mathbb{Z}_n}(I_k(A)) \neq \langle 0\rangle$, односно да постоји ненула елемент $x \in \mathbb{Z}_n$ такав да важи $x \cdot m = 0$ за свако $m \in I_k(A)$. Како је идеал $I_k(A)$ генерисан минором реда k тј. детерминантом $\det A$, то је $m = s \cdot \det A$ за неко $s \in \mathbb{Z}_n$, односно $y \cdot \det A = 0$ за $y = x \cdot s$, што значи да је $\det A \in Z(\mathbb{Z}_n)$. Обратно, ако је детерминанта матрице реда k делитељ нуле у прстену $\mathbb{Z}_n$, то значи да постоји бар један ненула елемент $x \in \mathbb{Z}_n$ такав да је $x \cdot \det A = 0$, а такав елемент припада анулатору $x \in \operatorname{Ann}_{\mathbb{Z}_n}(I_k(A))$, па је $\operatorname{Ann}_{\mathbb{Z}_n}(I_k(A)) \neq \langle 0\rangle$, одакле према дефиницији следи да k није ред максималног минора за који је анулатор идеала генерисаног тим минором тривијалан, односно да $\operatorname{rang}(A) \neq k$, па је $\operatorname{rang}(A) < k$ према својству **1**. □

Пример 28. Одредити ранг матрице $A = \begin{bmatrix} 2 & 2 \\ 0 & 2 \end{bmatrix} \in M_2(\mathbb{Z}_6)$.

Идеал $I_1(A)$ генерисан је свим минорима реда 1, па је

$$I_1(A) = 2\mathbb{Z}_6 = \{0, 2, 4\}.$$

Анулатор овог идеала јесте

$$\operatorname{Ann}_{\mathbb{Z}_6}(I_1(A)) = \operatorname{Ann}_{\mathbb{Z}_6}(2\mathbb{Z}_6) = 3\mathbb{Z}_6 = \{0, 3\} \neq \langle 0\rangle.$$

На основу **Теореме 7.** закључујемо да је $\operatorname{rang}(A) = 0$.

Пример 29. Одредити ранг матрице $B = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} \in M_2(\mathbb{Z}_6)$.

Идеал $I_1(B)$ генерисан је свим минорима реда 1, па је

$$I_1(B) = 2\mathbb{Z}_6 + 3\mathbb{Z}_6 = \mathbb{Z}_6.$$

Анулатор овог идеала јесте

$$\mathrm{Ann}_{\mathbb{Z}_6}(I_1(B)) = \mathrm{Ann}_{\mathbb{Z}_6}(\mathbb{Z}_6) = \{0\} = \langle 0 \rangle.$$

На основу **Теореме 7.** закључујемо да је $\mathrm{rang}(B) \neq 0$, као и да је $0 \leq \mathrm{rang}(B) \leq 2$. Проверићемо да ли је $\det B$ делитељ нуле у $\mathbb{Z}_6$. Како је $\det B = 0 \in Z(\mathbb{Z}_6)$, закључујемо да је према истој теореми $\mathrm{rang}(B) < 2$. Коначно можемо извести закључак да је $\mathrm{rang}(B) = 1$.

Пример 30. Одредити ранг матрице $C = \begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix} \in M_2(\mathbb{Z}_6)$.

Идеал $I_1(C)$ генерисан је свим минорима реда 1, па је

$$I_1(C) = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}.$$

Анулатор овог идеала јесте

$$\mathrm{Ann}_{\mathbb{Z}_6}(I_1(C)) = \mathrm{Ann}_{\mathbb{Z}_6}(\mathbb{Z}_6) = \{0\} = \langle 0 \rangle.$$

Дакле, према **Теореми 7.** $\mathrm{rang}(C) \neq 0$. Као и у претходном примеру одредићемо детерминанту матрице C. Како је $\det C = 5$, и $\det C$ није делитељ нуле у $\mathbb{Z}_6$, према истој теореми, закључујемо да је $\mathrm{rang}(C) \geq 2$.

Дакле, како важи $\mathrm{rang}(C) \neq 0,\ \mathrm{rang}(C) \geq 2,\ 0 \leq \mathrm{rang}(C) \leq 2$, следи да је $\mathrm{rang}(C) = 2$.

Природно је поставити питање у каквој су вези ранг матрице над прстеном $\mathbb{Z}_n$ који смо дефинисали у претходном делу, и ранг матрице над пољем[1] $\mathbb{Z}_p$ (p је прост број). Ранг матрице A над прстеном $\mathbb{Z}_n$ означаваћемо као и до сада $\mathrm{rang}(A)$, а ранг матрице над пољем $\mathbb{Z}_p$ са $\mathrm{rg}(A)$. Ранг матрице над пољем дефинише се као максималан број линеарно независних вектора врсте (колоне) матрице A. Познато је, да је ранг матрице над пољем једнак највећем броју t таквом да матрица A садржи подматрицу реда t са ненула детерминантом. Како је $\mathbb{Z}_p$ поље тада је $\mathrm{Ann}(I_t(A)) = \langle 0 \rangle$ ако и само ако је $I_t(A) \neq \langle 0 \rangle$. Међутим, $\mathrm{rang}(A)$ је највећи број t тако да A садржи подматрицу реда t чија је детерминанта ненула. Другим речима $\mathrm{rang}(A) = \mathrm{rg}(A)$. Зато се, када је $\mathbb{Z}_p$ поље дефиниција дата за ранг матрице над прстеном $\mathbb{Z}_n$ поклапа са класичном дефиницијом ранга матрице.

Пример 31. Одредити ранг матрице $D = \begin{bmatrix} 2 & 3 \\ 5 & 6 \end{bmatrix} \in M_2(\mathbb{Z}_7)$.

[1] класични ранг из линеарне алгебре

Идеал $I_1(D)$ генерисан је свим минорима реда 1, па је

$$I_1(D) = \mathbb{Z}_7.$$

Анулатор овог идеала јесте

$$\mathrm{Ann}_{\mathbb{Z}_7}(I_1(D)) = \mathrm{Ann}_{\mathbb{Z}_7}(\mathbb{Z}_7) = \{0\} = \langle 0 \rangle.$$

Дакле, према **Теореми 7.** $\mathrm{rang}(D) \neq 0$. Као и у претходном примеру одредићемо детерминанту матрице D. Како је $\det D = 4$, и $\det D$ није делитељ нуле у $\mathbb{Z}_7$, па према истој теореми, закључујемо да је $\mathrm{rang}(D) \geq 2$.

Дакле, како важи $\mathrm{rang}(D) \neq 0,\ \mathrm{rang}(D) \geq 2,\ 0 \leq \mathrm{rang}(D) \leq 2$, следи да је $\mathrm{rang}(D) = 2$.

С обзиром да је $\mathbb{Z}_7$ поље, одредимо ранг матрице D на класичан начин.

$$D = \begin{bmatrix} 2 & 3 \\ 5 & 6 \end{bmatrix} = \begin{bmatrix} 0 & 3 \\ 1 & 0 \end{bmatrix}$$

Број линеарно независних вектора врсте је 2, дакле $\mathrm{rg}(D) = 2$, што се слаже са својством да за поља важи $\mathrm{rang}(D) = \mathrm{rg}(D)$.

Пример 32. Одредити ранг матрице $E = \begin{bmatrix} 2 & 0 & -3 \\ 1 & 1 & 1 \end{bmatrix} \in M_{2\times 3}(\mathbb{Z}_{30})$.

Идеал $I_1(E)$ генерисан је свим минорима реда 1, па је

$$I_1(E) = \mathbb{Z}_{30}.$$

Анулатор овог идеала јесте

$$\mathrm{Ann}_{\mathbb{Z}_{30}}(I_1(E)) = \mathrm{Ann}_{\mathbb{Z}_{30}}(\mathbb{Z}_{30}) = \{0\} = \langle 0 \rangle.$$

Дакле, према **Теореми 7.** $\mathrm{rang}(E) \neq 0$.

Одредићемо идеал $I_2(E)$. Детерминанте подматрица су у овом случају $2, 3, 5$, па је

$$I_2(E) = 2\mathbb{Z}_{30} + 3\mathbb{Z}_{30} + 5\mathbb{Z}_{30} = \mathbb{Z}_{30}.$$

Анулатор овог идеала јесте

$$\mathrm{Ann}_{\mathbb{Z}_{30}}(I_2(E)) = \mathrm{Ann}_{\mathbb{Z}_{30}}(\mathbb{Z}_{30}) = \{0\} = \langle 0 \rangle.$$

Из дефиниције о рангу матрице добијамо да $\mathrm{rang}(E) = 2$.

Пример 33. Одредити ранг матрице $F = \begin{bmatrix} 2 & 3 & 5 \\ 2 & 0 & 2 \\ 2 & 4 & 6 \end{bmatrix} \in M_3(\mathbb{Z}_{12})$.

Идеал $I_1(F)$ генерисан је свим минорима реда 1, па је

$$I_1(F) = \mathbb{Z}_{12}.$$

Анулатор овог идеала јесте

$$\mathrm{Ann}_{\mathbb{Z}_{12}}(I_1(F)) = \mathrm{Ann}_{\mathbb{Z}_{12}}(\mathbb{Z}_{12}) = \{0\} = \langle 0 \rangle.$$

Дакле, према **Теореми 7.** закључујемо да је $\mathrm{rang}(F) \neq 0$.

Како је $\det F = 0 \in Z(\mathbb{Z}_{12})$, па према истој теореми, закључујемо да је $\mathrm{rang}(F) < 3$.

Одредићемо идеал $I_2(F)$. Детерминанте подматрица реда 2 су: -8 (тј. 4 у прстену $\mathbb{Z}_{12}$), 8, 8, $-2 = 10$, 2, 2, 6, $-6 = 6$, $-6 = 6$ па је њима генерисан идеал

$$I_2(F) = 2\mathbb{Z}_{12}.$$

Анулатор овог идеала јесте

$$\mathrm{Ann}_{\mathbb{Z}_{12}}(I_2(F)) = \mathrm{Ann}_{\mathbb{Z}_{12}}(2\mathbb{Z}_{12}) = 6\mathbb{Z}_{12} = \{0, 6\} \neq \langle 0 \rangle,$$

па према истој теореми, закључујемо да је $\mathrm{rang}(F) \neq 2$.

Дакле, како важи $\mathrm{rang}(F) \neq 0$, $\mathrm{rang}(F) < 3$, $\mathrm{rang}(F) \neq 2$, следи да је $\mathrm{rang}(F) = 1$.

Пример 34. Одредити ранг матрице $G = \begin{bmatrix} 1 & 4 & 2 & 7 \\ 2 & 1 & 8 & 2 \\ 3 & 0 & 3 & 4 \end{bmatrix} \in M_{3\times 4}(\mathbb{Z}_{12})$.

Идеал $I_1(G)$ генерисан је свим минорима реда 1, па је

$$I_1(G) = \mathbb{Z}_{12}.$$

Анулатор овог идеала јесте

$$\mathrm{Ann}_{\mathbb{Z}_{12}}(I_1(G)) = \mathrm{Ann}_{\mathbb{Z}_{12}}(\mathbb{Z}_{12}) = \{0\} = \langle 0 \rangle.$$

Дакле, према **Теореми 7.** $\mathrm{rang}(G) \neq 0$.

Одредићемо идеал $I_3(G)$. Детерминанте подматрица реда 3 су:

$$\det G_1 = \begin{vmatrix} 4 & 2 & 7 \\ 1 & 8 & 2 \\ 0 & 3 & 4 \end{vmatrix} = 9$$

$$\det G_2 = \begin{vmatrix} 1 & 2 & 7 \\ 2 & 8 & 2 \\ 3 & 3 & 4 \end{vmatrix} = 4$$

$$\det G_3 = \begin{vmatrix} 1 & 4 & 7 \\ 2 & 1 & 2 \\ 3 & 0 & 4 \end{vmatrix} = 11$$

$$\det G_4 = \begin{vmatrix} 1 & 4 & 2 \\ 2 & 1 & 8 \\ 3 & 0 & 3 \end{vmatrix} = 9$$

па је

$$I_3(G) = 11\mathbb{Z}_{12} = \mathbb{Z}_{12}.$$

Анулатор овог идеала јесте

$$\mathrm{Ann}_{\mathbb{Z}_{12}}(I_3(G)) = \mathrm{Ann}_{\mathbb{Z}_{12}}(\mathbb{Z}_{12}) = \{0\} = \langle 0 \rangle.$$

Из дефиниције о рангу матрице добијамо да је $\mathrm{rang}(G) = 3$.

Глава 6

Кинеска теорема о остацима

Теорема 8. Нека су $m_1, m_2, ..., m_n \geq 2$ цели бројеви за које је испуњено НЗД$(m_i, m_j) = 1$ за $i \neq j$. Тада су прстени $\mathbb{Z}_{m_1 m_2 \cdots m_n}$ и $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$ изоморфни.

Доказ. Нека је $m = m_1 m_2 \cdots m_n$. Приметимо да оба прстена имају m елемената. Стога је, за доказ постојања изоморфизма, довољно конструисати једну „1-1" функцију из једног у други, која се слаже са операцијама, јер ће та функција сигурно бити и „на", тј. изоморфизам (то су коначни скупови са истим бројем елемената). Ако са $\rho_k(x)$ означимо остатак при (еуклидском) дељењу x са k, онда је тражена функција $f : \mathbb{Z}_m \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$ дефинисана са:

$$f(x) := (\rho_{m_1}(x), \rho_{m_2}(x), ..., \rho_{m_n}(x)).$$

Докажимо да је f „1-1". Нека је $f(x) = f(y)$. То значи да за $i = \{1, ..., n\}$ важи: $\rho_{m_i}(x) = \rho_{m_i}(y)$. Но, ако два броја имају исти остатак при дељењу бројем m_i, онда је њихова разлика дељива са m_i. Дакле, за $i = \{1, ..., n\}$ важи: $m_i \mid (x - y)$. Како су бројеви m_i узајамно прости, следи да $m \mid (x - y)$. С обзиром да $x, y \in \mathbb{Z}_m = \{0, 1, ..., m - 1\}$, добијамо да је $x - y = 0$, тј. $x = y$.

Докажимо да се f слаже са операцијама, тј. да је за све $x, y \in \mathbb{Z}_m : f(x +_m y) = f(x) + f(y)$ и $f(x \cdot_m y) = f(x) \cdot f(y)$ (где је са $+$, односно $\cdot$ означена операција у директном производу, за коју знамо како се дефинише). Доказаћемо то за операцију множења.

Дакле, треба доказати да је $f(x \cdot_m y) = f(x) \cdot f(y)$ за све $x, y \in \mathbb{Z}_m$. С обзиром на дефиницију функције f и дефиницију операције $\cdot$, ово се своди на доказ чињенице да је за све $i = \{1, ..., n\}$ испуњено:

$$\rho_{m_i}(x \cdot_m y) = \rho_{m_i}(x) \cdot_{m_i} \rho_{m_i}(y).$$

Доказ ћемо извести тако што ћемо показати да су и лева и десна страна ове једнакости заправо остаци при дељењу $x \cdot y$ са m (где је овде

$\cdot$ операција множења целих бројева). Наиме, по дефиницији операције $\cdot_m$ имамо да је

$$x \cdot y \equiv x \cdot_m y \pmod{m}.$$

Приметимо да важи следеће: ако је $a \equiv b \pmod{m}$ и ако $k \mid m$, онда је и $a \equiv b \pmod{k}$. Наиме, $a \equiv b \pmod{m}$, је еквивалентно са $m \mid (a-b)$. Како $k \mid m$, то следи да је и $k \mid (a-b)$, што је еквивалентно са $a \equiv b \pmod{k}$. Стога, из

$$x \cdot y \equiv x \cdot_m y \pmod{m},$$

следи да за све $i = \{1, ..., n\}$ важи:

$$x \cdot y \equiv x \cdot_m y \pmod{m_i}.$$

С обзиром да је

$$x \equiv \rho_k(x) \pmod{k},$$

добијамо да је

$$x \cdot_m y \equiv \rho_{m_i}(x \cdot_m y) \pmod{m_i},$$

те, напокон, добијамо да је

$$x \cdot y \equiv \rho_{m_i}(x \cdot_m y) \pmod{m_i}.$$

С обзиром да је $\rho_{m_i}(x \cdot_m y) \in \mathbb{Z}_{m_i}$, следи да је тај број заправо остатак при дељењу $x \cdot y$ са m_i.

Како је $x \equiv \rho_{m_i}(x) \pmod{m_i}$ и $y \equiv \rho_{m_i}(y) \pmod{m_i}$, то је

$$\rho_{m_i}(x) \cdot_{m_i} \rho_{m_i}(y) \equiv x \cdot_{m_i} y \pmod{m_i}.$$

Но,

$$x \cdot_{m_i} y \equiv x \cdot y \pmod{m_i},$$

те је и

$$x \cdot y \equiv \rho_{m_i}(x) \cdot_{m_i} \rho_{m_i}(y) \pmod{m_i}.$$

С обзиром да $\rho_{m_i}(x) \cdot_{m_i} \rho_{m_i}(y) \in \{0, 1, ..., m_i - 1\}$, следи да је $\rho_{m_i}(x) \cdot_{m_i} \rho_{m_i}(y) \in \{0, 1, ..., m_i - 1\}$ остатак при дељењу $x \cdot y$ са m_i. Закључујемо да мора бити

$$\rho_{m_i}(x) \cdot_{m_i} \rho_{m_i}(y) = \rho_{m_i}(x \cdot_m y),$$

јер је и један и други број остатак при дељењу $x \cdot y$ са m_i. □

Теорема 9. (Кинеска теорема о остацима) Нека су $m_1, m_2, ..., m_n \geq 2$ цели бројеви за које је испуњено НЗД$(m_i, m_j) = 1$ за $i \neq j$. Тада за произвољне $x_i \in \mathbb{Z}, i = \{1, ..., n\}$, систем конгруенција

$$x \equiv x_1 \pmod{m_1}$$

$$x \equiv x_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv x_n \pmod{m_n}$$

има јединствено решење по модулу $m_1 m_2 \cdots m_n$.

Доказ. Функција f, дефинисана у претходној теореми, је изоморфизам. Ми ћемо искористити чињеницу да је она „на". Нека су $x_1, x_2, ..., x_n \in \mathbb{Z}$. Са r_i означимо остатак при дељењу броја x_i са m_i. Јасно је да тада важи $x_i \equiv r_i \pmod{m_i}$, за $i = \{1, ..., n\}$. Формирајмо n-торку $(r_1, r_2, ..., r_n) \in \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$. Како је f „на", то постоји $x \in \mathbb{Z}_m$ (где је $m = m_1 m_2 \cdots m_n$) за које је $f(x) = (r_1, r_2, ..., r_n)$. Но, с обзиром на дефиницију f, то заправо значи да је $x \equiv r_i \pmod{m_i}$ за $i = \{1, ..., n\}$, те је и $x \equiv x_i \pmod{m_i}$ за $i = \{1, ..., n\}$. Дакле, систем конгруенција има решење. Проверимо и јединственост решења. Нека је $x' \in \mathbb{Z}$ неки други цео број за који је $x' \equiv x_i \pmod{m_i}$ за $i = \{1, ..., n\}$. Добијамо да је $x \equiv x' \pmod{m_i}$ за $i = \{1, ..., n\}$. То значи да $m_i \mid (x - x')$ за $i = \{1, ..., n\}$. Како су m_i узајамно прости то даје: $m \mid (x - x')$, те је решење заиста јединствено по модулу m. □

Пример 35. За матрице $A = \begin{bmatrix} 15 & 17 & 12 \\ -3 & 5 & 6 \\ 0 & 2 & 14 \end{bmatrix}$ и $B = \begin{bmatrix} 33 & 60 & 12 \\ 10 & 13 & -27 \\ 18 & -20 & 31 \end{bmatrix}$

одредићемо $A + B$ и $A \cdot B$ у прстену $\mathbb{Z}_{30}$ користећи својство прстена

$$\mathbb{Z}_{30} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

тј. матричну верзију:

$$M_3(\mathbb{Z}_{30}) \cong M_3(\mathbb{Z}_2) \times M_3(\mathbb{Z}_3) \times M_3(\mathbb{Z}_5)$$

У $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5$ биће редом:

$$A_1 = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, A_2 = \begin{bmatrix} 0 & 2 & 0 \\ 0 & 2 & 0 \\ 0 & 2 & 2 \end{bmatrix}, A_3 = \begin{bmatrix} 0 & 2 & 2 \\ 2 & 0 & 1 \\ 0 & 2 & 4 \end{bmatrix}$$

$$B_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, B_2 = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, B_3 = \begin{bmatrix} 3 & 0 & 2 \\ 0 & 3 & 3 \\ 3 & 0 & 1 \end{bmatrix}$$

Производи матрица у $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5$ биће редом:

$$A_1 \cdot B_1 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}, A_2 \cdot B_2 = \begin{bmatrix} 2 & 2 & 0 \\ 2 & 2 & 0 \\ 2 & 1 & 2 \end{bmatrix}, A_3 \cdot B_3 = \begin{bmatrix} 1 & 1 & 3 \\ 4 & 0 & 0 \\ 2 & 1 & 0 \end{bmatrix}$$

Користећи Кинеску теорему о остацима формирамо системе из којих ћемо израчунати "непознате" елементе матрице

$$A \cdot B = \begin{bmatrix} \square & \square & \square \\ \square & \square & \square \\ \square & \square & \square \end{bmatrix}$$

Елемент са позиције 11 матрице $A \cdot B$ добићемо решавањем система добијеног помоћу елемената са позиција 11 из $A_1 \cdot B_1$, $A_2 \cdot B_2$ и $A_3 \cdot B_3$.

$$x \equiv 1 \pmod 2$$

$$x \equiv 2 \pmod 3$$

$$x \equiv 1 \pmod 5$$

Одакле следи:

$$x = 2q + 1$$

$$2q + 1 \equiv 2 \pmod 3$$

$$2q \equiv 1 \pmod 3 \quad / \cdot 2$$

$$q \equiv 2 \pmod 3$$

$$q = 3k + 2$$

$$x = 2 \cdot (3k + 2) + 1 = 6k + 5$$

$$6k + 5 \equiv 1 \pmod 5$$

$$6k \equiv -4 \pmod 5$$

$$k \equiv 1 \pmod 5$$

$$k = 5m + 1$$

$$x = 6 \cdot (5m + 1) + 5 = 30m + 11$$

$$x \equiv 11 \pmod{30}$$

Тако је

$$A \cdot B = \begin{bmatrix} 11 & \square & \square \\ \square & \square & \square \\ \square & \square & \square \end{bmatrix}$$

До истог закључка може се доћи и избором елемента који задовољава све три једначине система из скупа $\{1, 6, 11, 16, 21, 26\}$[1]. Зато ћемо други систем решити овим методом.

Елемент са позиције 21 матрице $A \cdot B$ добићемо решавањем система добијеног помоћу елемената са позиција 21 из $A_1 \cdot B_1$, $A_2 \cdot B_2$ и $A_3 \cdot B_3$.

$$x \equiv 1 \pmod 2$$
$$x \equiv 2 \pmod 3$$
$$x \equiv 4 \pmod 5$$

Скуп решења унутар кога се налази и решење датог система јесте $\{4, 9, 14, 19, 24, 29\}$, па је решење система:

$$x \equiv 29 \pmod{30}$$

Тако је

$$A \cdot B = \begin{bmatrix} 11 & \square & \square \\ 29 & \square & \square \\ \square & \square & \square \end{bmatrix}$$

Елемент са позиције 31 матрице $A \cdot B$ добићемо решавањем система добијеног помоћу елемената са позиција 31 из $A_1 \cdot B_1$, $A_2 \cdot B_2$ и $A_3 \cdot B_3$.

$$x \equiv 0 \pmod 2$$
$$x \equiv 2 \pmod 3$$
$$x \equiv 2 \pmod 5$$

Скуп решења унутар кога се налази и решење датог система јесте $\{2, 7, 12, 17, 22, 27\}$, па је решење система:

$$x \equiv 2 \pmod{30}$$

Тако се добија и последња вредност прве колоне матрице $A \cdot B$, тј.

$$A \cdot B = \begin{bmatrix} 11 & \square & \square \\ 29 & \square & \square \\ 2 & \square & \square \end{bmatrix}$$

На сличан начин, рачунањем са елементима одговарајућих позиција матрица $A_1 \cdot B_1$, $A_2 \cdot B_2$ и $A_3 \cdot B_3$, добијају се и сви остали елементи матрице $A \cdot B$.

[1]Елементи овог скупа су облика $p + k \cdot m \leq s,\ k \in \mathbb{N}_0$, где је први елемент p датог скупа остатак највећег модула m, и s модул по коме решавамо задати почетни систем.

Такође, до збира $A+B$ долази се аналогно, са разликом што се уместо производа у претходном излагању, посматра операција сабирања.

Глава 7

Системи једначина

У овом поглављу бавићемо се линеарним системима једначина над комутативним прстеном R.

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

Дати линеарни систем представља m једначина са n непознатих, коефицијентима a_{ij} и константама $b_1, b_2, ..., b_m$. Матрични облик датог система гласи

$$AX = B$$

где је $A = [a_{ij}] \in M_{m\times n}(R),\ B = [b_1, ..., b_m]^T \in R^m,\ X = [x_1, ..., x_n]^T \in (R[x_1, ..., x_n])^n$.

Систем једначина има решење ако постоји вектор $v \in R^n$ тако да важи $Av = B$. Ако је $B = 0$, тада се систем $AX = 0$ назива хомогени систем једначина. Хомогени систем једначина $AX = 0$ има најмање једно, тривијално решење $v = 0 = [0, ..., 0]^T \in R^n$. Нетривијално решење система $AX = 0$ је решење за које је $v \neq 0$ и $Av = 0$.

Теорема 10. (Крамерова теорема) Нека је $A \in M_n(R)$ и $\det A$ има инверзни елемент у R. Тада за свако $B = [b_1, ..., b_n]^T \in R^n$, једначина $AX = B$ има јединствено решење $v = [x_1, ..., x_n]^T$ где је

$$x_j = (\det A)^{-1} \cdot \det \begin{bmatrix} a_{11} & \cdots & a_{1j-1} & b_1 & a_{1j+1} & \cdots & a_{1n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & \cdots & a_{nj-1} & b_n & a_{nj+1} & \cdots & a_{nn} \end{bmatrix}$$

за свако $j = 1, ..., n$.

Доказ. Нека је $v = [x_1, ..., x_n]^T$, где је x_j дефинисано као у поставци теореме. Користећи Лапласов развој имамо

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

где је A_{ij} кофактор матрице A.

Дакле,

$$(\det A) \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \sum_{i=1}^{n} b_i A_{i1} \\ \vdots \\ \sum_{i=1}^{n} b_i A_{in} \end{bmatrix} = (\text{adj } A) \cdot B$$

Како је $(\det A)I = (\text{adj } A)A$ претходна једнакост постаје

$$(\text{adj } A)(Av) = (\text{adj } A)B$$

Такође adj A је инвертибилна матрица чији је инверз $(\det A)^{-1}A$ па одатле следи $Av = B$.

Претпоставимо да је v' још једно решење једначине $AX = B$. Тада је $Av' = Av = B$ па је $A(v - v') = 0$. Како је A инвертибилна матрица тада је $v - v' = 0$. Дакле v је јединствено решење једначине $AX = B$. □

Пример 36. Следећи систем једначина решићемо матричном методом у скупу Z_{14}.

$$x + y + z = 6$$
$$2x + y + 3z = 13$$
$$-x + 5y - 2z = 3$$

Матрични запис претходног система гласи:

$$\begin{bmatrix} 1 & 1 & 1 \\ 2 & 1 & 3 \\ -1 & 5 & -2 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 6 \\ 13 \\ 3 \end{bmatrix}$$

С обзиром да је $\mathbb{Z}_{14} \cong \mathbb{Z}_2 \times \mathbb{Z}_7$, тада дати систем решавамо у $\mathbb{Z}_2$ и $\mathbb{Z}_7$.

Дати систем решавамо у скупу $\mathbb{Z}_2$, па је тада:

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$$

До решења ћемо доћи користећи Крамерову теорему:

$$D = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix} = 1 \cdot \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} - 0 \cdot \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} + 1 \cdot \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = -1 \equiv_2 1$$

$$D_x = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix} = 1 \equiv_2 1$$

$$D_y = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix} = -2 \equiv_2 0$$

$$D_z = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} = 1 \equiv_2 1$$

Одређујемо вредности x, y, z :

$$D \cdot x = D_x$$
$$1 \cdot x \equiv_2 1$$
$$x \equiv_2 1$$

$$D \cdot y = D_y$$
$$1 \cdot y \equiv_2 0$$
$$y \equiv_2 0$$

$$D \cdot z = D_z$$
$$1 \cdot z \equiv_2 1$$
$$z \equiv_2 1$$

Полазни систем решавамо у скупу $\mathbb{Z}_7$, па је тада:

$$\begin{bmatrix} 1 & 1 & 1 \\ 2 & 1 & 3 \\ 6 & 5 & 5 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 6 \\ 6 \\ 3 \end{bmatrix}$$

Одакле следи да је:

$$x \equiv_7 1,\ y \equiv_7 2,\ z \equiv_7 3$$

Дакле, решења система по модулима су:

$$\mathbb{Z}_2 : \quad x = 1, y = 0, z = 1$$

$$\mathbb{Z}_7 : \quad x = 1, y = 2, z = 3$$

Из претходног облика одређујемо коначно решење система користећи Кинеску теорему о остацима:

$$x \equiv 1 \pmod 2$$

$$x \equiv 1 \pmod 7$$

Скуп решења унутар кога се налази и решење датог система јесте $\{1, 8\}$, па је решење система $x \equiv_{14} 1$.

$$y \equiv 0 \pmod 2$$

$$y \equiv 2 \pmod 7$$

Скуп решења унутар кога се налази и решење датог система јесте $\{2, 9\}$, па је решење система $y \equiv_{14} 2$.

$$z \equiv 1 \pmod 2$$

$$z \equiv 3 \pmod 7$$

Скуп решења унутар кога се налази и решење датог система јесте $\{3, 10\}$, па је решење система $z \equiv_{14} 3$.

Тако долазимо до коначног решења полазног система једначина у скупу $\mathbb{Z}_{14}$:

$$(x, y, z) = (1, 2, 3)$$

Пример 37. Следећи систем једначина решићемо матричном методом у скупу Z_{30}.

$$15x + 4y + 7z = 6$$

$$8x + 2y + 10z = 4$$

$$3x + 18y + 2z = 5$$

Матрични запис претходног система гласи:

$$\begin{bmatrix} 15 & 4 & 7 \\ 8 & 2 & 10 \\ 3 & 18 & 2 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 6 \\ 4 \\ 5 \end{bmatrix}$$

С обзиром да је $\mathbb{Z}_{30} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$, тада дати систем решавамо у $\mathbb{Z}_2$, $\mathbb{Z}_3$ и $\mathbb{Z}_5$.

Дати систем решавамо у скупу $\mathbb{Z}_2$, па је тада:

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

Одакле следи да је:

$$x = 1,\ y = t, t \in \mathbb{Z}_2, t \in \{0, 1\},\ z = -1 \equiv_2 1$$

Полазни систем решавамо у скупу $\mathbb{Z}_3$, па је тада:

$$\begin{bmatrix} 0 & 1 & 1 \\ 2 & 2 & 1 \\ 0 & 0 & 2 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}$$

Одакле следи да је:

$$x = -2 \equiv_3 1,\ y = -1 \equiv_3 2, z = 1$$

Полазни систем ћемо решити у скупу $\mathbb{Z}_5$, па је тада:

$$\begin{bmatrix} 0 & 4 & 2 \\ 3 & 2 & 0 \\ 3 & 3 & 2 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 1 \\ 4 \\ 0 \end{bmatrix}$$

У овом случају, до решења ћемо доћи користећи Крамерову теорему:

$$D = \begin{vmatrix} 0 & 4 & 2 \\ 3 & 2 & 0 \\ 3 & 3 & 2 \end{vmatrix} = 0 \cdot \begin{vmatrix} 2 & 0 \\ 3 & 2 \end{vmatrix} - 4 \cdot \begin{vmatrix} 3 & 0 \\ 3 & 2 \end{vmatrix} + 2 \cdot \begin{vmatrix} 3 & 3 \\ 2 & 3 \end{vmatrix} = -18 \equiv_5 2$$

$$D_x = \begin{vmatrix} 1 & 4 & 2 \\ 4 & 2 & 0 \\ 0 & 3 & 2 \end{vmatrix} = -4 \equiv_5 1$$

$$D_y = \begin{vmatrix} 0 & 1 & 2 \\ 3 & 4 & 0 \\ 3 & 0 & 2 \end{vmatrix} = -30 \equiv_5 0$$

$$D_z = \begin{vmatrix} 0 & 4 & 1 \\ 3 & 2 & 4 \\ 3 & 3 & 0 \end{vmatrix} = 51 \equiv_5 1$$

Одређујемо вредности x, y, z :

$$D \cdot x = D_x$$

$$2 \cdot x \equiv_5 1 \quad / \cdot 3$$
$$x \equiv_5 3$$

$$D \cdot y = D_y$$
$$2 \cdot y \equiv_5 0$$
$$y \equiv_5 0$$

$$D \cdot z = D_z$$
$$2 \cdot z \equiv_5 1 / \cdot 3$$
$$z \equiv_5 3$$

Дакле, решења система по модулима су:

$$\mathbb{Z}_2 : \quad x = 1, y = t, z = 1$$
$$\mathbb{Z}_3 : \quad x = 1, y = 2, z = 1$$
$$\mathbb{Z}_5 : \quad x = 3, y = 0, z = 3$$

Из претходног облика одређујемо коначно решење система користећи Кинеску теорему о остацима:

$$x \equiv 1 \pmod 2$$
$$x \equiv 1 \pmod 3$$
$$x \equiv 3 \pmod 5$$

Скуп решења унутар кога се налази и решење датог система јесте $\{3, 8, 13, 18, 23, 28\}$, па је решење система $x \equiv_{30} 13$.

$$y \equiv t \pmod 2, \quad t \in \{0, 1\}$$
$$y \equiv 2 \pmod 3$$
$$y \equiv 0 \pmod 5$$

Скуп решења унутар кога се налази и решење датог система јесте $\{0, 5, 10, 15, 20, 25, 30\}$, па је решење система $y \equiv_{30} 5$ или $y \equiv_{30} 20$.

$$z \equiv 1 \pmod 2$$
$$z \equiv 1 \pmod 3$$
$$z \equiv 3 \pmod 5$$

Скуп решења унутар кога се налази и решење датог система јесте $\{3, 8, 13, 18, 23, 28\}$, па је решење система $z \equiv_{30} 13$.

Тако долазимо до коначног решења полазног система једначина у скупу $\mathbb{Z}_{30}$:

$$(x, y, z) = (13, 5, 13)$$

$$(x, y, z) = (13, 20, 13)$$

Пример 38. Следећи систем једначина решићемо матричном методом у скупу Z_{21}.

$$3x + 2y + 2z = 1$$

$$2x + 3y + 2z = 0$$

$$2x + 2y + 3z = 0$$

Матрични запис претходног система гласи:

$$\begin{bmatrix} 3 & 2 & 2 \\ 2 & 3 & 2 \\ 2 & 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

С обзиром да је $\mathbb{Z}_{21} \cong \mathbb{Z}_3 \times \mathbb{Z}_7$, тада дати систем решавамо у $\mathbb{Z}_3$ и $\mathbb{Z}_7$. У скупу $\mathbb{Z}_3$, важи:

$$\begin{bmatrix} 0 & 2 & 2 \\ 2 & 0 & 2 \\ 2 & 2 & 0 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

Систем ћемо решити користећи Крамерову теорему.

$$D = \begin{vmatrix} 0 & 2 & 2 \\ 2 & 0 & 2 \\ 2 & 2 & 0 \end{vmatrix} \equiv_3 1$$

$$D_x = \begin{vmatrix} 1 & 2 & 2 \\ 0 & 0 & 2 \\ 0 & 2 & 0 \end{vmatrix} \equiv_3 2$$

$$D_y = \begin{vmatrix} 0 & 1 & 2 \\ 2 & 0 & 2 \\ 2 & 0 & 0 \end{vmatrix} \equiv_3 1$$

$$D_z = \begin{vmatrix} 0 & 2 & 1 \\ 2 & 0 & 0 \\ 2 & 2 & 0 \end{vmatrix} \equiv_3 1$$

Одређујемо вредности x, y, z :

$$D \cdot x = D_x$$
$$1 \cdot x \equiv_3 2$$
$$x \equiv_3 2$$

$$D \cdot y = D_y$$
$$1 \cdot y \equiv_3 1$$
$$y \equiv_3 1$$

$$D \cdot z = D_z$$
$$1 \cdot z \equiv_3 1$$
$$z \equiv_3 1$$

Дакле, решење система у $\mathbb{Z}_3$ је $x = 2, y = 1, z = 1$.
Полазни систем решавамо у скупу $\mathbb{Z}_7$, па је:

$$\begin{bmatrix} 0 & 2 & 2 \\ 2 & 0 & 2 \\ 2 & 2 & 0 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

Опет ћемо решити користећи Крамерову теорему.

$$D = \begin{vmatrix} 0 & 2 & 2 \\ 2 & 0 & 2 \\ 2 & 2 & 0 \end{vmatrix} \equiv_7 0$$

$$D_x = \begin{vmatrix} 1 & 2 & 2 \\ 0 & 0 & 2 \\ 0 & 2 & 0 \end{vmatrix} \equiv_7 5$$

$$D_y = \begin{vmatrix} 0 & 1 & 2 \\ 2 & 0 & 2 \\ 2 & 0 & 0 \end{vmatrix} \equiv_7 5$$

$$D_z = \begin{vmatrix} 0 & 2 & 1 \\ 2 & 0 & 0 \\ 2 & 2 & 0 \end{vmatrix} \equiv_7 5$$

Како је $D \cdot x = D_x$, добијамо $0 \cdot x \equiv_7 5$, из чега закључујемо да не постоји такво x, па и полазни систем **нема решења** у скупу $\mathbb{Z}_{21}$.

Пример 39. Следећи систем једначина решићемо матричном методом у скупу Z_{42}.

$$2x - 3y + z = 2$$
$$3x - 5y + 5z = 3$$
$$5x - 8y + 6z = 5$$

Матрични запис претходног система гласи:

$$\begin{bmatrix} 2 & -3 & 1 \\ 3 & -5 & 5 \\ 5 & -8 & 6 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \\ 5 \end{bmatrix}$$

С обзиром да је $\mathbb{Z}_{42} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_7$, тада дати систем решавамо у $\mathbb{Z}_2$, $\mathbb{Z}_3$ и $\mathbb{Z}_7$.

Дати систем решавамо у скупу $\mathbb{Z}_2$, па је тада:

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$$

Одакле следи да је:

$$x = 1,\ y = t,\ z = t,\ t \in \mathbb{Z}_2,\ t \in \{0, 1\}$$

Полазни систем решавамо у скупу $\mathbb{Z}_3$, па је тада:

$$\begin{bmatrix} 2 & 0 & 1 \\ 0 & 1 & 2 \\ 2 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 2 \\ 0 \\ 2 \end{bmatrix}$$

Систем ћемо решити користећи Крамерову теорему.

$$D = \begin{vmatrix} 2 & 0 & 1 \\ 0 & 1 & 2 \\ 2 & 1 & 0 \end{vmatrix} \equiv_3 0$$

$$D_x = \begin{vmatrix} 2 & 0 & 1 \\ 0 & 1 & 2 \\ 2 & 1 & 0 \end{vmatrix} \equiv_3 0$$

$$D_y = \begin{vmatrix} 2 & 2 & 1 \\ 0 & 0 & 2 \\ 2 & 2 & 0 \end{vmatrix} \equiv_3 0$$

$$D_z = \begin{vmatrix} 2 & 0 & 2 \\ 0 & 1 & 0 \\ 2 & 1 & 2 \end{vmatrix} \equiv_3 0$$

Како су све детерминанте нула, Гаусовом методом добићемо следећа решења:

$$(x, y, z) = (0, 2, 2)$$

$$(x, y, z) = (1, 0, 0)$$

$$(x, y, z) = (2, 1, 1)$$

Полазни систем ћемо решити у скупу $\mathbb{Z}_7$, па је тада:

$$\begin{bmatrix} 2 & 4 & 1 \\ 3 & 2 & 5 \\ 5 & 6 & 6 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \\ 5 \end{bmatrix}$$

Такође, $D = D_x = D_y = D_z = 0$, па Гаусовом методом добијамо:

$$(x, y, z) = (0, 0, 2)$$

$$(x, y, z) = (1, 0, 0)$$

$$(x, y, z) = (2, 0, 5)$$

$$(x, y, z) = (3, 0, 3)$$

$$(x, y, z) = (4, 0, 1)$$

$$(x, y, z) = (5, 0, 6)$$

$$(x, y, z) = (6, 0, 4)$$

У $\mathbb{Z}_2$ имамо 2 решења, у $\mathbb{Z}_3$ 3 решења, и у $\mathbb{Z}_7$ 7 решења, па решавањем система добијених њиховом комбинацијом, долазимо до решења система, којих је укупно $2 \cdot 3 \cdot 7 = 42$.

Нека од решења полазног система у скупу $\mathbb{Z}_{42}$ су:

$$(x, y, z) = (21, 14, 2)$$

$$(x, y, z) = (21, 14, 23)$$

$$(x, y, z) = (21, 14, 37)$$

$$(x, y, z) = (21, 35, 2)$$

$$(x, y, z) = (21, 35, 23)$$

$$(x, y, z) = (21, 35, 37)$$

Остала решења добијамо аналогно.

Пример 40. Следећи систем једначина са параметром $p \in \mathbb{Z}_{30}$ решићемо у скупу $\mathbb{Z}_{30}$

$$x + y - z = 1$$

$$2x + 3y + pz = 3$$

$$x + py + 3z = 2$$

На основу теореме о изоморфизму разлагања прстена следи:

$$\mathbb{Z}_{30} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

Дати систем решићемо у сваком од поља користећи Крамерову теорему.

У пољу $\mathbb{Z}_2$ дати систем прелази у:

$$x + y + z = 1$$

$$y + pz = 1$$

$$x + py + z = 0$$

Тада је

$$D = \begin{vmatrix} 1 & 1 & 1 \\ 0 & 1 & p \\ 1 & p & 1 \end{vmatrix} = p(1-p) \equiv_2 p(p+1)$$

$$D_x = \begin{vmatrix} 1 & 1 & 1 \\ 1 & 1 & p \\ 0 & p & 1 \end{vmatrix} = p(1-p) \equiv_2 p(p+1)$$

$$D_y = \begin{vmatrix} 1 & 1 & 1 \\ 0 & 1 & p \\ 1 & 0 & 1 \end{vmatrix} = p$$

$$D_z = \begin{vmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & p & 0 \end{vmatrix} = -p \equiv_2 p$$

Из $p(p+1) = 0$, с обзиром да смо у пољу, важи да је $p \equiv 0 \pmod 2$ или $p + 1 \equiv 0 \pmod 2$, тј. $p \equiv 1 \pmod 2$. Ако је $p \equiv 1 \pmod 2$, тада је $p = 2k + 1,\ k \leq 14$, па је

$$D = D_x = (2k+1)(2k+2) \equiv_2 0,\ D_y = D_z = 2k + 1 \equiv_2 1$$

Како је $D = 0$ и $D_y \neq 0$ према Крамеровој теореми, систем за дато $p = 2k + 1$ нема решења.

За $p \equiv 0 \pmod 2$, добијамо $D = D_x = D_y = D_z = 0$, па применом Гаусовог метода следи $(x, y, z) = (0, 1, 0),\ (x, y, z) = (1, 1, 1)$.

У пољу $\mathbb{Z}_3$ полазни систем прелази у:

$$x + y + 2z = 1$$
$$2x + pz = 0$$
$$x + py = 2$$

Тада је

$$D = \begin{vmatrix} 1 & 1 & 2 \\ 2 & 0 & p \\ 1 & p & 0 \end{vmatrix} = -p^2 + 5 \equiv_3 2p(1+p)$$

$$D_x = \begin{vmatrix} 1 & 1 & 2 \\ 0 & 0 & p \\ 2 & p & 0 \end{vmatrix} = -p^2 + 2p \equiv_3 2p(p+1)$$

$$D_y = \begin{vmatrix} 1 & 1 & 2 \\ 2 & 0 & p \\ 1 & 2 & 0 \end{vmatrix} = -p + 8 \equiv_3 2(p+1)$$

$$D_z = \begin{vmatrix} 1 & 1 & 1 \\ 2 & 0 & 0 \\ 1 & p & 2 \end{vmatrix} = 2p - 4 \equiv_3 2(p+1)$$

Ако је $2p(1+p) \equiv 0 \pmod 3$ тада је $p \equiv 0 \pmod 3$ или $p+1 \equiv 0 \pmod 3$, тј. $p \equiv 2 \pmod 3$. Ако је $p \equiv 0 \pmod 3$ тада је $D = D_x = 0$ и $D_y = D_z = 2(3k+1) = 2$, па дати систем нема решења. Ако је $p = 3k+1$, тада је $D = D_x = 2(3k+1)(3k+2) \equiv_3 1,\ D_y = D_z = 2(3k+2) \equiv_3 1$, па је решење $(x, y, z) = (1, 1, 1)$. И ако је $p \equiv 2 \pmod 3$, тада је $p = 3k+2,\ k \leq 9$, па је

$$D = D_x = D_y = D_z = 0$$

и применом Гаусовог метода закључујемо да је $(x, y, z) = (0, 1, 0),\ (x, y, z) = (1, 2, 2),\ (x, y, z) = (2, 0, 1)$.

У пољу $\mathbb{Z}_5$ полазни систем прелази у:

$$x + y + 4z = 1$$
$$2x + 3y + pz = 3$$
$$x + py + 3z = 2$$

Тада је

$$D = \begin{vmatrix} 1 & 1 & 4 \\ 2 & 3 & p \\ 1 & p & 3 \end{vmatrix} = -p^2 + 9p - 9 \equiv_5 (2p+1)^2$$

$$D_x = \begin{vmatrix} 1 & 1 & 4 \\ 3 & 3 & p \\ 2 & p & 3 \end{vmatrix} = -p^2 + 14p - 24 \equiv_5 (2p+1)^2$$

$$D_y = \begin{vmatrix} 1 & 1 & 4 \\ 2 & 3 & p \\ 1 & 2 & 3 \end{vmatrix} = -p + 7 \equiv_5 2(2p+1)$$

$$D_z = \begin{vmatrix} 1 & 1 & 1 \\ 2 & 3 & 3 \\ 1 & p & 2 \end{vmatrix} = -p + 2 \equiv_5 2(2p+1)$$

Ако је $p \equiv 0 \pmod 5$, тј. $p = 5k,\ k \leq 5$ тада је $D = D_x = (10k+1)^2 \equiv_5 1$ и $D_y = D_z = 2(10k+1) = 2$, па дати систем по Крамеровој теореми има решење $(x, y, z) = (1, 2, 2)$. Ако је $p = 5k+1$, тада је $D = D_x = (10k+3)^2 \equiv_5 4,\ D_y = D_z = 20k+6 \equiv_5 1$, па је $(x, y, z) = (1, 4, 4)$. За $p = 5k+2$ важи $(2p+1)^2 \equiv 0 \pmod 5$, па је $p \equiv 2 \pmod 5$, тј.

$$D = D_x = D_y = D_z = 0$$

и Гаусовом методом долазимо до решења $(x, y, z) = (0, 0, 4),\ (x, y, z) = (0, 1, 0),\ (x, y, z) = (0, 2, 1),\ (x, y, z) = (0, 3, 2),\ (x, y, z) = (0, 4, 3)$. За $p = 5k+3$, следи $D = D_x = (10k+7)^2 \equiv_5 4,\ D_y = D_z = 20k+14 \equiv_5 4$, па је $(x, y, z) = (1, 1, 1)$. На крају, за $p = 5k+4$, $D = D_x = (10k+10)^2 \equiv_5 1$ и $D_y = D_z = 20k+18 \equiv_5 3$, па дати систем по Крамеровој теореми има решење $(x, y, z) = (1, 3, 3)$.

Комбиновањем свих могућих решења из $\mathbb{Z}_2$, $\mathbb{Z}_3$ и $\mathbb{Z}_5$ добијамо коначна решења система у $\mathbb{Z}_{30}$.

С обзиром да у $\mathbb{Z}_2$ имамо 2 решења, у $\mathbb{Z}_3$ 4 решења, и у $\mathbb{Z}_5$ 9 решења, њиховом комбинацијом, и применом Кинеске теореме добићемо $2 \cdot 4 \cdot 9 = 72$ решења.

Да резимирамо: вредност параметра p припада скупу $\{0, 1, 2, ..., 29\}$. Ако избацимо све вредности за које неки од система у $\mathbb{Z}_2, \mathbb{Z}_3$ или $\mathbb{Z}_5$ нема решења,тј. све вредности које задовољавају $p = 2k+1$ и $p = 3k$, дати скуп се своди на

$$\{\not{0}, \not{1}, 2, \not{3}, 4, \not{5}, \not{6}, \not{7}, 8, \not{9}, 10, \not{11}, \not{12}, \not{13}, 14, \not{15}, 16, \not{17}, \not{18}, \not{19}, 20, \not{21}, 22, \not{23}, \not{24}, \not{25}, 26, \not{27}, 28, \not{29}\}$$

За дате вредности параметра $p \in \{2, 4, 8, 10, 14, 16, 20, 22, 26, 28\}$, систем има решење, а за преостале вредности параметра p нема решења у $\mathbb{Z}_{30}$.

Глава 8

Закључак

Рад *Матрице над* $\mathbb{Z}_n$ садржи доста примера који би подстакли ученике да истражују и закључују о разним алгебарским појмовима.

Надам се да ће овај рад бити користан свима које интересује ова проблематика. Такође, верујем да ће бити посебно занимљив ученицима гимназија, и да ће бити примамљиво штиво за додатну наставу математике.

Глава 9

Литература

1. Петровић, Зоран, Алгебра 1, Предавања за школску 2014/15. годину, Математички факултет, Београд.

2. Петровић, Зоран, Алгебра 2, Предавања за школску 2014/15. годину, Математички факултет, Београд.

3. Thomas W. Hungerford, Algebra, Cleveland State University, USA, 1974.

4. William C. Brown, Matrices over commutative rings, Michigen State University East Lansing, Michigan, 1993.