Mai întâi, continuarea exerciţiului despre idealele bilaterale din inelele de matrici.

1. Fie R un inel şi n un număr natural nenul. Idealele bilaterale ale inelului $\mathcal{M}_n(R)$ sunt de forma $\mathcal{M}_n(I)$, unde I este ideal bilateral al lui R. Pentru un astfel de ideal, avem că $\frac{\mathcal{M}_n(R)}{\mathcal{M}_n(I)} \simeq \mathcal{M}_n(\frac{R}{I})$. Această caracterizare este valabilă doar pentru idealele bilaterale.

Soluţie. E clar că, pentru orice $I \in \mathcal{I}d_b(R)$, $\mathcal{M}_n(I)$ e în $\mathcal{I}d_b(\mathcal{M}_n(R))$. Trebuie să vedem că această construcţie naturală umple întregul $\mathcal{I}d_b(\mathcal{M}_n(R))$ (comportamentul bun al "funcţiei" $\mathcal{M}_n$ faţă de subobiecte). Fie $\mathcal{I}$ un ideal bilateral din $\mathcal{M}_n(R)$. Cine să fie acel $I \in \mathcal{I}d_b(R)$ astfel încât $\mathcal{M}_n(I) = \mathcal{I}$? Spuneam că o primă idee este să luăm I drept mulţimea tuturor elementelor din R ce apar ca intrări în matricele din $\mathcal{I}$. Trebuie însă ţinut cont de naturaleţe: încă o dată, problema e la nivel de subobiecte, deci este în cadrul trecerii *naturale* de la $\mathcal{I}d_b(R)$ la $\mathcal{I}d_b(\mathcal{M}_n(R))$, iar pentru a găsi acel I cu $\mathcal{M}_n(I) = \mathcal{I}$ va trebui să ne uităm la nivelul elementelor, iar acolo trecerea *naturală* este $R \to \mathcal{M}_n(R)$, $r \mapsto \begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix}$. Astfel, vom considera $I = \{r \in R;$ există $A = (a_{ij})_{i,j} \in \mathcal{I}$ aşa încât $a_{11} = r\}$. Am văzut că I e ideal bilateral al lui R. Fie $A \in \mathcal{M}_n(I)$, $A = (a_{ij})_{i,j}$. Scriem $A = \sum_{1 \le i,j \le n} a_{ij}e_{ij}$ şi arătăm că $a_{ij}e_{ij} \in \mathcal{I}$, oricare ar fi $1 \le i, j \le n$. Fie, deci, i, j fixaţi, oarecare. Deoarece $a_{i,j} \in I$, există $A^{(ij)} \in \mathcal{I}$ aşa încât $a_{11}^{(ij)} = a_{ij}$, unde $A^{(ij)} = (a_{kl}^{(ij)})_{k,l}$. Pentru a extrage $a_{ij}e_{ij}$, înmulţim pe $A^{(ij)}$ la stânga cu e_{i1} şi la dreapta cu e_{1j} (aşa cum scoatem coordonatele în raport cu o bază ortonormată cu ajutorul unui produs scalar). Avem

$$\mathcal{I} \ni e_{i1}A^{(ij)}e_{1j} = e_{i1}(\sum_{k,l} a_{kl}^{(ij)}e_{kl})e_{1j} = e_{i1}\sum_{k,l} a_{kl}^{(ij)}\delta_{l1}e_{kj} = \sum_k a_{k1}^{(ij)}e_{i1}e_{kj} =$$
$$\sum_k a_{k1}^{(ij)}\delta_{1k}e_{ij} = a_{11}^{(ij)}e_{ij} = a_{ij}e_{ij}$$

Astfel, $A \in \mathcal{I}$, şi deci $\mathcal{M}_n(I) \subset \mathcal{I}$. Invers, fie $A = (a_{ij}) \in \mathcal{I}$ şi $1 \le i, j \le n$ oarecare, fixaţi. Vrem $a_{ij} \in I$, *i.e.* să găsim o matrice din $\mathcal{I}$ ce are a_{ij} pe poziţia $(1, 1)$. Avem (de data asta permutăm indicii ca să deplasăm a_{ij} pe o primă poziţie)

$$\mathcal{I} \ni e_{1i}Ae_{j1} = a_{ij}e_{11},$$

şi deci $a_{ij} \in I$. Aşadar, avem şi că $\mathcal{I} \subset \mathcal{M}_n(I)$.
Încă o precizare. Totuşi, de ce ne-am aştepta să şi funcţioneze acel I?

Adică să meargă treaba pivotând doar pe prima poziţie (sau, mai bine zis, doar pe o singură intrare, alegerea poziţiei $(1,1)$ fiind neesenţială): ne gândim, în acest sens, la aşa - numitele transformări elementare ale matricelor şi la faptul că situaţia de aici e invariantă la expresii conjugate (tocmai pentru că lucrăm cu ideale bilaterale!)...
Acum vedem că, într-adevăr, această construcţie nu mai e completă pentru ideale strângi, *i.e.* nu orice ideal stâng din $\mathcal{M}_n(R)$ e de forma $\mathcal{M}_n(I)$ cu I ideal stâng în R. Spre exemplu, fie $\mathcal{I} = \{\begin{pmatrix} * & 0 \\ * & 0 \end{pmatrix}\}_{*\in R}$. E clar că $\mathcal{I}$ e ideal stâng în $\mathcal{M}_n(R)$ (dar nu şi bilateral: înmulţiţi la dreapta matricea $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ cu $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ (totdeauna inelele sunt presupuse unitare, cu $1 \neq 0$)) şi că $\mathcal{I}$ nu e de forma $\mathcal{M}_n(I)$ cu I ideal stâng al lui R.
În fine, izomorfismul cerut e dat de morfismul canonic $\pi : R \to \frac{R}{I}$: avem morfismul indus, $\overline{\pi} : \mathcal{M}_n(R) \to \mathcal{M}_n(\frac{R}{I})$, $(a_{ij})_{i,j} \mapsto (\pi(a_{ij}))_{i,j}$, iar $ker(\overline{\pi}) = \mathcal{M}_n(I)$ şi aplicăm teorema fundamentală de izomorfism ($\overline{\pi}$ e surjectivă, π fiind astfel).

2. Fie k un corp si $E \in \mathcal{M}_n(k)$. Atunci E e divizor al lui zero dacă şi numai dacă E nu este inversabilă. Echivalenţa cade în cazul în care k nu mai e corp.

Soluţie. Şi aici e un raţionament de spaţii vectoriale. Necesitatea e evidentă. Presupunem că nu există E^{-1}. Atunci fie $E_1, \ldots, E_n$ liniile matricei E; privim E_i-urile precum vectori în k - spaţiul vectorial k^n. Deoarece $det(E) = 0$, rezultă că există $r_1, \ldots, r_n$ din R, nu toţi nuli, aşa încât $\sum_i r_i E_i = 0$ (ne amintim criteriul matriceal de liniar independenţă a unui sistem de vectori: vectorii $v_1, \ldots, v_n$ sunt liniar independenţi dacă matricea asociată lor are rang maxim). Atunci considerăm matricea $F \in \mathcal{M}_n(k)$ ale cărei linii sunt $F_1 = (r_1, \ldots, r_n)$ şi $F_i = (0, \ldots, 0)$ pentru $2 \leq i \leq n$. Avem că $FE = 0$ şi $F \neq 0$ (direct din construcţie).
Într-adevăr, dacă inelul intrărilor nu mai e corp, rezultatul nu mai are loc: de exemplu, dacă $k = \mathbb{Z}$, atunci $2I_n \in \mathcal{M}_n(\mathbb{Z})$ nu e element inversabil, dar nu e divizor al lui zero.

Deşi există divizori ai lui zero în inelele de matrici, ne putem convinge că nu sunt foarte mulţi. Încercaţi aşa: priviţi $\mathcal{M}_n(k)$ ca spaţiu topologic (să zicem $k = \mathbb{C}$) şi apoi vedeţi că submulţimea matricelor neinversabile e un închis (găsiţi o funcţie continuă aşa încât submulţimea noastră să fie preimaginea unui închis prin acea funcţie), deci cele inversabile formează un deschis. Acum amintiţi-vă o topologie în care deschişii erau mari (vom relua discuţia asta şubredă faţă în faţă).

Trecem la corpuri. Aceasta structură e fundamentală căci încarnează ideea de sistem numeric. Printre aceste sisteme numerice distingem anumite clase: acele corpuri care oferă un cadru pentru a face geometrie şi analiză (mediile continue), anume $\mathbb{R}$ şi $\mathbb{C}$, apoi discretizările acestora, anume corpurile finite $\mathbb{F}_{p^n}$, şi,alta clasa, corpurile aritmetice, anume cele ce stau între $\mathbb{Q}$ şi $\mathbb{C}$, precum corpurile ciclotomice $\mathbb{Q}(\omega)$ sau cele pătratice $\mathbb{Q}(\sqrt{d})$ (am discutat despre ele). Mai există şi alte tipuri de corpuri, iar toate aceste tipuri sunt profund legate prin raţiunile geometriei algebrice; altfel spus, via scopul primordial de a rezolva ecuaţii. Cu care tip de corpuri să începem? Cu acelea care par cele mai simple, bineînţeles: corpurile finite. Însă trebuie să înţelegem că, pentru noi, ceea ce primează nu ţine de simplitatea conchisă la modul direct şi superficial (în cazul de faţă, am spune că $\mathbb{F}_{p^n}$ e cel mai abordabil tip pentru că pur şi simplu e finit) ci mai degrabă ţine de ceea ce apare cel mai aproape de simţurile noastre: intuiţia e în primul rând legată de mediul continuu! Astfel, $\mathbb{R}$ şi $\mathbb{C}$ constituie startul (de menţionat că din punctul de vedere al algebrei pure, discuţia de până acum e de prisos pentru că atunci când zicem *corp* ne gândim la toate deodată şi dezvoltăm teoria cât de mult se poate).

Primele încercări de a efectua raţionamente din cadrul fiecărui tip de corp menţionat mai sus (deci de a pune într-o primă lumină legăturile) au aparţinut unui singur om: Gauss. Iată un exemplu (referitor la situaţia $\mathbb{R} \subset \mathbb{C}$):

Teorema fundamentală a algebrei. Orice ecuaţie polinomială $a_0 + a_1X + a_2X^2 \ldots + a_nX^n = 0$ cu $a_i \in \mathbb{C}$ oricare ar fi i, are exact n soluţii în $\mathbb{C}$ (numărate cu multiplicităţi).

Am discutat puţin despre acest rezultat (vom reveni asupra poveştii din spatele lui; dacă nu, vă veţi lămuri în anii II şi III).

În discuţia de până acum, totul a fost gândit în cadrul comutativ. Următorul exerciţiu arată că avem parte de schimbări violente atunci când pierdem comutativitatea.

3. Fie $\mathbb{H}$ corpul cuaternionilor. Atunci ecuaţia $X^2+1=0$ are o infinitate de soluţii în $\mathbb{H}$.

Soluţie. Vedem $\mathbb{H}$ sub formă matriceală:

$$\mathbb{H}=\{\begin{pmatrix} z & w \\ -\overline{w} & \overline{z}\end{pmatrix}; z,w\in\mathbb{C}\}.$$

Fie şi unităţile imaginare $I=\begin{pmatrix} i & 0 \\ 0 & -i\end{pmatrix}$, $J=\begin{pmatrix} 0 & 1 \\ -1 & 0\end{pmatrix}$, $K=\begin{pmatrix} 0 & i \\ i & 0\end{pmatrix}$; deci oricare ar fi $Q\in\mathbb{H}$, avem $Q=a_0I_2+a_1I+a_2J+a_3K$ cu $a_0,a_1,a_2,a_3\in\mathbb{R}$ ($\{I_2,I,J,K\}$ e baza canonică a $\mathbb{R}$ - spaţiului vectorial $\mathbb{H}$). Precum în $\mathbb{C}$, pentru orice $Q=a_0I_2+a_1I+a_2J+a_3K$ avem conjugatul său $\overline{Q}=a_0I_2-a_1I-a_2J-a_3K$, precum şi norma sa $|Q|=Q\overline{Q}$ (aceasta e doar funcţia modul specifică acestui sistem numeric; ca orice normă, e multiplicativă: $|aQ|=|a||Q|$ oricare ar fi $a\in\mathbb{R}$ şi $Q\in\mathbb{H}$, iar $|\cdot|$ nu vede lipsa comutativităţii, *i.e.* $|Q_1Q_2|=|Q_2Q_1|$ oricare ar fi $Q_1,Q_2\in\mathbb{H}$; de fapt, $|Q_1Q_2|=|Q_1||Q_2|$ căci $|Q|$ e doar o deghizare a determinantului: $|Q|=det(Q)I_2$).
Acum fie $Q\in\mathbb{H}$ aşa încât $Q^2+1=0$. Deoarece vedem $\mathbb{H}$ în context matriceal, asta înseamnă că $Q^2=-I_2$, $Q=a_0I_2+a_1I+a_2J+a_3K$ pentru nişte $a_0,a_1,a_2,a_3\in\mathbb{R}$. Luând determinantul, obţinem $(det(Q))^2=det(Q^2)=det(-I_2)=1$. Dar $det(Q)=a_0^2+a_1^2+a_2^2+a_3^2\geq 0$ (avem $Q=\begin{pmatrix} z & w \\ -\overline{w} & \overline{z}\end{pmatrix}$, unde $z=a_0+a_1i$ şi $w=a_2+a_3i$, deci $det(Q)=|z|^2+|w|^2$), de unde $det(Q)=1$, *i.e.* $|Q|=I_2$. Tot din $Q^2=-I_2$ obţinem şi că $Q^2\overline{Q}=-\overline{Q}$, sau $Q|Q|=-\overline{Q}$ sau $Q=-\overline{Q}$, de unde $a_0=0$ şi deci $Q=a_1I+a_2J+a_3K$.
Aşadar, dacă e să existe, orice soluţie din $\mathbb{H}$ a ecuaţiei $X^2+1=0$ e de forma $\alpha I+\beta J+\gamma K$, cu $\alpha^2+\beta^2+\gamma^2=1$. De fapt, acestea sunt toate (ca să vă convingeţi că orice astfel de cuaternion e soluţie, nu aveţi decât să urmaţi drumul invers din raţionamentul anterior) şi e clar că sunt în număr infinit: sunt punctele de pe sfera S^2!

E de aşteptat să avem o infinitate de soluţii în $\mathbb{H}$ pentru ecuaţia $X^2+1=0$. Pentru a vedea acest lucru, trebuie să schimbăm percepţia algebrică asupra lui $\mathbb{H}$ (cea matriceală, ca în exerciţiu) cu una geometrică. În acest scop, ne întoarcem la numerele complexe. Înmulţirea a două numere complexe poate fi privită ca operaţie între două rotaţii

în plan (formula de Moivre). Atunci încerăm să privim un cuaternion $Q \in \mathbb{H}$ precum un soi de vector $q = a_0 + \overrightarrow{v}$ unde a_0 e partea scalară (ce vine din $\mathbb{R}$) şi $\overrightarrow{v} = a_1 \overrightarrow{i} + a_2 \overrightarrow{j} + a_3 \overrightarrow{k}$ e partea vectorială (ce vine din $\mathbb{R}^3$) şi deci am putea defini înmulţirea acestora folosind rotaţiile din spaţiu (de precizat că lucrurile nu stau chiar aşa; doar intuitiv vorbim). Peste $\mathbb{C}$, ecuaţia $X^2 = -1$ are două soluţii pentru că avem doar două sensuri de mişcare (de rotaţie) pe S^1. Atunci, deoarece pe S^2 avem o infinitate de sensuri, ne aşteptăm să avem o infinitate de elemente din $\mathbb{H}$ care să satisfacă $X^2 = -1$.

Realizez că din discuţia de la început reiese că nu vom vorbi despre corpuri finite, însă o foarte scurtă privire trebuie aruncată şi asupra lor: e locul unde trăieşte un morfism crucial de care trebuie să fim conştienţi.
Fie k un corp finit (există astfel de corpuri: $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, de exemplu). Deoarece elementele 0, 1, $1+1$, $1+1+1$, ... nu pot fi toate diferite (k e finit), trebuie să avem $char(k) = p \neq 0$ (trebuie să fie prim datorită minimalităţii); deci corpul prim al lui k este $\mathbb{F}_p$. Aici avem:

Teoremă (WEDDERBURN) Orice corp finit e comutativ.

E dificil de explicat de ce trebuie să avem comutativitate. În orice caz, explicaţia sigur nu stă doar în faptul că avem un număr finit de elemente (vezi grupul Q_8 al cuaternionilor). Mai degrabă, explicaţia stă în nişte motive de simetrie: "$S^1 = lim_{n\to\infty} \mathbb{Z}/n\mathbb{Z} = lim_{n\to\infty} \mu_n$", unde μ_n e grupul rădăcinilor de ordin n ale unităţii din $\mathbb{C}$ (μ_n - urile aproximează cercul). Dar sunt elementele unui corp finit nişte rădăcini ale unităţii? Fie k un astfel de corp. Am văzut că $\mathbb{F}_p \subset k$, unde $p = char(k)$ şi deci k poate fi privit ca $\mathbb{F}_p$ - spaţiu vectorial. Atunci fie $n = dim_{\mathbb{F}_p} k$; fie şi $q = \#k$ (cardinalul lui k). Observăm că $q = p^n$ (q e tot una cu numărul alegerilor de vectori cu n componente peste $\mathbb{F}_p$: $k \simeq \mathbb{F}_p \times \ldots \times \mathbb{F}_p$ (de n ori) ca şi spaţii vectoriale). Apoi, grupul $k^* = k \setminus \{0\}$ (partea multiplicativă subiacentă corpului k) are $q-1$ elemente şi fie $x \in k^*$ oarecare. Atunci $ord(x)$ divide $q-1$ (teorema lui Lagrange) şi deci $x^{q-1} = 1$. Astfel, $x^q - x = 0$ pentru orice $x \in k$ (inclusiv 0). Cum numărul de rădăcini ale polinomului $X^q - X \in \mathbb{F}_p[X]$ nu depăşeşte q, "vedem" astfel cine este k (aşa cum $\mathbb{R}$ se poate completa algebric la $\mathbb{C}$, şi pentru $\mathbb{F}_p$ există un astfel de completat, notat $\overline{\mathbb{F}_p}$ şi numit închiderea algebrică a lui $\mathbb{F}_p$ - ca să-l obţinem punem laolaltă toate rădăcinile tuturor polinoamelor cu coeficienţi în $\mathbb{F}_p$). Acest k se

notează $\mathbb{F}_{p^n}$.

4. Fie k un corp comutativ, $char(k) = p > 0$. Se consideră aplicaţia $\varphi : k \longrightarrow k$ dată prin $\varphi(x) = x^p$.
(a) φ este endomorfism de inel al lui k, numit morfismul Frobenius.
(b) Dacă k e corp finit, atunci φ e automorfism.

Soluţie. (a) Evident, $\varphi(xy) = \varphi(x)\varphi(y)$ (k e comutativ). Avem şi $\varphi(x + y) = \varphi(x) + \varphi(y)$, oricare ar fi $x, y \in k$, pentru că

$$\varphi(x + y) = (x + y)^p = \sum_{i=0}^{p} \binom{p}{i} x^{p-i} y^i,$$

iar $\binom{p}{i} = \frac{p!}{(p-i)!i!}$ se divide cu p atunci când $i \neq 0, p$ şi deci $\binom{p}{i} = 0$ în k pentru $i \neq 0, p$ ($char(k) = p$).
(b) În general, φ e injectiv (fără ideale netriviale aici), iar dacă k e mulţime finită, φ e automat şi surjectiv. (Verificaţi)

În cazul în care corpul k e $\mathbb{F}_q$, morfismul Frobenius se notează φ_q. Importanţa acestor morfisme provine din faptul că soluţiile din $\mathbb{F}_q$ ale unor ecuaţii precum $Y^2 - aX - b = 0$ sunt exact punctele fixe ale aplicaţiei ce duce punctul de coordonare (x, y) în punctul $(\varphi_q(x), \varphi_q(y))$ - remarca lui Hasse!

Observaţia anterioară relevă partea bună (şi foarte importantă), însă să remarcăm şi partea nu prea fericită: din moment ce ne reducem peste un corp finit (aşa cum ne reducem de la $\mathbb{Z}$ peste $\mathbb{Z}/p\mathbb{Z}$ atunci când avem de rezolvat o ecuaţie în $\mathbb{Z}$), pierdem din informaţia operaţiilor algebrice: $(x+y)^p = x^p + y^p$! Cum remediem situaţia? Răspuns: inelul vectorilor Witt... Aici nu mai intrăm în amănunte. Suficient e să ştiţi că $\mathbb{F}_q$ - urile apar ca reducţii ale altor tipuri de corpuri, numite corpuri p-adice ($\mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C} \hookrightarrow \ldots$ nu e singurul drum!), care la rândul lor sunt "variantele locale" ale corpurilor aritmetice dintre $\mathbb{Q}$ şi $\mathbb{C}$ (cum ziceam la început, toate sunt intim legate): dacă ne liftăm la aceste sisteme p-adice, recuperăm informaţia.