III.C. Matrix rings

Let R be a *commutative* ring; then a matrix $A = \sum_{i,j=1}^{n} a_{ij}\mathbf{e}_{ij} \in M_n(R)$ has a **determinant**:

III.C.1. DEFINITION. $\det(A) := \sum_{\sigma\in\mathfrak{S}_n} \mathrm{sgn}(\sigma)\prod_{i=1}^{n} a_{i,\sigma(i)} \in R$.

As immediate consequences of this definition,

$$\det \text{ is } \textit{alternating} \text{ and } \textit{multilinear}$$

in the columns $\{\underline{a}_j\}$ of A, viewed as elements of R^n:

(III.C.2)
$$\begin{cases} \text{(i)} \quad \det(\underline{a}_1,\ldots,r\underline{a}_k+r'\underline{a}_k',\ldots,a_n) & = \quad r\det(\underline{a}_1,\ldots,\underline{a}_k,\ldots,\underline{a}_n) \\ & \qquad\qquad +r'\det(\underline{a}_1,\ldots,\underline{a}_k',\ldots,\underline{a}_n) \\ \text{(ii)} \quad \det(\underline{a}_1,\ldots,\underline{a}_k,\ldots,\underline{a}_\ell,\ldots,\underline{a}_n) & = \quad -\det(\underline{a}_1,\ldots,\underline{a}_\ell,\ldots,\underline{a}_k,\ldots,\underline{a}_n) \\ \text{(iii)} & = \quad 0 \ \text{ if } \underline{a}_k=\underline{a}_\ell. \end{cases}$$

(Note that if $2|\mathrm{char}(R)$, then (iii) does not follow from (ii), but it follows directly from III.C.1.) Moreover, since $\mathrm{sgn}(\sigma^{-1})=\mathrm{sgn}(\sigma)$,

$$\det({}^tA)=\det(A) \quad\Longrightarrow\quad \text{(III.C.2) holds for } \textit{rows}.$$

This means that the **elementary row operations (EROs)**

$$\text{(III.C.3)} \quad \begin{cases} \text{(I)} & \text{adding } r \text{ times the } j\text{th row } (r\in R) \text{ to the } i\text{th row} \\ \text{(II)} & \text{swapping } i\text{th and } j\text{th rows} \\ \text{(III)} & \text{multiplying the } i\text{th row by } r\ (r\in R^*), \end{cases}$$

which are invertible, have the following effects on $\det(A)$: none; multiply by -1; multiply by r (respectively). EROs correspond to multiplying A on the left by the **elementary matrices**

$$\text{(III.C.4)} \quad \begin{cases} & \underline{\text{elementary matrix}} & \underline{\det} \\ \text{(I)} & \mathbb{1}+r\mathbf{e}_{ij} & 1 \\ \text{(II)} & \mathbb{1}+\mathbf{e}_{ij}+\mathbf{e}_{ji}-\mathbf{e}_{ii}-\mathbf{e}_{jj} & -1 \\ \text{(III)} & \mathbb{1}+(r-1)\mathbf{e}_{ii} & r. \end{cases}$$

When R is a field, such as $\mathbb{R}$ (as in the standard linear algebra course), EROs can be used to put A into a unique **reduced row echelon form**:

$$\text{(III.C.5)}\qquad \begin{cases} \bullet \text{ each row has a ``leading 1'' as its first nonzero entry} \\ \bullet \text{ in row } j\text{, this occurs in the } \mu(j)^{\text{th}} \text{ entry, where } \mu \text{ is} \\ \qquad \text{a strictly increasing } \mathbb{Z}_{>0}\text{-valued function} \\ \bullet \text{ for each } j\text{, all entries in the } \mu(j)^{\text{th}} \text{ column are zero,} \\ \qquad \text{except for the leading 1.} \end{cases}$$

(If $\mu(j) > n$, the j^{th} row is zero.) The resulting matrix

$$\text{(III.C.6)}\qquad \operatorname{rref}(A) = \underbrace{E_N \cdots E_1}_{\text{as in (III.C.4)}} A$$

is either $\mathbb{1}$ or has last row $\underline{0}$. Moreover, by (III.C.3)-(III.C.4) it is clear that

$$\text{(III.C.7)}\qquad \det(\operatorname{rref}(A)) = \left(\prod_{i=1}^N \det(E_i)\right) \det(A).$$

Since the $\det(E_i) \neq 0$ and the E_i are invertible, this yields the

III.C.8. PROPOSITION. *When R is a field,*

$$\det(A) \neq 0 \iff \operatorname{rref}(A) = \mathbb{1} \iff A \textit{ is invertible}.$$

It also gives a way to compute the inverse: assuming $\operatorname{rref}(A) = \mathbb{1}$,

$$\text{(III.C.9)}\qquad E_N \cdots E_1 (\underbrace{A \mid \mathbb{1}}_{n\times 2n}) = (\underbrace{E_N \cdots E_1 A}_{\mathbb{1}} \mid \underbrace{E_N \cdots E_1}_{A^{-1}}),$$

i.e. computing $\operatorname{rref}(A \mid \mathbb{1})$ gives $(\mathbb{1} \mid A^{-1})$. Moreover, (III.C.9) shows that any matrix B with nonzero determinant is a product of elementary matrices $\prod_{i=1}^M E_i$, and so by (III.C.3)-(III.C.4) we get that first $\det(B) = \prod_{i=1}^M \det(E_i)$ then

$$\text{(III.C.10)}\qquad \det(BC) = \det(B)\det(C),$$

arguing by induction on M.

Turning to the next level of generality, suppose that R is a Euclidean domain. To produce an analogue of the rref, find the nonzero entry b in the first (nonzero) column with the lowest $\delta(b)$, then apply

$a = bq + r$ to the other entries in that column and use a type (I) ERO to kill the bq's. Repeat this step on the column until all but one entry is zero; swap it to the top position. Restricting to the $(n-1)\times n$ submatrix below the first row, we repeat the algorithm to arrive at

$$\left(\begin{array}{c|c} \begin{matrix} 0 \cdots 0 & r_1 & * \cdots * & s \\ 0 & \cdots\cdots\cdots & 0 & r_2 \end{matrix} & \\ \hline \Large 0 & \Large ? \end{array}\right)$$

where by a type (I) ERO together with the Euclidean algorithm we can assume $\delta(s) < \delta(r_2)$. Using type (I) and (II) EROs, we eventually produce a matrix in **Hermite normal form**

(III.C.11)

$$\mathrm{Herm}(A) = (\alpha_{ij}) = \begin{pmatrix} 0\cdots 0 \;\; \alpha_{1,\mu(1)} \;\; * \cdots * \;\; \alpha_{1,\mu(2)} \;\; * \cdots * & \alpha_{1,\mu(3)} & \\ 0 \;\cdots\cdots\cdots\cdots\cdots\; 0 \;\; \alpha_{2,\mu(2)} \;\; * \cdots * & \alpha_{2,\mu(3)} & \text{etc.} \\ 0 \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots 0 & \alpha_{3,\mu(3)} & \\ \vdots & & \end{pmatrix}$$

where $\delta(\alpha_{i,\mu(j)}) < \delta(\alpha_{j,\mu(j)})$ for all $i < j$, and all entries below the diagonal are 0. Clearly we still have (by (III.C.3)-(III.C.4)) that

$$\text{(III.C.12)} \qquad \begin{cases} \mathrm{Herm}(A) = E_N \cdots E_1 A \\ \det(\mathrm{Herm}(A)) = \left(\prod_i \det(E_i)\right)\det(A) \end{cases}$$

where $\prod_i \det(E_i) \in R^*$, and so

(III.C.13)

$$\det(A) \neq 0 \iff \underbrace{\det(\mathrm{Herm}(A))}_{=\prod_{i=1}^n \alpha_{ii}} \neq 0 \iff \mu(j) = j \;(\forall j).$$

Assume the $\alpha_{ii} \neq 0$ $(\forall i)$. We need the following

III.C.14. LEMMA. $\prod_{i=1}^n \alpha_{ii} \in R^* \iff \alpha_{ii} \in R^* \;(\forall i)$.

PROOF. If $n = 2$, then this says that $rs \in R^* \iff r, s \in R^*$. Suppose $rs = u \in R^*$; then u^{-1} exists, and $r(su^{-1}) = 1 \implies r \in R^*$. Now induce on n. $\square$

Putting this all together,

$$\det(A) \in R^* \underset{\text{(III.C.12)}}{\iff} \det(\mathrm{Herm}(A)) \in R^*$$
$$\underset{\text{(III.C.13)}}{\iff} \prod \alpha_{ii} \in R^* \underset{\text{(III.C.14)}}{\iff} \alpha_{ii} \in R^* \ (\forall i).$$

But if the $\alpha_{ii} \in R^*$, we may (if necessary) kill all the off-diagonal entries (by type (I) EROs) and scale the diagonal ones to 1 (by type (III) EROs). Since elementary matrices are invertible, we arrive at the

III.C.15. THEOREM. *For R Euclidean, the following are equivalent:*
(i) $\mathrm{Herm}(A)$ *has diagonal entries in* R^**;*
(ii) $\det(A) \in R^*$*; and*
(iii) A is invertible.
In this case, (III.C.9) *still gives a way to compute* A^{-1}*.*

Now here's a problem: we can't prove $\det(AB) = \det(A)\det(B)$ as we did above if neither A nor B satisfies these equivalent conditions – let alone if R isn't a Euclidean domain (or a domain!).

Fortunately, the solution is straightforward (if a bit ugly). Suppose, once again, that R is a *general commutative ring*.

III.C.16. PROPOSITION. $\det(AB) = \det(A)\det(B)$.

PROOF. Write $C = AB$, so that $c_{j\ell} = \sum_{k=1}^n a_{jk} b_{k\ell}$. We compute

$$\begin{aligned}
\det(A)\det(B) &= \sum_{\sigma \in \mathfrak{S}_n} \mathrm{sgn}(\sigma) \prod_{j=1}^n a_{j,\sigma(j)} \times \sum_{\eta \in \mathfrak{S}_n} \mathrm{sgn}(\eta) \prod_{k=1}^n b_{k,\eta(k)} \\
\text{[taking } \rho = \eta \circ \sigma] \quad &= \sum_{\rho \in \mathfrak{S}_n} \mathrm{sgn}(\rho) \sum_{\sigma \in \mathfrak{S}_n} \prod_{j=1}^n a_{j,\sigma(j)} \prod_{k=1}^n b_{k,\rho(\sigma^{-1}(k))} \\
\text{[identify } k = \sigma(j)] \quad &= \sum_{\rho \in \mathfrak{S}_n} \mathrm{sgn}(\rho) \sum_{\sigma \in \mathfrak{S}_n} \prod_{j=1}^n a_{j,\sigma(j)} b_{\sigma(j),\rho(j)} \\
\text{[see below]} \quad &\boxed{=} \sum_{\rho \in \mathfrak{S}_n} \mathrm{sgn}(\rho) \prod_{j=1}^n \sum_{\ell=1}^n a_{j\ell} b_{\ell,\rho(j)} \\
&= \sum_{\rho \in \mathfrak{S}_n} \mathrm{sgn}(\rho) \prod_{j=1}^n c_{j,\rho(j)} = \det(C).
\end{aligned}$$

As for the boxed equality, first observe[7] that

$$\text{(III.C.17)} \qquad \prod_{j=1}^{n}\left(\sum_{\ell=1}^{n} a_{j\ell}b_{\ell,\rho(j)}\right) = \sum_{\mu\in\mathfrak{T}_n}\prod_{j=1}^{n} a_{j,\mu(j)}b_{\mu(j),\rho(j)}$$

where $\mathfrak{T}_n$ denotes *all* maps from $\{1,\ldots,n\}$ to itself (not just permutations). For each $\mu \in \mathfrak{T}_n$, let $B^{(\mu)}$ denote the $n\times n$ matrix whose i^{th} row is the $\mu(i)^{\text{th}}$ row of B for each i. Applying a variant of the first 3 steps above in reverse gives

$$\begin{aligned}
\sum_{\rho\in\mathfrak{S}_n}\operatorname{sgn}(\rho)\sum_{\mu\in\mathfrak{T}_n\setminus\mathfrak{S}_n}\prod_{j=1}^{n} a_{j,\mu(j)}b_{\mu(j),\rho(j)} &= \sum_{\rho\in\mathfrak{S}_n}\sum_{\mu\in\mathfrak{T}_n\setminus\mathfrak{S}_n}\prod_{j=1}^{n} a_{j,\mu(j)}\prod_{k=1}^{n} b_{\mu(\rho^{-1}(k)),k} \\
&= \sum_{\mu\in\mathfrak{T}_n\setminus\mathfrak{S}_n}\left(\prod_{j=1}^{n} a_{j,\mu(j)}\sum_{\rho\in\mathfrak{S}_n}\operatorname{sgn}(\rho)\prod_{k=1}^{n} b_{\mu(\rho^{-1}(k)),k}\right) \\
&= \sum_{\mu\in\mathfrak{T}_n\setminus\mathfrak{S}_n}\left(\prod_{j=1}^{n} a_{j,\mu(j)}\sum_{\rho\in\mathfrak{S}_n}\operatorname{sgn}(\rho)\prod_{k=1}^{n} b^{(\mu)}_{\rho^{-1}(k),k}\right) \\
&= \sum_{\mu\in\mathfrak{T}_n\setminus\mathfrak{S}_n}\left(\prod_{j=1}^{n} a_{j,\mu(j)}\det B^{(\mu)}\right) \;=\; 0
\end{aligned}$$

since $B^{(\mu)}$ has repeated rows for $\mu\in\mathfrak{T}_n\setminus\mathfrak{S}_n$. This shows that after multiplying (III.C.17) by $\operatorname{sgn}(\rho)$ and summing over $\rho\in\mathfrak{S}_n$ we can omit terms with $\mu\notin\mathfrak{S}_n$, proving the boxed equality. □

What about invertibility? Well, you may recall that adjugate matrices and Cramer's rule were always the most horrible approach to computing inverses and solving systems of equations in linear algebra, *unless* the matrix entries were (say) transcendentals, polynomials, etc. Since our entries are now in a general commutative ring, let's try this approach. Defining the **cofactor**

$$\text{(III.C.18)} \qquad A_{ij} := (-1)^{i+j}\det\Big(\overbrace{(a_{k\ell})_{\substack{k\neq i\\ \ell\neq j}}}^{(n-1)\times(n-1)}\Big),$$

[7]When expanding the LHS, the μ^{th} term on the RHS is obtained by choosing the $\mu(j)^{\text{th}}$ term (of the sum in parentheses) from the j^{th} factor, as j runs from 1 to n.

as an immediate (computational) consequence of III.C.1 we have the **Laplace expansions**

$$\det(A) = \sum_{\ell=1}^{n} a_{i\ell} A_{i\ell} = \sum_{k=1}^{n} a_{ki} A_{ki}. \tag{III.C.19}$$

Now let A' (resp. A'') be the matrices obtained by deleting the i^{th} row (resp. column) and replacing it by the j^{th} row (resp. column). The repeated row (resp. column) makes the determinant zero:

$$\left.\begin{array}{r} 0 = \det A' = \sum_{\ell=1}^{n} a_{j\ell} A_{i\ell} \\ 0 = \det A'' = \sum_{k=1}^{n} a_{kj} A_{ki} \end{array}\right\} (j \neq i). \tag{III.C.20}$$

Overall, (III.C.19)-(III.C.20) $\implies$

$$\sum_{\ell=1}^{n} a_{j\ell} A_{i\ell} = (\det A)\delta_{ij} = \sum_{k=1}^{n} a_{kj} A_{ki}. \tag{III.C.21}$$

Defining the **adjugate matrix** (or "classical adjoint") by

$$\text{adj}(A) \;:=\; n \times n \text{ matrix with } (i,j)\text{th entry } A_{ji}\,, \tag{III.C.22}$$

we have the

III.C.23. PROPOSITION. $(\text{adj}A)A = \det(A)\mathbb{1} = A(\text{adj}A)$.

PROOF. The (i,j)th entry of $(\text{adj}A)A$ is

$$\sum_{k=1}^{n} [\text{adj}A]_{ik} a_{kj} = \sum_{k=1}^{n} a_{kj} A_{ki} = (\det A)\delta_{ij}. \qquad \square$$

This leads to the

III.C.24. THEOREM. *$A \in M_n(R)$ belongs to $M_n(R)^*$ (=: $\mathrm{GL}_n(R)$) if and only if $\det(A) \in R^*$.*

PROOF. ($\implies$): by III.C.23, $(\frac{\text{adj}A}{\det A})A = \mathbb{1} = A(\frac{\text{adj}A}{\det A})$.
($\impliedby$): by III.C.16, $AB = \mathbb{1} \implies \det(A)\det(B) = 1$. $\square$

Even for R a field, for $n > 1$ $M_n(R)$ is not a division ring; even the subring of diagonal matrices isn't! On the other hand, the diagonal matrices with all entries equal yield a subring which is isomorphic to R. Are there other sorts of "in-between" subrings that are still division rings,[8] i.e. have all nonzero elements invertible?

III.C.25. EXAMPLE. Consider the subset of $M_2(\mathbb{C})$ comprising matrices of the form

$$M = \begin{pmatrix} \alpha & \gamma \\ -\bar{\gamma} & \bar{\alpha} \end{pmatrix} = \begin{pmatrix} a+b\mathbf{i} & c+d\mathbf{i} \\ -c+d\mathbf{i} & a-b\mathbf{i} \end{pmatrix}.$$

Since

$$\begin{pmatrix} \alpha & \gamma \\ -\bar{\gamma} & \bar{\alpha} \end{pmatrix} \begin{pmatrix} \alpha' & \gamma' \\ -\bar{\gamma}' & \bar{\alpha}' \end{pmatrix} = \begin{pmatrix} \alpha\alpha' - \gamma\bar{\gamma}' & \alpha\gamma' + \gamma\bar{\alpha}' \\ -\bar{\gamma}\alpha' - \bar{\alpha}\bar{\gamma}' & -\bar{\gamma}\gamma' + \bar{\alpha}\bar{\alpha}' \end{pmatrix}$$

is still such a matrix, and closure is obvious for addition, this is a *subring*. Moreover,

$$0 = \det(M) = |\alpha|^2 + |\gamma|^2 \iff \alpha = \gamma = 0 \iff M = 0.$$

Hence, all nonzero entries of this type are invertible, and this subset is a division ring, which we will later identify with $\mathbb{H}$.

[8]Keep in mind here that $\mathrm{GL}_n(R)$ is not a subring, since it's not closed under addition. It's just a group under multiplication.