A USEFUL LITTLE FACT

Let R and $\widetilde{R}$ be commutative rings with multiplicative identity. Suppose that we have a ring homomorphism that preserves multiplicative identities,

$$f : R \longrightarrow \widetilde{R}, \qquad f(1_R) = 1_{\widetilde{R}}.$$

Let n be a positive integer. We will show that the matrix map obtained by applying f entrywise to n-by-n matrices,

$$g : \mathrm{M}_n(R) \longrightarrow \mathrm{M}_n(\widetilde{R}), \quad g([r_{ij}]) = [f(r_{ij})],$$

is a ring homomorphism that preserves multiplicative identities. As such, it restricts to a *group* homomorphism

$$g : \mathrm{GL}_n(R) \longrightarrow \mathrm{GL}_n(\widetilde{R}),$$

and the group homomorphism takes the special linear subgroup into the special linear subgroup,

$$g : \mathrm{SL}_n(R) \longrightarrow \mathrm{SL}_n(\widetilde{R}).$$

(Again, to make sure that the notation is clear: f takes ring elements to ring elements, while g takes matrices to matrices by applying f entrywise.)

The argument is straightforward. First, the map

$$g : \mathrm{M}_n(R) \longrightarrow \mathrm{M}_n(\widetilde{R})$$

is characterized by the property

$$(g(m))_{ij} = f(m_{ij}), \quad m \in \mathrm{M}_n(R),\ i, j \in \{1, \cdots, n\}.$$

It follows immediately that g preserves matrix sums. Indeed, using the characterizing property, compute that for any row and column indices $i, j \in \{1, \cdots, n\}$ and for any matrices $a = [a_{ij}]$ and $b = [b_{ij}]$ in $\mathrm{M}_n(R)$,

$$\begin{aligned}
(g(a+b))_{ij} &= f((a+b)_{ij}) && \text{by the characterizing property of } g \\
&= f(a_{ij} + b_{ij}) && \text{since matrix addition proceeds entrywise} \\
&= f(a_{ij}) + f(b_{ij}) && \text{since } f \text{ preserves scalar addition} \\
&= (g(a))_{ij} + (g(b))_{ij} && \text{by the characterizing property of } g.
\end{aligned}$$

Since i and j are arbitrary, $g(a+b) = g(a) + g(b)$, i.e., g preserves sums as desired.

Similarly, g preserves matrix products in consequence of f being a ring homomorphism. Again using the characterizing property, compute that for any i, j and a, b

as before,

$$\begin{aligned}
(g(ab))_{ij} &= f((ab)_{ij}) && \text{by the characterizing property of } g \\
&= f\left(\sum_k a_{ik}b_{kj}\right) && \text{by definition of multiplication in } \mathrm{M}_n(R) \\
&= \sum_k f(a_{ik})f(b_{kj}) && \text{because } f \text{ is a ring homomorphism} \\
&= \sum_k g(a)_{ik}g(b)_{kj} && \text{by the characterizing property of } g \\
&= (g(a)g(b))_{ij} && \text{by definition of multiplication in } \mathrm{M}_n(\widetilde{R}).
\end{aligned}$$

Since i and j are arbitrary, $g(ab) = g(a)g(b)$, i.e., g preserves products as desired.

Also, since $f(1_R) = 1_{\widetilde{R}}$, it follows that $g(I_{n,R}) = I_{n,\widetilde{R}}$.

To summarize so far, $g : \mathrm{M}_n(R) \longrightarrow \mathrm{M}_n(\widetilde{R})$ is a ring homomorphism that preserves multiplicative identities.

Next, since

$$\mathrm{GL}_n(R) = (\mathrm{M}_n(R))^\times,$$

and similarly with $\widetilde{R}$ in place of R, and since any ring homomorphism that preserves multiplicative identities restricts to a homomorphism of multiplicative groups, we have immediately that g restricts to a homomorphism

$$g : \mathrm{GL}_n(R) \longrightarrow \mathrm{GL}_n(\widetilde{R}),$$

Two comments are relevant here. First, the general argument that any ring homomorphism h that preserves multiplicative identities restricts to a homomorphism of multiplicative groups is

$$xy = 1 \implies h(x)h(y) = h(xy) = h(1) = 1,$$

so that if x is multiplicatively invertible then so is $h(x)$. Second, the multiplicative group

$$\mathrm{GL}_n(R) = \{m \in \mathrm{M}_n(R) : \det(m) \in R^\times\}.$$

consists of the matrices having *invertible* determinants rather than *nonzero* determinants. In the context of linear algebra, where the matrix entries are always elements of a field, all nonzero scalars are invertible, but this condition does not hold in a general ring.

Next we show that

$$\det(g(m)) = f(\det(m)), \quad m \in \mathrm{M}_n(R).$$

(The equality has g on the left side since m is a matrix with entries in R, and it has f on the right side since $\det m$ is an element of R.) The displayed identity holds because the n-by-n determinant is a universal polynomial of the matrix entries, making the result an immediate consequence of f being a ring homomorphism,

$$\begin{aligned}
\det(g(m)) &= \det(\{(g(m))_{ij}\}) && \text{viewing det as a polynomial of the entries} \\
&= \det(\{f(m_{ij})\}) && \text{rewriting the entries} \\
&= f(\det(\{m_{ij}\})) && \text{because } f \text{ is a ring homomorphism} \\
&= f(\det(m)) && \text{returning to det as a function of matrices.}
\end{aligned}$$

Especially, the identity combines with the condition $f(1_R) = 1_{\widetilde{R}}$ to show that g takes $\mathrm{SL}_n(R)$ into $\mathrm{SL}_n(\widetilde{R})$,

$$\det(g(m)) = f(\det(m)) = f(1_R) = 1_{\widetilde{R}}, \quad m \in \mathrm{SL}_n(R)$$

A relevant example on the midterm is that the matrix reduction map

$$g : \mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$$

is a group homomorphism because the scalar reduction map

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}/N\mathbb{Z}$$

is a ring homomorphism that preserves multiplicative identities.

Another example on the midterm is that the map

$$\mathrm{SL}_2(\mathbb{Z}/p^{e+1}\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$$

is a surjective group homomorphism. It is a group homomorphism because in the successive containments

$$p^{e+1}\mathbb{Z} \subset p^e\mathbb{Z} \subset \mathbb{Z},$$

$p^{e+1}\mathbb{Z}$ is an ideal of $\mathbb{Z}$ and a subring of $p^e\mathbb{Z}$, which in turn is an ideal of $\mathbb{Z}$, so that the third *ring* isomorphism theorem gives

$$(\mathbb{Z}/p^{e+1}\mathbb{Z})/(p^e\mathbb{Z}/p^{e+1}\mathbb{Z}) \approx \mathbb{Z}/p^e\mathbb{Z}, \quad (n + p^{e+1}\mathbb{Z}) + p^e\mathbb{Z} \longmapsto n + p^e\mathbb{Z},$$

Consequently the following diagram of ring homomorphisms commutes:

$$\begin{tikzcd}
 & \mathbb{Z} \arrow[dl] \arrow[dr] & \\
\mathbb{Z}/p^{e+1}\mathbb{Z} \arrow[r] & (\mathbb{Z}/p^{e+1}\mathbb{Z})/(p^e\mathbb{Z}/p^{e+1}\mathbb{Z}) \arrow[r] & \mathbb{Z}/p^e\mathbb{Z}.
\end{tikzcd}$$

It follows that the following diagram of group homomorphisms commutes:

$$\begin{tikzcd}
 & \mathrm{SL}_2(\mathbb{Z}) \arrow[dl] \arrow[dr] & \\
\mathrm{SL}_2(\mathbb{Z}/p^{e+1}\mathbb{Z}) \arrow[rr] & & \mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z}).
\end{tikzcd}$$

Because the diagram commutes and the right diagonal map surjects (by exercise 2 on the midterm), the map across the bottom surjects.

In a similar vein, the Sun-Ze ring isomorphism

$$\mathbb{Z}/N\mathbb{Z} \xrightarrow{\sim} \prod_{p^e \| N} \mathbb{Z}/p^e\mathbb{Z}$$

underlies a ring isomorphism

$$\mathrm{M}_2(\mathbb{Z}/N\mathbb{Z}) \xrightarrow{\sim} \mathrm{M}_2\Big(\prod_{p^e \| N} \mathbb{Z}/p^e\mathbb{Z}\Big),$$

and then further identifying *matrices of vectors* with *vectors of matrices* gives

$$\mathrm{M}_2(\mathbb{Z}/N\mathbb{Z}) \xrightarrow{\sim} \prod_{p^e \| N} \mathrm{M}_2(\mathbb{Z}/p^e\mathbb{Z}).$$

The ring isomorphism restricts to an isomorphism of multiplicative groups,

$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \xrightarrow{\sim} \prod_{p^e \parallel N} \mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$$

that further specializes to a smaller group isomorphism

$$\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \xrightarrow{\sim} \prod_{p^e \parallel N} \mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z}).$$