A USEFUL LITTLE FACT

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

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

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

$$g : M_n(R) \longrightarrow M_n(\tilde{R}), \quad g([r_{ij}]) = [f(r_{ij})],$$

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

$$g : \text{GL}_n(R) \longrightarrow \text{GL}_n(\tilde{R}),$$

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

$$g : \text{SL}_n(R) \longrightarrow \text{SL}_n(\tilde{R}).$$

(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

$$g : M_n(R) \longrightarrow M_n(\tilde{R})$$

is characterized by the property

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

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 $M_n(R),$

$$(g(a + b))_{ij} = f((a + b)_{ij}) \quad \text{by the characterizing property of } g$$

$$= f(a_{ij} + b_{ij}) \quad \text{since matrix addition proceeds entrywise}$$

$$= f(a_{ij}) + f(b_{ij}) \quad \text{since } f \text{ preserves scalar addition}$$

$$= (g(a))_{ij} + (g(b))_{ij} \quad \text{by the characterizing property of } g.$$

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,

\[(g(ab))_{ij} = f((ab)_{ij}) \quad \text{by the characterizing property of } g\]

\[= f \left( \sum_k a_{ik}b_{kj} \right) \quad \text{by definition of multiplication in } M_n(R)\]

\[= \sum_k f(a_{ik})f(b_{kj}) \quad \text{because } f \text{ is a ring homomorphism}\]

\[= \sum_k g(a)_{ik}g(b)_{kj} \quad \text{by the characterizing property of } g\]

\[= (g(a)g(b))_{ij} \quad \text{by definition of multiplication in } M_n(\tilde{R}).\]

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

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

To summarize so far, \(g : M_n(R) \to M_n(\tilde{R})\) is a ring homomorphism that preserves multiplicative identities.

Next, since

\[GL_n(R) = (M_n(R))^\times,\]

and similarly with \(\tilde{R}\) 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

\[g : GL_n(R) \to GL_n(\tilde{R}),\]

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

\[GL_n(R) = \{m \in M_n(R) : \det(m) \in R^\times\}.\]

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

\[\det(g(m)) = f(\det(m)), \quad m \in M_n(R).\]

(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,

\[\det(g(m)) = \det(\{(g(m))_{ij}\}) \quad \text{viewing } \det \text{ as a polynomial of the entries}\]

\[= \det(\{f(m)_{ij}\}) \quad \text{rewriting the entries}\]

\[= f(\det(\{m_{ij}\})) \quad \text{because } f \text{ is a ring homomorphism}\]

\[= f(\det(m)) \quad \text{returning to } \det \text{ as a function of matrices.}\]
A USEFUL LITTLE FACT

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

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

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

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

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

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

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

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

Consequently the following diagram of ring homomorphisms commutes:

It follows that the following diagram of group homomorphisms commutes:

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

$$\mathbb{Z}/N\mathbb{Z} \cong \prod_{p^n \mid N} \mathbb{Z}/p^e\mathbb{Z}$$

underlies a ring isomorphism

$$\text{M}_2(\mathbb{Z}/N\mathbb{Z}) \cong \text{M}_2 \left( \prod_{p^n \mid N} \mathbb{Z}/p^e\mathbb{Z} \right),$$

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

$$\text{M}_2(\mathbb{Z}/N\mathbb{Z}) \cong \prod_{p^n \mid N} \text{M}_2(\mathbb{Z}/p^e\mathbb{Z}).$$
The ring isomorphism restricts to an isomorphism of multiplicative groups,
\[ \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \xrightarrow{\sim} \prod_{p^e \mid N} \text{GL}_2(\mathbb{Z}/p^e\mathbb{Z}) \]
that further specializes to a smaller group isomorphism
\[ \text{SL}_2(\mathbb{Z}/N\mathbb{Z}) \xrightarrow{\sim} \prod_{p^e \mid N} \text{SL}_2(\mathbb{Z}/p^e\mathbb{Z}). \]