HW 9 Solutions

#1) Let's check $N \trianglelefteq G$ (assuming already $N \leq G$).

Let $A \in G$, $M \in N$, ie $\det M = 1$.

Then $\det(AMA^{-1}) = \det A \det M \det(A^{-1})$
$= \det A \cdot 1 \cdot \frac{1}{\det A} = 1$,

so $AMA^{-1} \in N$, and $N \trianglelefteq G$.

Next, let's look at cosets.

<u>Claim:</u> $AN = \{B \in G : \det B = \det A\}$, ie,

the coset containing A is precisely the set of matrices whose determinants are the same as A's.

Let's check: $B \in AN$ iff $A^{-1}B \in N$ (using our coset equivalence relation) iff $\det(A^{-1}B) = 1$.

Rearranging, this is true iff $\det(A^{-1}) \det B = 1$

iff $\frac{1}{\det A} \cdot \det B = 1$ iff $\det B = \det A$.

Since ~~cosets~~ ~~can~~ elements of G can have any nonzero determinant, we are expecting one coset per real number in $\mathbb{R}^*$.

We can use the 1^{st} Isom Thm to prove $G/N \cong \mathbb{R}^*$, as follows.

Let $\varphi: G \longrightarrow \mathbb{R}^*$

$B \longmapsto \det B$.

We have already seen that this is a group homomorphism. ~~It is~~ Its image is all of $\mathbb{R}^*$, since for example $\begin{bmatrix} r & & 0 \\ & 1 & \\ 0 & & \ddots & \\ & & & 1 \end{bmatrix} \longmapsto r$

for any $r \in \mathbb{R}^*$, and its kernel is all matrices with determinant 1, ie N.

Thus $G/N \cong \mathbb{R}^*$

③

#2a) We already know R is a comm ring; it remains to check that R has no zero divisors.

Let $a(x) = a_k x^k + a_{k+1} x^{k+1} + \cdots$ and

$b(x) = b_l x^l + b_{l+1} x^{l+1} + \cdots$ be nonzero elements in R,

where $a_k, b_l \neq 0$. I.e. we have not written any small terms with 0 coeffs..

Then ~~a(x)b~~ consider $a(x) \cdot b(x)$

$$= (a_k x^k + a_{k+1} x^{k+1} + \cdots)(b_l x^l + b_{l+1} x^{l+1} + \cdots)$$

Only one pair in this product contributes to the x^{k+l} term, i.e. $a_k x^k \cdot b_l x^l = a_k b_l x^{k+l}$.

(In contrast with later terms, e.g.

$(a_k b_{l+1} + a_{k+1} b_l) x^{k+l+1}$.)

④

Thus, since $a_k, b_\ell \neq 0$ and $\mathbb{R}$ is an integral domain, we know $a_k b_\ell \neq 0$, so $a(x)\, b(x)$ has at least one nonzero term and is thus not the zero power series.

Thus R is an integral domain.

#2b) Any x^n with $n \geq 1$ is neither a unit nor a zero divisor.

Since R is an integral domain, the product $x^n \cdot p(x)$ has degree at least n whenever p(x) is not the zero element.

Since 1 and 0 are constants, no choice of p(x) will be an inverse of x^n or the other half of a zero divisor pair. (For the latter, you could just say we proved in 2a that there are no zero divisors.)

#2c) $(ax-1)^{-1} = -1 - ax - a^2x^2 - a^3x^3 - \cdots$

$$= \sum_{k \geq 0} -a^k x^k \quad \text{(infinitely many terms)}$$

Check their product is 1 (~~all~~ all higher degree terms cancel out in pairs)

#3a) There are 6^4 elements in R → 6 choices for each of 4 entries.

Subrings are also additive subgroups, so by Lagrange, their orders must be divisors of 6^4.

Since a subring must contain $\begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{bmatrix}$, which has order 6, subrings must have order at least 6.

#3b) Nonzero elements M of R are

$$\begin{cases} \text{units} & \text{if } \det M = \bar{1} \text{ or } \bar{5} \\ \text{zero divisors} & \text{if } \det M = \bar{0}, \bar{2}, \bar{3} \text{ or } \bar{4} \end{cases}$$

Proof →

6

Let $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. As with real/complex/integer matrices, if

$\det M$ has a multiplicative inverse, then

$$M^{-1} = (\det M)^{-1} \cdot \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

this gives us no trouble here for units.

Note it is always the case that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} ad-bc & 0 \\ 0 & ad-bc \end{bmatrix} = \det M \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

this can help us build zero divisor pairs when

$\det M = 0, 2, 3,$ or 4.

If $\det M = 0$, then M and $\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ are

a zero divisor pair. (Since M doesn't have

all zero entries, neither will $\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.)

If $\det M = 2$ or 4, then M and

$3\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ will form a zero divisor pair,

<u>if</u> the latter is not the zero matrix. But we can get around this: If a, b, c, d are all divisible by 2 or 4, ~~divide them 2 or 4 but first, then multiply by 3.~~ then take $\begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix}$ as the other half of your zero divisor pair.

If $\det M = 3$, then M and $2\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ will form a zero divisor pair, as long as the latter is not the zero matrix. If it is, i.e. all of a, b, c, d are multiples of 3, then take $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$ instead.

Thus all nonzero elements of R are units

or zero divisors.

#3c) the obvious solutions come from factoring.

$$X^2 - 4X + 3I = (X - 3I)(X - I) = 0$$

So $X = 3I$ or $X = I$.

You can find more by experimenting with the entries:

Let $X = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ then our equation becomes

$$\begin{bmatrix} a^2 + bc - 4a + 3 & ab + bd - 4b \\ ac + cd - 4c & bc + d^2 - 4d + 3 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Since the 0's are in $\mathbb{Z}_6$, we actually expect more than one solution to this. I would try for an upper triangular one first

~~If det M ∈ $\mathbb{Z}_6^\times$, take at least one entry~~

If $c=0$, we have:

$$\begin{bmatrix} a^2-4a+3 & ab+bd-4b \\ 0 & d^2-4d+3 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

this forces $a^2-4a+3 \equiv 0 \mod 6$

so $a = 1$ or 3

$d^2-4d+3 \equiv 0 \mod 6$

so $d \equiv 1$ or 3

~~We already have cases when a, d match~~

If we try $a, d \equiv 1$, we need

$ab+bd-4b = -2b \equiv 0 \mod 6$. $b=0$ is already covered, so ~~th~~ take $b \equiv 3$.

You can check $\begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}$ satisfies our equation.