Reading Questions 5

page 29: Definition 1.60

1. The group $\mathrm{GL}(2, Z_3)$ is a group of matrices. T
2. In the general linear group $\mathrm{GL}(n, F)$, F is a field. T
3. List an element in $\mathrm{GL}(2, Z_3)$ which contains all nonzero entries. You may use the notation $[[1, 0], [0, 1]]$ to represent the matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ $\begin{matrix} 1 & 1 \\ 2 & 1 \end{matrix}$ $\begin{matrix} 1 & 2 \\ 2 & 1 \end{matrix}$ $\begin{matrix} 1 & 1 \\ 1 & 2 \end{matrix}$

Section 1.4 Invertible Matrices (Part 1)

Definitions

P 1. Let $A = \begin{bmatrix} 3 & 2 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{bmatrix} \in \mathrm{GL}(3, Z_5)$. Compute $\det(A)$.

P 2. Let $A \in \mathrm{GL}(2, Z_7)$ such that $A = \begin{bmatrix} 3 & 2 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{bmatrix}$. Determine if $A \in \mathrm{SL}(2, Z_7)$.

Section 2.1 Definitions and Examples (Part 1)

Definitions

P 1. List the identity element for the following groups. $(\mathbb{Z}, +), (Z_n^\times), \mathrm{GL}(2, Z_5), \mathrm{SL}(2, Z_7)$.

P 2. Show that $(\mathbb{Z}, +)$ is a group.

1.4:

$\mathbb{R}$ - real numbers

$\mathbb{C}$ - complex numbers $a + bi$ $a, b \in \mathbb{R}$ $i = \sqrt{-1}$

$\mathbb{Z}$ - integers

$\mathbb{Q}$ - rational numbers $\frac{m}{n}$ $n \neq 0$ $m, n \in \mathbb{Z}$

Def: (for F)
det A is det A in F $\forall A \in GL(n, F)$

(for $\mathbb{Z}_p$, p-prime)

det A is $(\det A \text{ in } \mathbb{C}) \bmod p$ $\forall A \in GL(n, \mathbb{Z}_p)$

Ex: Let $\begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} \in GL(2, \mathbb{Z}_5)$.

$$\det \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} = (3 \cdot 1 - 2 \cdot 0) \bmod 5$$

$$\equiv 3 \bmod 5 = 3$$

$$\det \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix} = (3 \cdot 1 - 2 \cdot 2) \bmod 5$$

$$\equiv -1 \bmod 5 = 4$$

Def: The special linear group

$$SL(n, F) = \{ A \in GL(n, F) : \det A = 1 \}$$

Ex: Let $A \in GL(2, \mathbb{Z}_5)$ such that

$A = \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix}$. We saw $\det A = 3 \neq 1$.

Hence $A \notin SL(2, \mathbb{Z}_5)$

WRONG!!!

$\frac{1}{4} A \in SL(2, \mathbb{Z}_5)$

$\parallel$

$4A = \begin{pmatrix} 2 & 3 \\ 0 & 4 \end{pmatrix}$ - check

$4^{-1} = \frac{1}{4}$

$\det 4A \neq \underbrace{4 \det A}_{\substack{\parallel \\ 1}}$

$\parallel$

4

$2 \cdot \det A = 2 \cdot 3 \bmod 5$

$\Rightarrow 2 \det A \equiv 1$

$\Rightarrow \det \begin{pmatrix} 3 \cdot 2 & 2 \cdot 2 \\ 0 & 1 \end{pmatrix} =$

Ex: Let $A \in GL(2, \mathbb{Z}_5)$ such that $A = \begin{pmatrix} 4 & 2 \\ 0 & 4 \end{pmatrix}$.

Then $\det A = 4 \cdot 4 \mod 5 = 1$.

$$\det \begin{pmatrix} 3 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 2 \end{pmatrix} = 3 \det \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

Exam:
P: $\det A = 5 \mod 7$

Find $B = A$ (times a scalar row) such that $\det B = 1$.

2.1: Def: (group) Let G be a nonempty set and let $*$ be an operation. Then $(G, *)$ is a group if

$\forall a, b, c \in G$

(1) $a * b \in G$ (closure)

(2) $(a * b) * c = a * (b * c)$ (associativity)

(3) $\exists\, e \in G$ such that $\forall a \in G$ (identity)

$e * a = a * e = a$

(4) $\forall a \in G$ $\exists\, x \in G$ such that (inverse)

$ax = xa = e$

Ex: D_{2n}, $(\mathrm{Perm}(\Omega), \circ)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +)$, $((\mathbb{Z}_n)^\times, \cdot)$

$GL(n, F)$, $SL(n, F)$ are all groups.

Def: Let $(G, *)$ be a group. The order of G is the number of elements in the group G denoted by $|G|$.

G is abelian if $\forall a, b \in G$, $a * b = b * a$.

Ex: $((\mathbb{Z}_n)^\times, \cdot)$ is abelian and

D_8 is not abelian.

Section 2.1 Definitions and Examples (Part 1)

Definitions

P 1. List the identity element for the following groups. $(\mathbb{Z}, +), (Z_n^\times), \mathrm{GL}(2, Z_5), \mathrm{SL}(2, Z_7)$.

P 2. Show that $(\mathbb{Z}, +)$ is a group.