Section 1.4 Matrix Groups

Recall: $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a,n)=1\}$ is a group with operation $\cdot$.
If n is prime, $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \bar{3} \dots \overline{n-1}\}$

$GL_n(\mathbb{R}) = \{ A \mid A \text{ is } n \times n \text{ matrix with real entries, } \det(A) \neq 0 \}$

This is a group under matrix multiplication

(i) Matrix multiplication is associative.

(ii) $I = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix} \in GL_n(\mathbb{R})$ is identity: $AI = IA = A \quad \forall A$.

(iii) If $A \in GL_n(\mathbb{R})$, then $\det(A) \neq 0$ so $\exists\ A^{-1} \in GL_n(\mathbb{R})$ with $AA^{-1} = A^{-1}A = I$.

Called the <u>general linear group</u> of $n \times n$ matrices.

There is nothing special about $\mathbb{R}$ here. In linear algebra you may have also used $\mathbb{C}$ in its place. In fact $\mathbb{R}$ can be replaced with any algebraic structure that is a field.

<u>Today</u>: ① Define algebraic structure $\mathbb{F}$, called a field.
② Examine the group $GL_n(\mathbb{F})$

<u>Definition</u> A <u>field</u> is a set $\mathbb{F}$ on which is defined two operations $+$ and $\cdot$ satisfying the following:

① $(\mathbb{F}, +)$ is an abelian group with identity 0.

② $(\mathbb{F} - \{0\}, \cdot)$ is an abelian group with identity 1.

③ The distributive law holds: $a(b+c) = a \cdot b + a \cdot c$.

<u>Examples</u>: $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ (∞ fields)

<u>Example</u>: $\mathbb{Z}/p\mathbb{Z}$ where p is prime (finite fields)

① $(\mathbb{Z}/p\mathbb{Z}, +)$ is an abelian group

② $(\mathbb{Z}/p\mathbb{Z} - \{\bar{0}\}, \cdot) = ((\mathbb{Z}/p\mathbb{Z})^\times, \cdot)$ is an abelian group.

③ $\bar{a}(\bar{b}+\bar{c}) = \bar{a} \cdot \overline{b+c} = \overline{a(b+c)} = \overline{ab+ac}$
$= \overline{ab} + \overline{ac}$
$= \bar{a}\bar{b} + \bar{a}\bar{c}$.

Definition Given a field $\mathbb{F}$,

$GL_n(\mathbb{F}) = \{ A \mid A \text{ is } n \times n \text{ matrix w/ entries from } \mathbb{F}, \text{ and } \det(A) \neq 0 \}$

This is a group with identity $I = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & \cdots & 1 \end{bmatrix}$.

Reason: In linear algebra, the proofs that matrix multiplication is associative, and $\det(A) \neq 0 \iff A^{-1}$ exists etc. used only the field axioms for $\mathbb{R}$ and nothing else specific to $\mathbb{R}$. Hence they also hold if $\mathbb{R}$ is replaced by an arbitrary field $\mathbb{F}$.

Example:

$$GL_2(\mathbb{Z}/2\mathbb{Z}) = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \right\}$$

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1+1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{etc.}$$

General facts about fields

① If $\mathbb{F}$ is a finite field, then $|\mathbb{F}| = p^m$ for some prime p.

② If $|\mathbb{F}| = q$ then $|GL_n(\mathbb{F})| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$

Reason for ②. As example, consider $GL_3(\mathbb{F})$

$\begin{bmatrix} (q) & (q) & (q) \\ & & \end{bmatrix}$ There are $q \cdot q \cdot q = q^3$ different 1st rows you could make. But the one row of all 0's is not allowed. Thus $q^3 - 1$ possible first rows.

$\begin{bmatrix} * & * & * \\ (q) & (q) & (q) \end{bmatrix}$ There are q^3 choices for 2nd row. But 2nd row can't be multiple of 1st. There are q multiples of 1st. Thus $q^3 - q$ possible 2nd rows.

$\begin{bmatrix} * & * & * \\ * & * & * \\ (q) & (q) & (q) \end{bmatrix}$ q^3 possible 3rd rows, but it can't be a linear combo of 1st two. There are $q \cdot q = q^2$ linear combos of top two rows. Thus $q^3 - q^2$ possible 3rd rows

$$|GL_3(\mathbb{F})| = (q^3 - 1)(q^3 - q)(q^3 - q^2)$$

$$|GL_3(\mathbb{Z}/2\mathbb{Z})| = (2^3 - 1)(2^3 - 2)(2^3 - 4) = (26)(24)(18) = 11{,}232.$$

Section 1.5 The Quaternion Group

Definition The quaternion group Q_8 is

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

with the following product:

$$1a = a1 = a \quad \forall\, a \in Q_8$$
$$(-1)a = a(-1) = -a \quad \forall\, a \in Q_8$$
$$(-1)(-1) = 1$$
$$ii = jj = kk = -1$$

$$ij = k \qquad ji = -k$$
$$jk = i \qquad kj = -i$$
$$ki = j \qquad kk = -j$$

Thus 1 is the identity. Inverses are as follows:

$$(-1)^{-1} = -1 \quad i^{-1} = -i \quad j^{-1} = -j \quad k^{-1} = -k$$
$$1^{-1} = 1 \quad (-i)^{-1} = i \quad (-j)^{-1} = j \quad (-k)^{-1} = k$$

But why should we believe the associativity? Here is one way to look at it.

$$Q_8 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} \right\}$$

(1, −1, i, $-i$, j, $-j$, k, $-k$ respectively; $i = \sqrt{-1}$)

$$\subseteq GL_2(\mathbb{C})$$

Check:

$$ii = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -1$$
$$ij = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} = k$$
$$jk = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} = -k \quad \text{etc.}$$

Thus $Q_8 \subseteq GL_2(\mathbb{C})$ is associative because $GL_2(\mathbb{C})$ is associative.