GTLA Lecture 01.09.2020

Block decomposition Let $\mathbb{F}$ be a field. Let $n \in \mathbb{Z}_{>0}$ and $A \in M_n(\mathbb{F})$ and let $m_A(x)$ be the minimal polynomial of A. Let $V = \mathbb{F}^n$. Let

$$m_A(x) = p(x)q(x) \quad \text{with}$$

$\gcd(p(x), q(x)) = 1$. Then let $r(x), s(x) \in \mathbb{F}[x]$ so that

$$1 = p(x)r(x) + q(x)s(x)$$

Let $P_U = p(A)r(A)$ and $P_W = q(A)s(A)$.

Then

$$P_U + P_W = 1, \quad P_U P_W = 0, \quad P_U^2 = P_U$$

$$P_W^2 = P_W \qquad \text{(projectors).}$$

Let $U = P_U V$ and $W = P_W V$.

Then $V = U \oplus W$ and both U and W are A-invariant subspaces.

<u>Theorem</u> (Jordan Normal Form). Let $A \in M_n(\mathbb{C})$ then there exists $P \in GL_n(\mathbb{C})$ such that

$P^{-1}AP$ is a direct sum of Jordan blocks.

Let $\mathbb{F}$ be a field and $n \in \mathbb{Z}_{>0}$. A matrix $P \in M_n(\mathbb{F})$ is <u>invertible</u> if there exists $P^{-1} \in M_n(\mathbb{F})$ such that

$P^{-1}P = 1$ and $PP^{-1} = 1$.

The <u>general linear group</u>

$$GL_n(\mathbb{F}) = \left\{ P \in M_n(\mathbb{F}) \;\middle|\; P \text{ is invertible} \right\}$$

(1 and -1 are invertible in $\mathbb{Z}$. $1 \cdot 1 = 1$, $(-1)(-1) = 1$. But $1 + (-1) = 0$, which is <u>not</u> invertible)

$GL_n(\mathbb{F})$ does not have an addition operation.

If $P_1, P_2 \in GL_n(\mathbb{F})$ then let $Q = P_2^{-1} P_1^{-1}$

$QP_1P_2 = (P_2^{-1} P_1^{-1}) P_1 P_2 = 1$ and

$P_1 P_2 \in GL_n(\mathbb{F})$.

$GL_n(\mathbb{F})$ does have multiplication.

The conjugation action of $GL_n(\mathbb{F})$ on $M_n(\mathbb{F})$ is given by

$$\begin{aligned} GL_n(\mathbb{F}) \times M_n(\mathbb{F}) &\longrightarrow M_n(\mathbb{F}) \\ (P, A) &\longrightarrow P^{-1}AP. \end{aligned}$$

This is a motivation for

Groups and Group Actions

A group is a set G with a function

$$\begin{aligned} G \times G &\longrightarrow G \\ (a, b) &\longmapsto ab \end{aligned}$$

such that

(a) If $g_1, g_2, g_3 \in G$ then
$$(g_1 g_2) g_3 = g_1 (g_2 g_3).$$

(b) There exists $1 \in G$ such that

if $g \in G$ then $1 \cdot g = g$ and $g 1 = g$.

(c) If $g \in G$ then there exist $g^{-1} \in G$ such that

$$g^{-1} g = 1 \text{ and } g g^{-1} = 1.$$

Let G be a group and S a set.

An <u>action of G on S</u> is a function

$$G \times S \longrightarrow S$$
$$(g, x) \longmapsto g \cdot x$$

such that

(a) If $g_1, g_2 \in G$ and $x \in S$ then

$$g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x.$$

(b) If $x \in S$ then $1 \cdot x = x$.

Let G be a group.

A <u>subgroup</u> of G is a subset $H \subseteq G$ such that

(a) If $h_1, h_2 \in H$ then $h_1 h_2 \in H$.

(b) $1 \in H$

(c) If $h \in H$ then $h^{-1} \in H$.

<u>Example</u> $G = GL_n(\mathbb{F})$

$H = SL_n = \{ P \in GL_n(\mathbb{F}) \mid \det(P) = 1 \}$.

(a) If $P_1, P_2 \in SL_n(\mathbb{F})$ then

$\det(P_1 P_2) = \det(P_1)\det(P_2) = 1 \cdot 1 = 1$.

So $P_1 P_2 \in SL_n(\mathbb{F})$. So (a) is satisfied.

(b) $\det(I) = \det\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} = 1$. So

$I = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} \in SL_n(\mathbb{F})$ So (b) is satisfied

(c) If $P \in SL_n(\mathbb{F})$ then

$\det(P^{-1}) = \det(P)^{-1} = 1^{-1} = 1$,

So $P^{-1} \in SL_n(\mathbb{F})$. So (c) is satisfied.

So $SL_n(\mathbb{F})$ is a subgroup of $GL_n(\mathbb{F})$.

<u>The symmetric group S_n</u>

$$S_n = \left\{ P \in GL_n(\mathbb{C}) \;\middle|\; \begin{array}{l} P \text{ has exactly one } 1 \\ \text{in each row and} \\ \text{each column and} \\ \text{all other entries } 0 \end{array} \right\}$$

$$S_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

$$S_3 = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \right\}$$

Let G be a group.
The order of G, or cardinality of G, is the number of elements in G.

$|G|$ is a common notation.

$\mathrm{Card}(G)$ is my preferred notation.

$\mathrm{Card}(S_2) = 2$, $\mathrm{Card}(S_3) = 6$

$\mathrm{Card}(GL_n(\mathbb{C})) = \infty$

Let

$$H = \left\{ \underset{a}{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}, \underset{b}{\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}} \right\} \subseteq S_3$$

$$K = \left\{ \underset{A}{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}, \underset{B}{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}} \right\} \subseteq S_3.$$

Multiplication tables

$\cdot$	a	b
a	a	b
b	b	a

H

$\cdot$	A	B
A	A	B
B	B	A

K

$+$	0	1
0	0	1
1	1	0

$\mathbb{Z}/2\mathbb{Z}$ only consider addition to view $\mathbb{Z}/2\mathbb{Z}$ as group.

$\cdot$	1	-1
1	1	-1
-1	-1	1

$\mu_2 = \{1, -1\}$

Are these the same group or different groups?

"Isomorphic".