Groups of unitary matrices

Teo Banica

"Introduction to matrix groups", 1/6

08/20

Groups 1/3

Definition. A group is a set G with a multiplication operation

$$(g, h) \to gh$$

satisfying the following conditions:

(1) Associativity: $(gh)k = g(hk)$.

(2) Unit: $\exists 1 \in G$, $g1 = 1g = g$.

(3) Inverses: $\forall g, \exists g^{-1}$, $gg^{-1} = g^{-1}g = 1$.

Groups 2/3

Examples.

(1) $\mathbb{R}$ with the addition operation $x + y$. Here the unit is 0 (!) and the inverses are $-x$.

(2) $\mathbb{R}^*$ with the multiplication operation xy. Here the unit is 1 and the inverses are x^{-1}.

(3) $\mathbb{Z}, \mathbb{Q}, \mathbb{C}$ with the addition operation $x + y$, and $\mathbb{Q}^*, \mathbb{C}^*$ with the multiplication operation xy.

Note that $(\mathbb{N}, +)$ and $(\mathbb{N}, \cdot)$ and $(\mathbb{Z}^*, \cdot)$ are not groups, because here we have no inverses.

Groups 3/3

More examples.

(1) The group S_N of permutations $\sigma : \{1, \ldots, N\} \to \{1, \ldots, N\}$. Note that we have $\sigma\tau \neq \tau\sigma$ in general, in this group.

(2) The groups $GL_N(\mathbb{Q})$, $GL_N(\mathbb{R})$, $GL_N(\mathbb{C})$ of invertible $N \times N$ matrices over $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Here $gh = hg$ fails too, in general.

Conventions.

– When $ab = ba$ we say that the group is abelian.

– We usually denote the operation of an abelian group by a sum, $g + h$, the unit element by 0, and the inverses by $-g$.

– This is not a general rule. What is true, however, is that if a group is denoted $(G, +)$, then the group must be abelian.

Orthogonal groups 1/4

Notations. We use the usual scalar product and norm on $\mathbb{R}^N$:

$$< x, y >= \sum_i x_i y_i \quad , \quad ||x|| = \sqrt{< x, x >}$$

Theorem. For a matrix $U \in M_N(\mathbb{R})$, the following are equivalent, and if they are satisfied, we say that U is orthogonal:

(1) $< Ux, Uy >=< x, y >$.

(2) $||Ux|| = ||x||$.

(3) $U^t = U^{-1}$, where $(U^t)_{ij} = U_{ji}$.

(4) The rows of U form an orthonormal basis of $\mathbb{R}^N$.

(5) The columns of U form an orthonormal basis of $\mathbb{R}^N$.

Proof. All this follows from $< Ux, y >=< x, U^t y >$.

Orthogonal groups 2/4

Theorem. The set formed by the orthogonal matrices

$$O_N = \left\{ U \in M_N(\mathbb{R}) \Big| U^t = U^{-1} \right\}$$

is a group, with the usual multiplication of the matrices.

Proof. Assuming $U, V \in O_N$, we have $UV \in O_N$, because:

$$(UV)^t = V^t U^t = V^{-1} U^{-1} = (UV)^{-1}$$

Also, $1_N \in O_N$, and $U \in O_N \implies U^{-1} \in O_N$.

Orthogonal groups 3/4

Theorem. The elements of O_2 fall into two classes:

(1) Rotations. The rotation of angle $t \in \mathbb{R}$ is given by the following formula:

$$R_t = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}$$

The rotations are exactly the elements of O_2 having determinant 1, and they form a group, denoted SO_2.

(2) Symmetries. The symmetry with respect to the Ox axis rotated by $t/2 \in \mathbb{R}$ is given by the following formula:

$$S_t = \begin{pmatrix} \cos t & \sin t \\ \sin t & -\cos t \end{pmatrix}$$

The symmetries are exactly the elements of O_2 having determinant -1, and they do not form a group.

Orthogonal groups 4/4

Theorem. The elements of O_N fall into two classes:

(1) Those of determinant 1, which form a group, denoted SO_N:

$$SO_N = \left\{ U \in O_N \middle| \det U = 1 \right\}$$

(2) Those of determinant -1, which do not form a group.

Proofs. For $U \in O_N$ we have $\det(UU^t) = 1$, so $\det U = \pm 1$.

The set SO_N is a group, because $\det(UV) = \det U \det V$, and its complement is not a group, because $\det(1_N) = 1$.

Finally, the various 2D formulae are well-known, and elementary.

Unitary groups 1/4

<u>Notations</u>. We use the usual scalar product and norm on $\mathbb{C}^N$:

$$< x, y >= \sum_i x_i \bar{y}_i \quad , \quad ||x|| = \sqrt{< x, x >}$$

<u>Theorem</u>. For a matrix $U \in M_N(\mathbb{C})$, the following are equivalent, and if they are satisfied, we say that U is unitary:

(1) $< Ux, Uy >=< x, y >$.

(2) $||Ux|| = ||x||$.

(3) $U^* = U^{-1}$, where $(U^*)_{ij} = \bar{U}_{ji}$.

(4) The rows of U form an orthonormal basis of $\mathbb{C}^N$.

(5) The columns of U form an orthonormal basis of $\mathbb{C}^N$.

<u>Proof</u>. All this follows from $< Ux, y >=< x, U^* y >$.

Unitary groups 2/4

Theorem. The set formed by the unitary matrices

$$U_N = \left\{ U \in M_N(\mathbb{C}) \Big| U^* = U^{-1} \right\}$$

is a group, with the usual multiplication of the matrices.

Proof. Assuming $U, V \in U_N$, we have $UV \in U_N$, because:

$$(UV)^* = V^* U^* = V^{-1} U^{-1} = (UV)^{-1}$$

Also, $1_N \in U_N$, and $U \in U_N \implies U^{-1} \in U_N$.

Unitary groups 3/4

Theorem. The determinant of a unitary matrix $U \in U_N$ must be a number on the unit circle:

$$\det U \in \mathbb{T}$$

The unitary matrices $N \times N$ having determinant 1 form a group, denoted SU_N:

$$SU_N = \left\{ U \in U_N \middle| \det U = 1 \right\}$$

Any matrix $U \in U_N$ is proportional to a matrix in SU_N, the proportionality factor being a number $d \in \mathbb{T}$.

Proof. For $U \in U_N$ we have $\det(UU^*) = 1$, so $|\det U| = 1$.

The second assertion is clear from $\det(UV) = \det U \det V$.

The third assertion follows by dividing by $d = (\det U)^{1/N}$.

Unitary groups 4/4

Theorem. We have the following formula,

$$SU_2 = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \Big| \, |a|^2 + |b|^2 = 1 \right\}$$

as well as the following formula:

$$U_2 = \left\{ d \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \Big| \, |a|^2 + |b|^2 = 1, |d| = 1 \right\}$$

Proof. For $U = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ of determinant 1, $U^* = U^{-1}$ reads:

$$\begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Thus $c = -\bar{b}, d = \bar{a}$. Finally, $\det U = 1$ gives $|a|^2 + |b|^2 = 1$.

Subgroups 1/4

The groups that we considered so far are as follows:

$$\begin{array}{ccc}
O_N & \longrightarrow & U_N \\
\uparrow & & \uparrow \\
SO_N & \longrightarrow & SU_N
\end{array}$$

It is possible to construct more groups along these lines:

(1) By multiplying by $\mathbb{Z}_r = \{w \in \mathbb{C} | w^r = 1\}$.

(2) By imposing the condition $(\det U)^s = 1$.

We can equally talk about the symplectic groups $Sp_N \subset U_N$.

Subgroups 2/4

Another big class of groups of matrices comes by looking at

$$U_N^{diag} = \mathbb{T}^N$$

and its subgroups. We have for instance the groups

$$\mathbb{Z}_{r_1} \times \ldots \times \mathbb{Z}_{r_N}$$

for any choice of numbers $r_1, \ldots, r_N \in \mathbb{N} \cup \{\infty\}$.

Subgroups 3/4

Importantly, the permutation groups S_N appear as well as groups of unitary matrices,

$$S_N \subset O_N \subset U_N$$

by making each $\sigma \in S_N$ act on the coordinate axes of $\mathbb{R}^N$. Indeed, this action is clearly isometric, so $S_N \subset O_N$.

Subgroups 4/4

In fact, any finite group G appears as a group of unitary matrices. Indeed, we can make act G on itself, by left multiplication,

$$G \subset S_G \quad , \quad \sigma_g(h) = gh$$

and so with $N = |G|$ we have embeddings as follows:

$$G \subset S_N \subset O_N \subset U_N$$

However, groups such as $D_N \subset O_N$ show that each finite group G has its own "privileged" embedding $G \subset U_N$.