Algebras and Other Stories

Part 2

Larry Susanka

June 7, 2023

Introduction

These notes accompany the second set of what will be a number of related talks in this colloquium series (not all on consecutive weeks of course!) on algebras and representation theory—critical topics in mathematical physics.

They comprise an outline of (some of) the things that were/will be said at the talks themselves.

In the previous set of talks we gave a quick review of linear algebra. Here our main objects of concern are groups. We discuss the definitions, a few theorems and most pertinent (for us) examples. Of particular interest will be representations of these in matrices.

Some groups related to tessellation or tiling of the plane are considered as interesting and important examples.

Groups

A group is a set together with an associative binary operation with identity and for which elements have inverses.

More precisely, a group is a set G together with a binary operation $\odot \colon G \times G \to G$ with the following properties.

- For all $a, b, c \in G$ we have $a \odot (b \odot c) = (a \odot b) \odot c$.
- There is an element e with $a \odot e = e \odot a = a$ for all $a \in G$.
- For each a there is an element b for which $a \odot b = b \odot a = e$.

The element b in the third item is called the inverse of a with regard to this operation. Depending on the specific notation used for $\odot$ this element may be denoted a^{-1} or $-a$. The last notation is only used when the group is commutative: i.e.

- $a \odot b = b \odot a$ for all $a, b \in G$.

Commutative groups are often called Abelian.

When studying small groups it is often convenient to specify the group operation by a "multiplication table."

Here is a table for a generic group with four elements.

$\odot$	e	a	b	c
e	e	a	b	c
a	a	a^2	$a \odot b$	$a \odot c$
b	b	$b \odot a$	b^2	$b \odot c$
c	c	$c \odot a$	$c \odot b$	c^2

Associativity and the uniqueness of inverses limits the possibilities for table entries.

There are only two possible groups (except for re-labeling of the elements) of order[1] four and both are Abelian.

[1] The order of a group is defined to be its cardinality, as a set.

When G has more than one operation in play the notation $(G, \odot)$ may be used to remind us, specifically, *which* group structure on G we have in mind.

You have seen many groups before. If $\mathcal{V}$ is any vector space $(\mathcal{V}, +)$ is an Abelian group, and that includes $(\mathbb{R}, +)$.

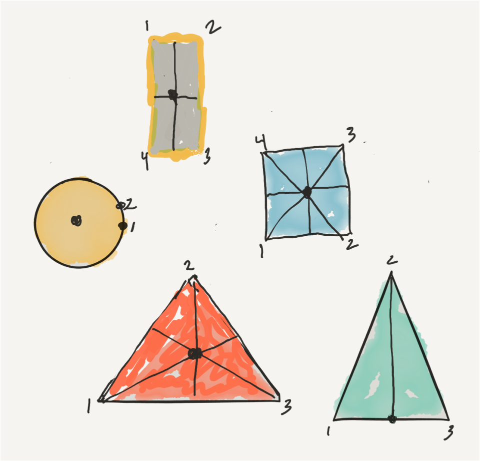
If $\mathbb{Q}$ and $\mathbb{Z}$ denote the rational numbers and integers, respectively, then $(\mathbb{Q}, +)$ and $(\mathbb{Z}, +)$ are Abelian groups.

If $\mathbb{R}_+$ and $\mathbb{R}_\emptyset$ are the positive real numbers and the nonzero real numbers, respectively, then $(\mathbb{R}_+, \cdot)$ and $(\mathbb{R}_\emptyset, \cdot)$ are Abelian groups, where $\cdot$ denotes ordinary multiplication. Also $\{-1, 1\}$ and the singleton set $\{1\}$ are groups with multiplication, subgroups of $(\mathbb{R}_\emptyset, \cdot)$.

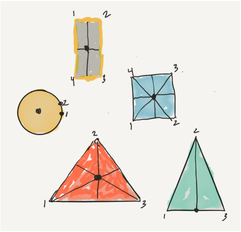
If $\mathbb{C}$ denotes the complex numbers and $\mathbb{S}$ denotes the unit complex numbers then both the nonzero complex numbers $\mathbb{C}_\emptyset$ and $\mathbb{S}$ are Abelian groups with complex multiplication.

Rotational Symmetry in Two Dimensions

Why do we think an object such as a square or an equilateral triangle or a circle is symmetric?



Rotational Symmetry Groups



We will call a "symmetry move" a way of rotating or otherwise performing a rigid motion on an object in such a way that after the motion is complete we cannot detect that anything has been done without examining the "labels" on the corners.

Composition of "symmetry moves" is a "symmetry move." Reversing a "symmetry move" is also a "symmetry move". Doing nothing is the "identity move". The collection of all symmetry moves is, therefore, a group.

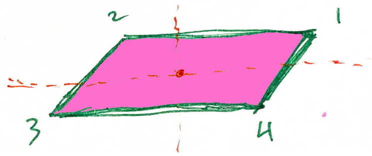
Rotational Symmetry Groups

Cataloging all the symmetry moves for a certain shape reveals important information about it. You almost get the sense that this catalog DEFINES the shape in elemental ways, maybe all the ways that are important to you. What is it, exactly, that is the same when two shapes have the same symmetry group?

Let's try to do that specifically for these shapes by "doing" the "symmetry moves" we can think of using matrices.

Remember, the matrix that acts on vectors in $\mathbb{R}^2$ to implement a linear transformation T is given by $(\, T(e_1)\ T(e_2)\,)$ where the e_i are unit vectors in the axis directions and members of $\mathbb{R}^2$ are represented as columns.

ParalleloSym: Order Two

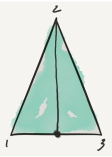


$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \quad \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$$

Reflection across the origin (180 degree rotation) is the only possible "symmetry move" here, and even *that* is made possible only by choosing the origin at the center of the parallelogram.

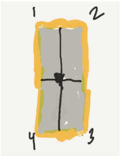
Choosing an origin is part of *recognizing* a symmetry move.

IsoscSym: Order Two



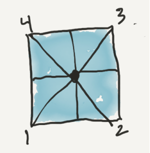
$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \quad \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}$$

RectSym: Order Four



$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \quad \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix} \quad \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \quad \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$$

SquareSym: Order Eight



$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad b = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

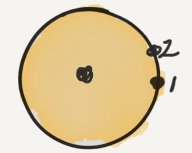
$$c = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

$$a^2 = -e \quad b^2 = c^2 = e \quad ab = -ba = c \quad cb = -bc = a \quad ca = -ac = b$$

SquareSym is *not* commutative![2]

[2] Later we encounter a *different* group of order 8 related to the quaternions.

CircleSym



$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} \cos(t) & -\sin(t) \\ \sin(t) & \cos(t) \end{pmatrix}$$
$$\begin{pmatrix} -\cos(u) & -\sin(u) \\ -\sin(u) & \cos(u) \end{pmatrix}$$

Lots of symmetry . . . BIG symmetry group . . . *not* commutative . . . lots of subgroups, including *all* the symmetry groups we looked at previously.

Lots of Subgroups

The notation $A \leq B$ indicates that A is a subgroup of B. We have:

$$\text{IsoscSym} \;\leq\; \text{RectSym} \;\leq\; \text{SquareSym} \;\leq\; \text{CircleSym}$$

What does it mean about the object when it's symmetry group is a subgroup of the symmetry group of another object?

Complex Numbers as Matrices

Letting the complex number i be represented as $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $e^{it} = \sum_{n=0}^{\infty} \frac{t^n}{n!} i^n$ it is straightforward to show that

$$e^{it} = \cos(t) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \sin(t) \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \cos(t) & -\sin(t) \\ \sin(t) & \cos(t) \end{pmatrix}$$

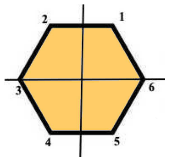
which is a rotation matrix, counterclockwise by angle t. The sum formulas for sin and cosine show that $e^{is}e^{it} = e^{i(s+t)}$. For positive integer k the matrices

$$R_k = \left\{ e^{\frac{2\pi}{k} i},\; e^{\frac{2\pi}{k} 2i},\; \ldots,\; e^{\frac{2\pi}{k} ki} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 \right\}$$

forms a group of rotations of the plane of order (that is, size) k. These groups are cyclic: that is, integer powers of a single element (in this case $e^{\frac{2\pi}{k} i}$) generate the whole group.[3]

[3] If α is an irrational multiple of π do the powers of $e^{i\alpha}$ form a group?

The Hexagon



Evaluating $e^{\frac{2\pi}{k}ni} = \begin{pmatrix}\cos\left(\frac{2\pi}{k}n\right) & -\sin\left(\frac{2\pi}{k}n\right)\\ \sin\left(\frac{2\pi}{k}n\right) & \cos\left(\frac{2\pi}{k}n\right)\end{pmatrix}$ for $k=6$ we find

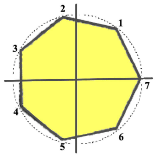
$$R_6 = \left\{ e^{\frac{\pi}{3}i},\ e^{\frac{\pi}{3}2i},\ e^{\pi i},\ e^{\frac{\pi}{3}4i},\ e^{\frac{\pi}{3}5i},\ e^{2\pi} = I_2 \right\}$$

is part of the symmetry group of the hexagon.

The rest consists of maps that reverse the order of corners and *then* rotate, so we have a symmetry group of order 12

$$\text{HexSym} = R_6 \bigcup \left(R_6 \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix} \right).$$

The Septagon



Something similar happens with odd numbers of edges/vertices.

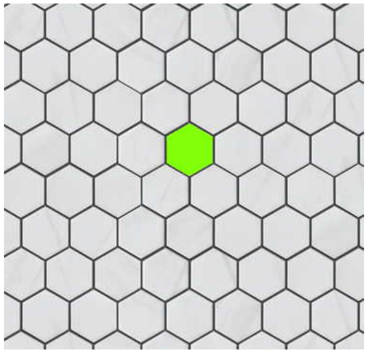
$$R_7 = \left\{ e^{\frac{2\pi}{7}i},\ e^{\frac{2\pi}{7}2i},\ e^{\frac{2\pi}{7}3i},\ e^{\frac{2\pi}{7}4i},\ e^{\frac{2\pi}{7}5i},\ e^{\frac{2\pi}{7}6i},\ e^{2\pi} = I_2 \right\}$$

with the complete symmetry group of order 14 given as

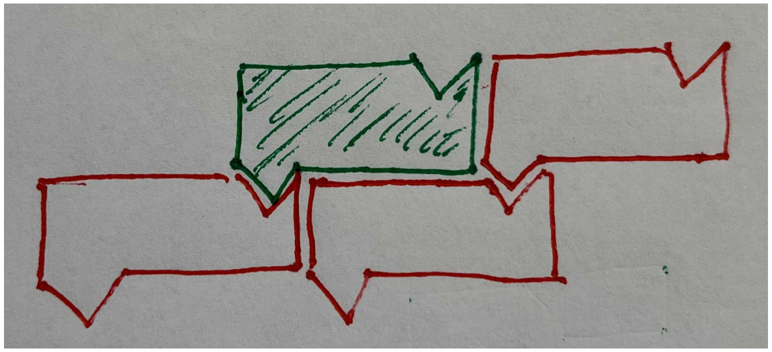
$$\text{SeptSym} = R_7 \bigcup \left(R_7 \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \right).$$

Notice here that the reflection across the y axis is *required* to produce the "second 7" of reversed rotations. With an even number of vertices either x or y reflection does the job.

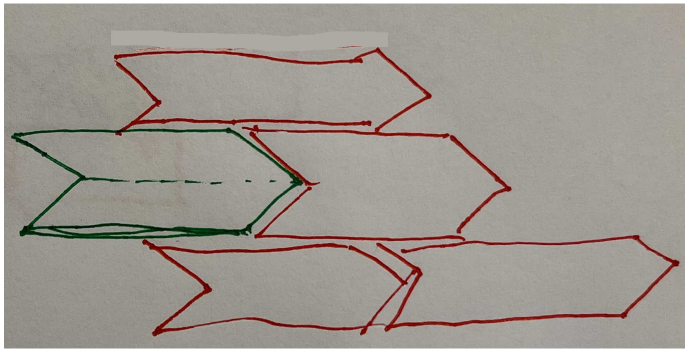
Tesselations of the Plane



The plane can be covered or "tiled" with repeating regular shapes in many ways and these patterns, also called tessellations, have been studied by many mathematicians from ancient times to this very day, including by our own mathematician/artist Luke Rawlings.



In this and the previous case the picture can be shifted in various ways and rotated/reflected to lie on itself.



These correspond to reflections/rotations in the plane coupled with translations: these "symmetry moves" are affine maps.

To analyze the regularities of the covered plane[4] one might consider both the symmetries of the individual tiles and symmetries of the overall pattern, and groups appear naturally in trying to understand both parts of this puzzle.

A symmetry of a tile must correspond to an isometry of the plane and must be affine so we don't need to consider the possibility of "wild" isometries that map a tiling onto itself, by the Mazur-Ulam Theorem.

Any linear isometry of the plane is a combination of one or two reflections, by the Cartan-Dieudonné Theorem, and two reflections form a rotation.

The affine transformations that map a tiling onto itself form a group. Any such transformation has the form $T(w) = v + Fw$ for some constant vector v and some rotation or reflection F.

[4] There are "quasi-repeating" tilings called Penrose tilings which are fascinating and exhibit patterns, even reflection or rotational symmetries, but **not** translational symmetries. Their study goes well beyond our introduction.

Suppose H is a group of translations that "preserve" a tessellation and G is a group of linear transformations (i.e. rotations and/or reflections) that also preserve it. Then any affine map of the form

$$T(w) = v + Fw$$

will too if the maps $A(w) = v + w$ and $B(w) = Fw$ are in H and G, respectively.

If $S(w) = z + Mw$ is another such then $K = S \circ T$ must also preserve the tiling.

$$\begin{aligned} K(w) = (S \circ T)(w) = S(v + Fw) &= z + M(v + Fw) \\ &= Mv + (z + MFw). \end{aligned}$$

So the translations v and the linear transformations M must be closely related: any M in G must map any translation vector from H to another translation vector from H.

If $(H, \odot)$ and $(G, \otimes)$ are groups the direct product group is defined with set $H \times G = \{ (h, g) \mid h \in H,\ g \in G \}$ with operations $(h_1, g_1)(h_2, g_2) = (h_1 \odot h_2,\ g_1 \otimes g_2)$.

However if we consider the situation of symmetry group of the previous slide where H is a group of translations and G is a group of linear transformations, composition of affine maps corresponds to operation

$$(z, M)(v, F) = (z + Mv, MF)$$

and not

$$(z, M)(v, F) = (z + v, MF).$$

The product set with operation corresponding to composition of affine functions is called a semidirect product and this type of group is the one studied by crystallographers and . . . some mathematicians.

Lets take another look at the set of affine transformations: all maps from $\mathbb{R}^2$ to $\mathbb{R}^2$ of the form

$$T(w) = v + Fw$$

for 2×2 matrix F and $v \in \mathbb{R}^2$.

The action of T on w can be calculated as the top two entries of

$$\begin{pmatrix} F & v \\ 0\,0 & 1 \end{pmatrix}\begin{pmatrix} w \\ 1 \end{pmatrix} = \begin{pmatrix} f_{1,1} & f_{1,2} & v_1 \\ f_{2,1} & f_{2,2} & v_2 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} w_1 \\ w_2 \\ 1 \end{pmatrix} = \begin{pmatrix} Fw + v \\ 1 \end{pmatrix}.$$

The product of this matrix with another representing affine S

$$\begin{pmatrix} M & z \\ 0\,0 & 1 \end{pmatrix}\begin{pmatrix} F & v \\ 0\,0 & 1 \end{pmatrix} = \begin{pmatrix} MF & z + Mv \\ 0\,0 & 1 \end{pmatrix}$$

has the same form, so compositions of affine functions and, ultimately, $S \circ T(w)$ itself, can be calculated by matrix multiplication alone.

The set of all these 3×3 matrices is a group, designated Aff_2.

$\mathbb{Z}_n$ AND $_n$

$\mathbb{Z}_n$ is the non-negative integers less n made into a group with $\bmod\ n$ arithmetic.

We let $a + b \mod n$ be the remainder of $a + b$ after division by n. Any such group is Abelian.

Thus in $\mathbb{Z}_2$ we have set $\{0, 1\}$ and $1 + 1 \mod 2 = 0$.

And in $\mathbb{Z}_4$ we have set $\{0, 1, 2, 3\}$ with

$$\begin{aligned} 1+1 \mod 4 &= 2, & 1+2 \mod 4 &= 3, & 1+3 \mod 4 &= 0, \\ 2+2 \mod 4 &= 0, & 2+3 \mod 4 &= 1, & 3+3 \mod 4 &= 2. \end{aligned}$$

$\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$, which has set $\{(0,0), (1,0), (0,1), (1,1)\}$, are the two possible groups[5] of order 4: any member of $\mathbb{Z}_2 \times \mathbb{Z}_2$ added to itself is the identity. But in $\mathbb{Z}_4$ we find $3 + 3 \mod 4 = 2$.

[5] We will prove this later.

$_n$ is the group of positive integers less than n and relatively prime to n with multiplication $\bmod\ n$. (By definition this always includes 1.)

Using the fact that integers a and n are relatively prime if and only if there are integers x and y for which $xa + yn = 1$ it is straightforward to show that $\bmod\ n$ multiplication is closed in $_n$. These groups are all Abelian too.

For instance $_8$ has set $\{1, 3, 5, 7\}$ and so its table must be like the table of $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

But 9, 25 and 49 are all "equal to" or in the usual vocabulary "congruent to" 1 in $\bmod\ 8$ arithmetic, we see the table matches that of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

The order or "size" of $_n$ is not so easy to determine as n grows. That number is called "Euler's totient function" and explicit formulas for it involve the prime factorization of n.

THE QUATERNION GROUP

The group of order 8 given by set $\{\pm 1, \pm\vec{\imath}, \pm\vec{\jmath}, \pm\vec{k}\}$ and multiplication table determined by associativity and

$$\vec{\imath}^{\,2} = \vec{\jmath}^{\,2} = \vec{k}^{\,2} = -1 \text{ and } \vec{\imath}\,\vec{\jmath} = \vec{k}, \quad \vec{\jmath}\,\vec{k} = \vec{\imath}, \quad \vec{k}\,\vec{\imath} = \vec{\jmath}$$

is called the quaternion group. I am tempted to call this one *Quat*, but the anti-euphonious nature of the word forbids it.

$$\text{The set} \quad \mathbb{H} = \{ w + x\vec{\imath} + y\vec{\jmath} + z\vec{k} \mid w, x, y, z \in \mathbb{R} \}$$

is a four-dimensional real vector space and will be important to us later. It contains the quaternion group and its nonzero members $\mathbb{H}_0$ form a group themselves with the implied multiplication. The unit sphere of quaternions may be identified with the 3-dimensional sphere in $\mathbb{R}^4$ and may be denoted $\mathbb{S}^3$.

$\mathbb{S}^3$ allows us to handle rotations in $\mathbb{R}^3$ in a way that is similar to how complex numbers do in the plane.

Quaternion's "Are" Matrices Too

As with complex numbers, you can reproduce the quaternion multiplication table using matrices as group elements, and in this sense the quaternions "are" matrices.

Consider the real vector space consisting of all matrices which can be formed, for real w, x, y and z, as

$$\begin{aligned} Q =& w \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + x \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} + y \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + z \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \\ =& \begin{pmatrix} w & 0 \\ 0 & w \end{pmatrix} + \begin{pmatrix} yi & -x+zi \\ x+zi & -yi \end{pmatrix} = \begin{pmatrix} w+yi & -x+zi \\ x+zi & w-yi \end{pmatrix}. \end{aligned}$$

The matrix Q is associated with $q = w + x\vec{i} + y\vec{j} + z\vec{k}$.

The unit quaternions are those for which $w^2 + x^2 + y^2 + z^2 = 1$. These matrices are exactly those complex matrices for which $MM^* = I_2$ and they are also known as special unitary matrices.

A Bit More Notation involving Quaternions

You may recall that $\mathbb{S}$ is the set of rotations in the plane, which may be identified with the group of unit complex numbers and also the unit circle in the plane.

If conjugation of quaternion $q = w + x\vec{i} + y\vec{j} + z\vec{k} = w + \vec{v}$ is given by $q^* = w - \vec{v}$ then the square magnitude[6] of q is given as the positive real number $qq^* = w^2 + x^2 + y^2 + z^2$. A rather tedious calculation shows that $\|pq\| = \|p\| \, \|q\|$ for any p, q.

It follows that $\mathbb{S}^3$, the unit-magnitude quaternions, is also a group with Hamilton product.

Note that $\mathbb{S}^n$ is the unit sphere in $\mathbb{R}^n$ and *not* the set of n-tuples $\mathbb{S} \times \cdots \times \mathbb{S}$, whose coordinates are points on the unit circle or, if you prefer, unit magnitude complex numbers. That direct product group is called a torus, denoted $\mathbb{T}^n$.

[6] Unlike complex conjugation, we have $(pq)^* = q^*p^*$ and *not* $(pq)^* = p^*q^*$.

Continuous Groups

CircleSym is different from the other symmetry groups: it is "continuous" in the sense that its members can be identified by a continuous matrix-valued function of a real parameter.

$$\begin{pmatrix} \cos(t) & -\sin(t) \\ \sin(t) & \cos(t) \end{pmatrix} \qquad \begin{pmatrix} -\cos(u) & -\sin(u) \\ -\sin(u) & \cos(u) \end{pmatrix}$$

Members of $\mathbb{H}_0$, the group of nonzero quaternions,

$$w + x\vec{i} + y\vec{j} + z\vec{k}$$

are also defined by the real coefficients on 1, $\vec{i}$, $\vec{j}$ and $\vec{k}$.

We will see that the quaternions themselves can be represented as matrices, so the nonzero quaternions can be represented as a continuous group of matrices with four real parameters.

The continuous Heisenberg group, $H_3(\mathbb{R})$, is the set of 3×3 matrices of the form $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ with three real parameters.

If $A = I_3 + U_1$ and $B = I_3 + U_2$ are two Heisenberg matrices then $AB = I_3 + U_1 + U_2 + U_1U_2$ which is also a Heisenberg matrix. And

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}.$$

It is a subgroup of the six-parameter group of affine transformations in two dimensions, Aff_2, the group of matrices of the form

$$\begin{pmatrix} f_{1,1} & f_{1,2} & v_1 \\ f_{2,1} & f_{2,2} & v_2 \\ 0 & 0 & 1 \end{pmatrix}$$

We will want to consider $n \times n$ matrices with real, complex or quaternion entries. The real vector space of these will be denoted $\mathbb{M}_{n\times n}(\mathbb{F})$ where $\mathbb{F}$ is one of $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$.

Since $\mathbb{C}$ has dimension 2 over $\mathbb{R}$ and $\mathbb{H}$ has dimension 4 over $\mathbb{R}$ it is easy to see that these matrix vector spaces have dimensions n^2, $2n^2$ or $4n^2$ as real vector spaces.

$$\begin{aligned} \mathbb{F} = \mathbb{C} \qquad & M = M_1 + iM_2 \\ \mathbb{F} = \mathbb{H} \qquad & M = M_1 + M_2\vec{i} + M_3\vec{j} + M_4\vec{k} \\ & \quad = (M_1 + M_2\vec{i}\,) + (M_3 + M_4\vec{i}\,)\,\vec{j}. \end{aligned}$$

$GL_n(\mathbb{F})$ consists of the members of $\mathbb{M}_{n\times n}(\mathbb{F})$ which are nonsingular: that is

$$Mx = 0 \text{ implies } x = 0 \text{ where } x \text{ is taken from } \mathbb{F}^n.$$

In the real or complex case this happens exactly when M is invertible, and that happens exactly when M has nonzero determinant. But the usual definition of determinant uses the commutative property throughout, and so the determinant construction fails for quaternionic matrices.

Still, quaternionic M is nonsingular exactly when it has an inverse matrix[7], and by representing quaternions themselves as matrices a determinant condition equivalent to invertibility can be resurrected for quaternionic matrices too.

$GL_n(\mathbb{F})$ is a group for each n and for all three possibilities for $\mathbb{F}$.

[7] A one-sided quaternionic inverse matrix is actually a two-sided inverse, but this is not entirely obvious.

$GL_n(\mathbb{F})$ has lots of named subgroups corresponding to various properties and the names vary depending on $\mathbb{F}$.

For instance O_n is the subgroup of $GL_n(\mathbb{R})$ consisting of the orthogonal matrices[8] that is, those matrices with $M^T = M^{-1}$. Note: such matrices must have determinant ± 1.

The real special linear matrices and $SL_n(\mathbb{R})$ are the matrices with determinant 1.

The intersection of any two subgroups of a group is also a subgroup, and in this case we have $O_n \cap SL_n(\mathbb{R}) = SO_n$, the special orthogonal group.

These groups will all be very important to us later.

[8] CircleSym is actually O_2, and SO_2 is the subgroup consisting of the matrices with positive determinant.

U_n, the unitary matrices, is the subgroup of $GL_n(\mathbb{C})$ consisting of those matrices for which $M^*M = I_n$ where M^* denotes the Hermitian conjugate of matrix M, the conjugate transpose of M, and I_n is the $n \times n$ identity matrix.

The determinant of a unitary matrix must have *magnitude* 1. The complex matrices with determinant 1 is denoted $SL_n(\mathbb{C})$, the complex special linear group.

The subgroup of U_n consisting of those matrices whose determinant is *actually* 1, $U_n \cap SL_n(\mathbb{C})$, is called the special unitary group and denoted SU_n.

We will consider symplectic groups and groups of quaternionic matrices later.

None of these groups are commutative.

A Nomenclature Puzzle

These groups have been studied for over 100 years and every conceivable feature and property is known and recorded. Somewhere. I find it entirely odd that the group of real matrices with determinant ±1 has no name, other than its defining description. Nor does the group of complex matrices with determinant of *magnitude* 1. If $\|\det(M)\| = \|\det(N)\| = 1$ then

$$\|\det(MN)\| = \|\det(M)\det(N)\| = \|\det(M)\|\,\|\det(N)\| = 1.$$

$$\begin{aligned} 1 = \ & \det(I_n) = \|\det(MM^{-1})\| \\ = \ & \|\det(M)\|\,\|\det(M^{-1})\| = \|\det(M^{-1})\|. \end{aligned}$$

I have queried and received null responses from 8 different mathematicians including one famous author of a linear algebra text, two other not-so-famous authors of such texts, an author of a wonderful text on Lie Groups and Algebras and an author of a well-known book on Matrix Analysis.

I posted the question to the Math Stack Exchange site at math.stackexchange.com. No joy.

ChatGPT4 gave responses (yes, it was PROBED) that sounded like a student who hadn't done enough homework trying to transform BS and fancy vocabulary into an answer on an essay exam. It was very polite though.

A puzzle.

Group Homomorphisms

A group homomorphism is a map $F\colon (G, \odot) \to (H, \cdot)$ between two groups that preserves the group operation.

$$F(g \odot k) = F(g) \cdot F(k) \quad \text{for all} \quad g, k \in G.$$

If group homomorphism F is invertible then F^{-1} is also a group homomorphism and it is called a group isomorphism. It is called a group endomorphism if $(G, \odot) = (H, \cdot)$ and a group automorphism if it is an invertible group endomorphism.

This vocabulary is very similar to the vocabulary for linear transformations on a vector space, and in fact variants of these terms are to be found throughout mathematics.

We write $G \cong H$ if G and H are isomorphic groups.

Isomorphic groups are regarded as, essentially, the same group. They are two manifestations of the same group structure.

A permutation of any set G is a one-to-one and onto function $P\colon G \to G$. So invertible P "switches around" the members of G. The set of ALL permutations on G is a group with composition of functions, denoted $Perm_G$. The identity map id on G is the group identity. Every group $(G, \cdot)$ is (isomorphic to) a subgroup of a permutation group. To see this we will create a group isomorphism.

If $g \in G$ define $F_g\colon G \to G$ by $F_g(h) = g \cdot h$ for all $h \in G$.

So if g_1 and g_2 are in G then for every $h \in G$

$(F_{g_1} \circ F_{g_2})(h) = F_{g_1}(g_2 \cdot h) = g_1 \cdot (g_2 \cdot h) = (g_1 \cdot g_2) \cdot h = F_{g_1 \cdot g_2}(h).$

So $F_{g_1} \circ F_{g_2} = F_{g_1 \cdot g_2}$ and in particular we have $F_{g^{-1}} \circ F_g = F_e = id$.

Let H be the set of all F_g for $g \in G$.

$(H, \circ)$ is a subgroup of $(Perm_G, \circ)$.

Then the function $\Psi\colon G \to H$ given by $\Psi(g) = F_g$ for each $g \in G$ is a group isomorphism onto H.

We now show that any group of permutations G on a finite set $A = \{1, \ldots, n\}$ is associated with a group of $n \times n$ matrices with matrix multiplication. If σ is a permutation let

$$\Psi(\sigma) = \left(e_{\sigma(1)}\; e_{\sigma(2)}\; \cdots\; e_{\sigma(n)}\right)$$

be the matrix of column basis vectors in permuted order. So $\Psi(\sigma)(e_i) = e_{\sigma(i)}$ for each i. This matrix re-orders the column vectors in the same way that σ re-orders the integers.

A calculation shows that

$$\Psi(\sigma)\Psi(\tau) = \Psi(\sigma \circ \tau)$$

and so this set of matrices with matrix multiplication is isomorphic to the permutation group G.

The composition of isomorphisms is an isomorphism. Our conclusion is that any permutation group on a finite set of integers—and therefore any finite group at all—is isomorphic to a group of permutation matrices.

Here is another interesting isomorphism. Consider the group $(\mathbb{R}^n, +)$, the vectors with ordinary vector addition.

Consider too the $n \times n$ matrices of the form $(\lambda_1, \ldots, \lambda_n)$ where the numbers λ_i are **positive**, arranged along the diagonal of the matrix, with all other entries 0. The set $(H, \cdot)$ of all matrices of this form with matrix multiplication is a group, a subgroup of the group of all invertible $n \times n$ matrices.

Define $\Psi\colon \mathbb{R}^n \to H$ on $x \in \mathbb{R}^n$ by $\Psi(x) = diag\left(e^{x^1}, \ldots, e^{x^n}\right)$.

It is easy to show that $\Psi(x + y) = \Psi(x) \cdot \Psi(y)$, that Ψ is invertible (apply the logarithm function to the diagonal elements) and is an isomorphism.

This is an example of something that will be of concern to us in more complex (and, arguably, more interesting) situations: the **representation** of a group as a group of matrices with matrix multiplication.

Counting with Cosets

If S is a subgroup of group G and $g \in G$ the sets

$$gS = \{\, gs \mid s \in S\} \quad \text{and} \quad Sg = \{\, sg \mid s \in S\}$$

are called left or, respectively, right cosets of S in G.

$gS \subset S$ if and only if $g \in S$ if and only if $gS = S$ and the same is true for right cosets.

And if $gS \cap hS \neq \varnothing$ then there are members $s_1, s_2 \in S$ with

$$gs_1 = hs_2 \implies h^{-1}g = s_2 s_1^{-1} \in S.$$

It follows that $hS = hh^{-1}gS = egS = gS$. So left cosets are either disjoint or equal. The same result holds for right cosets.

Since cosets partition G and cosets all have the same cardinality we have $|G| = (\text{number of left cosets})|S|$ where we use $|A|$ to denote the cardinality of set A. Therefore the cardinality of any subgroup S must divide the cardinality of G.

This counting principle is a powerful tool to understanding the structure of groups of a given cardinality.

If G is a group and $g \in G$ the cyclic group generated by g, denoted (g), is the commutative group consisting of all g^n where $n \in \mathbb{N}$. This set could be finite or infinite, and the cardinality of (g) is called the order of g. The order of any element of g is a factor of the cardinality of G.

You may recall that I said there were only two groups of order 4, and we can prove this easily now.

Suppose G is such a group. It either has an element of order 4 or not. If $|(g)| = 4$ then $G = (g)$ and its table is determined. If not it has three elements of order 2 and one (the identity) of order 1. In that case its table is determined also, and easily seen to be (isomorphic to) $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Normal Subgroups and the Kernel

A subgroup N of group G it is called normal if $gNg^{-1} \subset N$ for every $g \in G$. This implies $gN \subset Ng$ and (switching g and g^{-1}) $Ng \subset gN$ for every g, so $gN = Ng$ for every g and $gNg^{-1} = N$.

Left and right cosets coincide for a normal subgroup.

If $T \colon G \to H$ is a group homomorphism it is easy to show that the kernel of T, defined by $\ker(T) = \{ g \in G \mid T(g) = e_H \}$, where e_H is the identity element of H, is a normal subgroup.

$\ker(T)$ is nonempty, since $T(e_G)$ must equal e_H. It could also, possibly, be all of G if T is the trivial homomorphism. And $\ker(T) = \{ e_G \}$ if and only if T is one-to-one.

If A, B are two nonempty subsets of group G define

$$AB = \{ab \mid a \in A, b \in B\}$$

If N is normal in G and W is the set of cosets of N then a product on W given by

$$gN \odot hN = (gN)(hN) = (Ng)(hN) = NghN = (ghN)N = ghN$$

is well-defined (that is, it doesn't depend on the representatives gN and hN chosen to define it) and makes W into a group called the quotient group of G by N. The quotient group W is usually denoted G/N. Its identity is the coset $N = e_G N$. The function

$$T \colon G \to G/N \text{ via } T(g) = gN$$

is a group homomorphism with kernel N.

So normal subgroups coincide exactly with the kernels of homomorphisms.

Suppose $T \colon G \to H$ is a group homomorphism.

Define the image of T to be the set

$$T(G) = \{T(g) \mid g \in G\} \subset H.$$

Note that $T(G)$ is closed under multiplication in H, since every element in $T(G)$ is of the form $T(g)$. So $T(g)T(h) = T(gh) \in T(G)$.

Also, if $T(g) \in T(G)$ then $e_H = T(e_G) = T(gg^{-1}) = T(g)T(g^{-1})$ so $T(g^{-1}) = T(g)^{-1} \in T(G)$.

This means $T(G)$ is a subgroup of H.

The First Isomorphism Theorem

Let $N = \ker(T)$. Then G/N is isomorphic to the image $T(G)$ of T.

Define $\Psi \colon T(G) \to G/N$ by $\Psi(T(g)) = gN$.

If $T(g) = T(h)$ then $T(h^{-1}g) = e_H$ so $h^{-1}g \in N$. But then $hN = hh^{-1}gN = gN$. So Ψ is well-defined.

And it is obviously onto: any $gN \in G/N$ is $\Psi(T(g))$.

$\Psi(T(g)) = \Psi(T(h))$ implies $hN = gN$ so $h^{-1}g \in N = \ker(T)$. So $T(h)e_H = T(h)T(h^{-1}g) = T(hh^{-1}g) = T(g)$: that is, Ψ is also one-to-one.

Finally,

$$\Psi(T(g)T(h)) = \Psi(T(gh)) = ghN = gNhN = \Psi(T(g))\Psi(T(h))$$

So Ψ is a homomorphism, and invertible: $T(G) \cong G/N$.

Simple Groups

A group is called simple if it has no nontrivial normal subgroups. This is equivalent to saying that the only nontrivial homomorphisms with domain G are isomorphisms[9].

Simple groups are important because they are "rigid" in the sense that there is no way to "switch around" their members except in ways that preserve *everything important* about the group. Simple groups are the "atoms" of the group "periodic table." An important goal in understanding a group is to understand how its atoms—the simple groups that may be nested inside if it is not, itself, simple—are organized.

The words "simple" and "irreducible" are related, and we will have more to say about this later.

[9] No commutative group of non-prime order can be simple. So simplicity is a concept more relevant for *non-commutative* groups.

More Examples of Homomorphisms and Normal Subgroups

Let $\mathbb{S}$ denote the group of complex numbers of norm 1 and define $T\colon \mathbb{R} \to \mathbb{S}$ by $T(x) = e^{2\pi x\, i}$. So T is onto $\mathbb{S}$ but *not* one-to-one. And $T(x+y) = e^{2\pi(x+y)\, i} = e^{2\pi x\, i}e^{2\pi y\, i} = T(x)T(y)$ so T is a group homomorphism.

$T(x) = 1$ if and only if $x \in \mathbb{Z}$ so $\mathbb{Z} = \ker(T)$.

That means $\mathbb{S} \cong \mathbb{R}/\mathbb{Z}$.

For $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$ we know that $\det\colon GL_n(\mathbb{F}) \to \mathbb{F}_{\emptyset}$ is a group homomorphism.

$\ker(\det) = SL_n(\mathbb{F})$ and so $GL_n(\mathbb{F})/SL_n(\mathbb{F}) \cong \mathbb{F}_{\emptyset}$

Let $\mathbb{S}^3$ denote the group of quaternions[10] of norm 1. This is the 3-dimensional sphere in $\mathbb{R}^4$. We identify $\mathbb{R}^3$ with the space of pure quaternions in $\mathbb{R}^4$.

It is a fact (references provided upon request) that any rotation in space (i.e a member of SO_3) can be implemented using unit quaternions as either $q\vec{v}q^*$ or $(-q)\vec{v}(-q^*)$ where $q \in \mathbb{S}^3$ and $\vec{v}$ is a point in space, and these two quaternions $\pm q$ are the only two quaternions that will act as this rotation. And any map $\vec{v} \to q\vec{v}q^*$ is an isometry on space with determinant 1 and so is actually a rotation.

The map $T\colon \mathbb{S}^3 \to SO_3$ given by this map is a homomorphism:

$$T(pq)\vec{v} = (pq)\vec{v}(pq)^* = pq\vec{v}q^*p^* = p(T(q)(\vec{v}))p^* = T(p)T(q)\vec{v}.$$

So $SO_3 \cong \mathbb{S}^3/\{\pm 1\}$.

Note: $\mathbb{S}^n/\{\pm 1\}$ is called real projective space, denoted $\mathbb{RP}^n$.

[10] We will see later that $\mathbb{S}^3 \cong SU_2$.

It is a fact (references provided upon request) that any rotation in $\mathbb{R}^4$ (i.e a member of SO_4) can be implemented using unit quaternions as either pwq^* or $(-p)w(-q^*)$ where p and q are in $\mathbb{S}^3$ and w is a point in $\mathbb{R}^4$: that is, a quaternion.

The two pairs of quaternions (p, q) and $(-p, -q)$ are the only two unit quaternion pairs that will act as this rotation. And any map $w \to pwq^*$ is an isometry on $\mathbb{R}^4$ with determinant 1 and so is actually a rotation of $\mathbb{R}^4$.

The map $T\colon \mathbb{S}^3 \times \mathbb{S}^3 \to SO_4$ given by this map is a homomorphism and this is proved by means very similar to the previous slide.

So $SO_4 \cong (\mathbb{S}^3 \times \mathbb{S}^3)/\{\,(1,1),\ (-1,-1)\,\}$.

A Compendium of Examples

We have seen MANY example groups in this chunk of slides.

$\mathcal{V}$ (any vector space) and , $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}, \mathbb{H}, \mathbb{M}_{n \times n}(\mathbb{F})$ with addition

$\mathbb{R}_+, \mathbb{R}_\emptyset, \mathbb{C}_\emptyset, \mathbb{H}_\emptyset$ and the tori $\mathbb{T}^n$ with multiplication

$\{-1, 1\}$, $\mathbb{S}$ and $\mathbb{S}^3$ (unit spheres of dimensions 0, 1, 3)

Parallelo, *Isosc*, *Rect*, *Square*, *Circle*, *Hex*, *Sept* (symmetry)

R_k (finite cyclic, order k) Aff_2 (affine group in two dimensions)

$\mathbb{Z}_n$ and $\mathit{RelPrime}_n$ (finite abelian, mod n arithmetic on integers)

Quat and $H_3(\mathbb{R})$ (Heisenberg) and Perm_G (permutations)

$GL_n(\mathbb{F}),\ SL_n(\mathbb{R}),\ SL_n(\mathbb{C})$ (general and special linear)

Real matrices: $O_n,\ SO_n$ (orthogonal and special orthogonal)

$\mathbb{RP}^3 = \mathbb{S}^3/\{\pm 1\}$ (real projective space of dimension 3)

Complex matrices: $U_n,\ SU_n$ (unitary and special unitary)