Math 417 Intro to abstract algebra

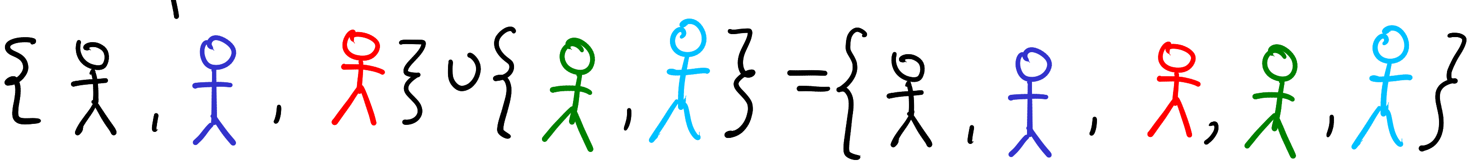
Lecture 1

What is abstract algebra?

"Abstract": from Latin "abstraho" meaning "to pull away."

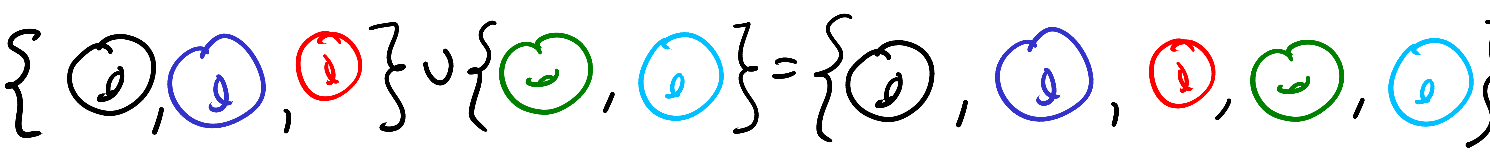
"Algebra": from title of 9th Century treatise:
ٱلْكِتَاب ٱلْمُخْتَصَر فِي حِسَاب ٱلْجَبْر وَٱلْمُقَابَلَة
by al-Khwarizmi. The word means "restoring broken parts" and originally refered to one particular method but now represents the whole subject.

Example of abstraction:



3 people 2 people 5 people

$$3+2=5$$



3 donuts 2 donuts 5 donuts

$$3+2=5$$

When we learn to count, we "draw away" from the particular kind of objects (people, donuts) and consider only their number.

Addition has various properties

- $(a+b)+c = a+(b+c)$
- $a+0 = 0+a = a$
- $a+(-a) = (-a)+a = 0$
- $a+b = b+a$

These rules hold no matter what numbers a, b, c are. We can apply them without knowing the specific values.

Abstract algebra takes this to another level: we don't even assume that a, b, c are numbers, but merely some things that can be combined so that certain rules hold.

A set of objects
+ one or more operations
+ a list of rules

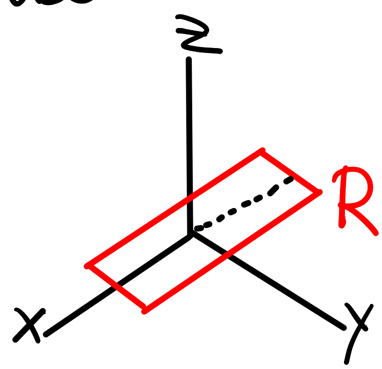
} <u>Algebraic Structure</u>

Algebraic structures in 417:
Groups, Rings, and Fields (most of the course deals with groups)

<u>Groups</u>: Start by considering some examples.

1. Symmetries

Imagine a rectangle R sitting in xy-plane in 3D space.



Consider the rotations of 3D space that bring R back to itself.

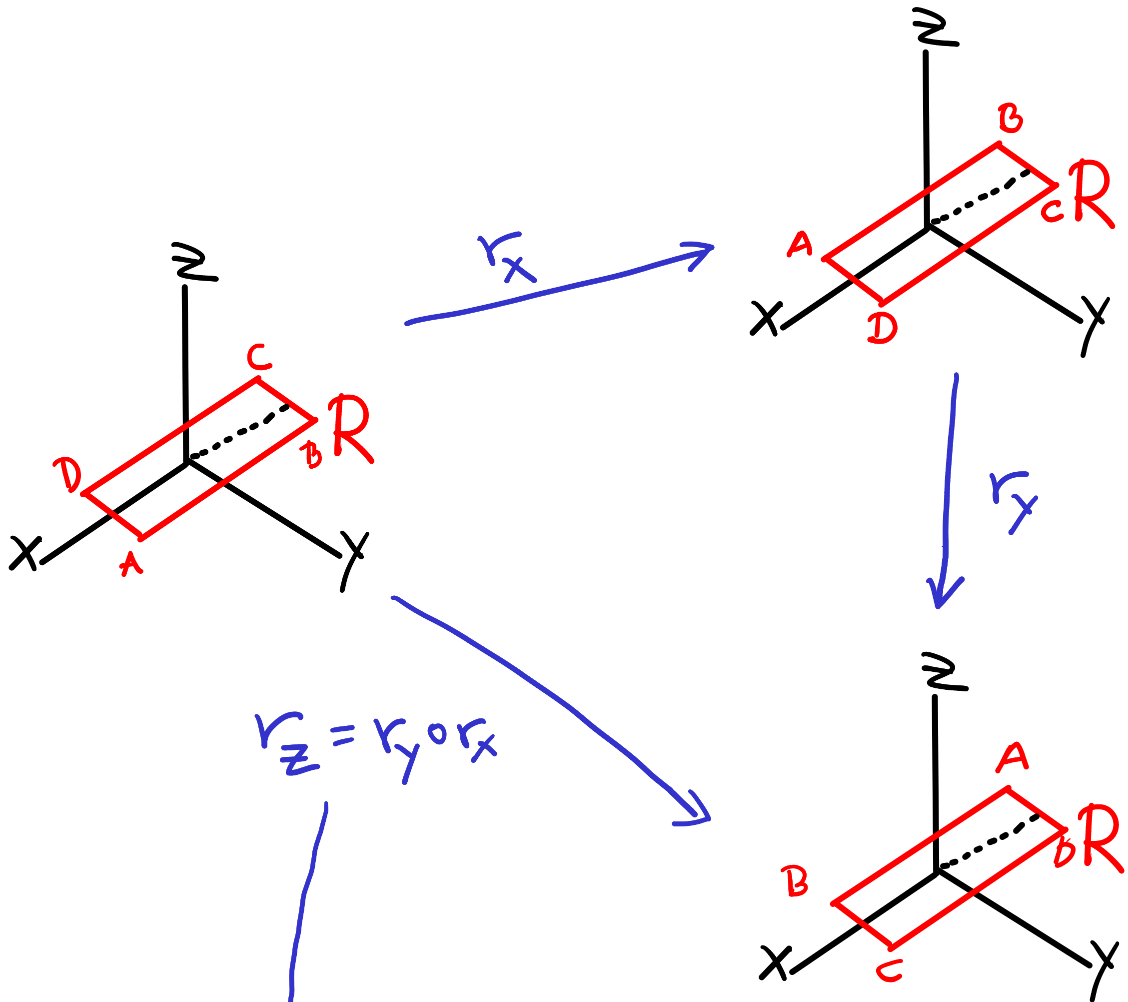
r_x = Rotation by π around x-axis

r_y = Rotation by π around y-axis

r_z = Rotation by π around z-axis

I = do nothing "Identity transformation"

What if we do one rotation r that takes $R \to R$ followed by another rotation r' that takes $R \to R$? We write $r' \circ r$ for this transformation, the <u>composition</u> of r and r'. Then $r' \circ r$ is another rotation that takes $R \to R$.



$r_z = r_y \circ r_x$

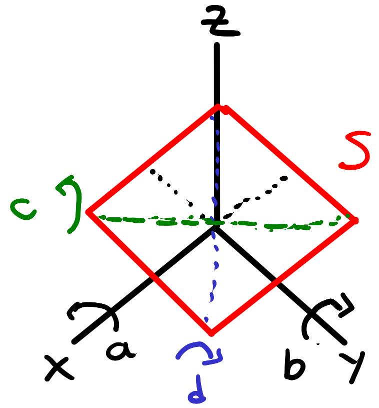
	I	r_x	r_y	r_z
I	I	r_x	r_y	r_z
r_x	r_x	I		
r_y	r_y	r_z	I	
r_z	r_z			I

"multiplication" table: entry in row r' and column r is $r' \circ r$

Symmetries of $R = \{I, r_x, r_y, r_z\}$

This is an example of a group.

S = square. More "symmetric" than R, so has more symmetries.



I = do nothing

r = rotate by $\pi/2$ around z-axis.

r^2 = rotate by π around z-axis.

r^3 = rotate by $3\pi/2$ around z-axis.

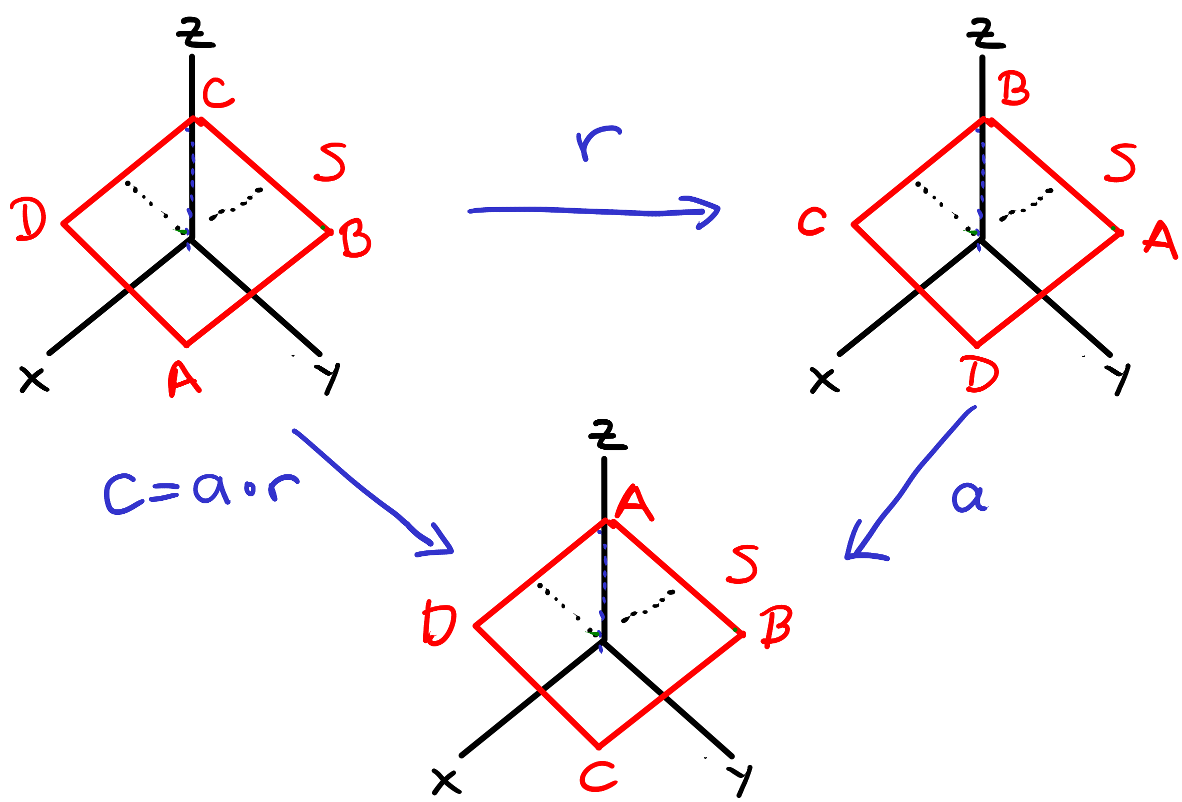
a = rotate by π around x-axis.

b = rotate by π around y-axis.

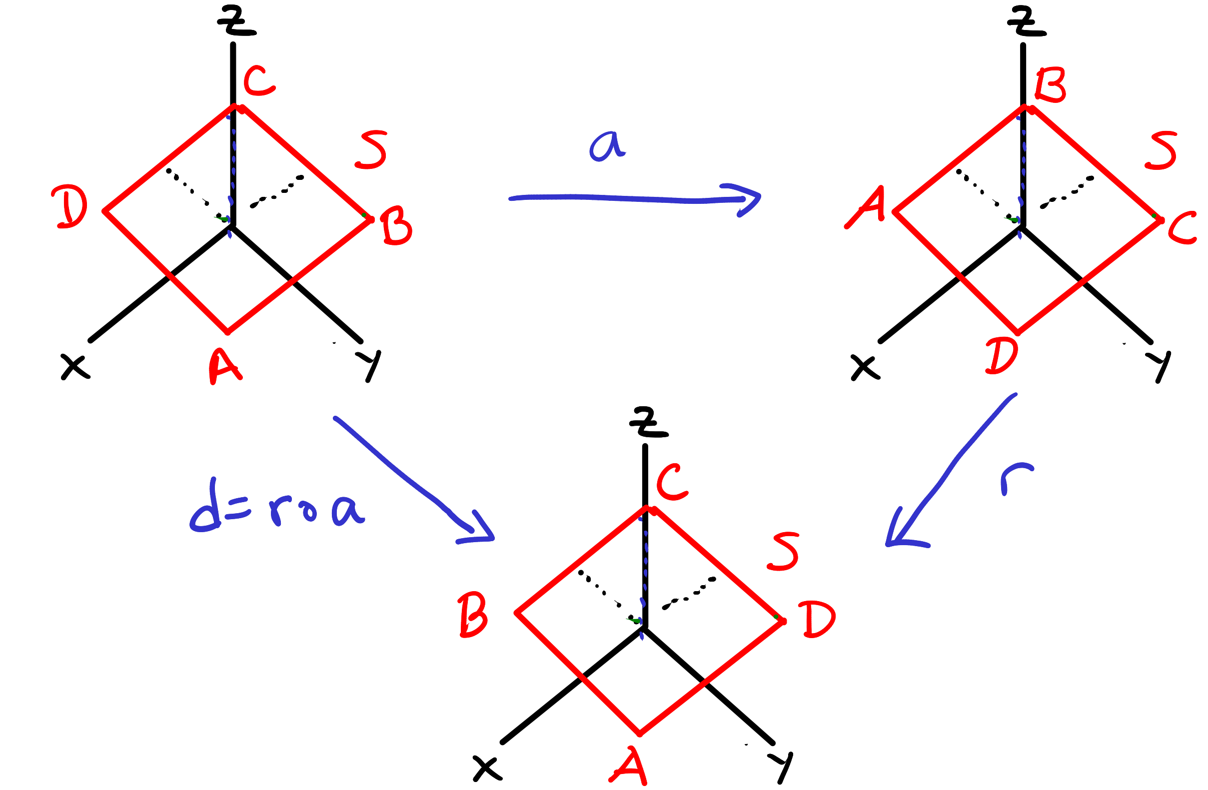
but now also: c = rotate by π around diagonal.

d = rotate by π around other diagonal.

Symmetries of $S = \{I, r, r^2, r^3, a, b, c, d\}$



Other order:



Multiplication table:

	I	r	r^2	r^3	a	b	c	d
I	I	r	r^2	r^3	a	b	c	d
r	r	r^2	r^3	I	d			
r^2	r^2	r^3	I	r				
r^3	r^3	I	r	r^2				
a	a	c						
b	b							
c	c							
d	d							

exercise: fill out the rest.

3D space = vector space $\mathbb{R}^3$.

Rotations are linear transformations of $\mathbb{R}^3$, so can be represented by 3×3 matrices.

composition $\leftrightarrow$ matrix multiplication.

<u>Rectangle example:</u>

$$r_x(x,y,z) = (x,-y,-z) \quad \leftrightarrow \quad r_x = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

$$r_y(x,y,z) = (-x,y,-z) \quad \leftrightarrow \quad r_y = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

$$r_z(x,y,z) = (-x,-y,z) \quad \leftrightarrow \quad r_z = \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$I(x,y,z) = (x,y,z) \quad \leftrightarrow \quad I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Now $\quad r_x r_y = \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = r_z$

<u>Square example:</u>

$$r(x,y,z) = (y,-x,z) \quad \leftrightarrow \quad r = \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$a(x,y,z) = (x,-y,-z) \quad \Leftrightarrow \quad a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

Then $ra = \begin{bmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix} = d$

$ar = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix} = c$.

Let us formalize the concept of "symmetries of an object $R \subset \mathbb{R}^3$"

Distance: $\vec{x} = (x_1, x_2, x_3)$ $\vec{y} = (y_1, y_2, y_3)$

$$d(\vec{x},\vec{y}) = \|\vec{x} - \vec{y}\|$$
$$= \sqrt{(x_1-y_1)^2 + (x_2-y_2)^2 + (x_3-y_3)^2}$$

Definition: An isometry of $\mathbb{R}^3$ is a function $T: \mathbb{R}^3 \to \mathbb{R}^3$ that preserves distances between all pairs of points:

$$\forall \vec{x}, \vec{y} \in \mathbb{R}^3, \quad d(T(\vec{x}), T(\vec{y})) = d(\vec{x}, \vec{y}).$$

Definition: let $R \subset \mathbb{R}^3$ be a subset.
A symmetry of R is an isometry $T: \mathbb{R}^3 \to \mathbb{R}^3$ that maps points in R to points in R:
$$T(R) \subset R.$$

If T_1 and T_2 are isometries then $T_1 \circ T_2$ is also an isometry.

Proof: $d(T_1 \circ T_2(\vec{x}), T_1 \circ T_2(\vec{y}))$

$= d(T_1(T_2(\vec{x})), T_1(T_2(\vec{y})))$ Def. of $\circ$

$= d(T_2(\vec{x}), T_2(\vec{y}))$ T_1 is isometry

$= d(\vec{x}, \vec{y})$ T_2 is isometry.

Also, if $T_1(R) \subset R$ and $T_2(R) \subset R$ then $T_1 \circ T_2(R) = T_1(T_2(R)) \subset T_1(R) \subset R$.

Conclusion: if T_1 and T_2 are symmetries of R, then $T_1 \circ T_2$ is also a symmetry of R.

Or, the set of symmetries of R is "closed under composition."

We can describe all possible isometries of $\mathbb{R}^3$

Write points as column vectors $\vec{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$

Theorem: A function $T: \mathbb{R}^3 \to \mathbb{R}^3$ is an isometry if and only if it is an affine transformation

$$T(\vec{x}) = A\vec{x} + \vec{b}$$

where A is a 3×3 orthogonal matrix and $\vec{b}$ is a vector.

Recall the definition of an orthogonal matrix:

$A^T A = I = A A^T$, or $A^T = A^{-1}$, or columns of A form an orthonormal basis.

We will not present the proof of the preceding theorem here.

Consequence: If $T: \mathbb{R}^3 \to \mathbb{R}^3$ is an isometry, then $T(\vec{x}) = A\vec{x} + \vec{b}$, and T has an inverse given by $T^{-1}(\vec{x}) = A^T\vec{x} - A^T\vec{b}$.

Check:
$$\begin{aligned} T^{-1}(T(\vec{x})) &= A^T(A\vec{x} + \vec{b}) - A^T\vec{b} \\ &= A^TA\vec{x} + A^T\vec{b} - A^T\vec{b} \\ &= A^TA\vec{x} = I\vec{x} = \vec{x} \end{aligned}$$

Define $\mathrm{Sym}(R) = \{T : \mathbb{R}^3 \to \mathbb{R}^3 \mid T \text{ is an isometry and } T(R) < R\}$
the set of symmetries of R.

This set has some key properties that we wish to abstract/pull away from this situation.

$\mathrm{Sym}(R)$ has a binary operation, composition, under which it is closed:

$$T_1, T_2 \in \mathrm{Sym}(R) \implies T_1 \circ T_2 \in \mathrm{Sym}(R).$$

This operation is

(1) Associative: $T_1 \circ (T_2 \circ T_3) = (T_1 \circ T_2) \circ T_3$

(2) has identity: $T \circ I = I \circ T = T$

(3) has inverses: $T \in \mathrm{Sym}(R) \implies \exists\, T^{-1} \in \mathrm{Sym}(R)$
$T^{-1} \circ T = I = T \circ T^{-1}$.

<u>Remark</u> The precise definition of a <u>rotation</u> of $\mathbb{R}^3$ is an isometry of the form

$$T(\vec{x}) = A\vec{x}$$

where A is orthogonal <u>and</u> $\det(A) = 1$.