Math 451: Abstract Algebra I

Wolmer V. Vasconcelos

Set 2

Fall 2009

Outline

1 Symmetry
2 Rigid Motions
3 Rigid Motions in the Plane
4 Homework #4
5 Finite Groups of Motions
6 Discrete Groups of Motions
7 Abstract Symmetry
8 The Operation on Cosets
9 Homework #5
10 The Counting Formula
11 Finite Subgroups of the Rotation Group
12 Permutation Representation
13 Symmetric groups

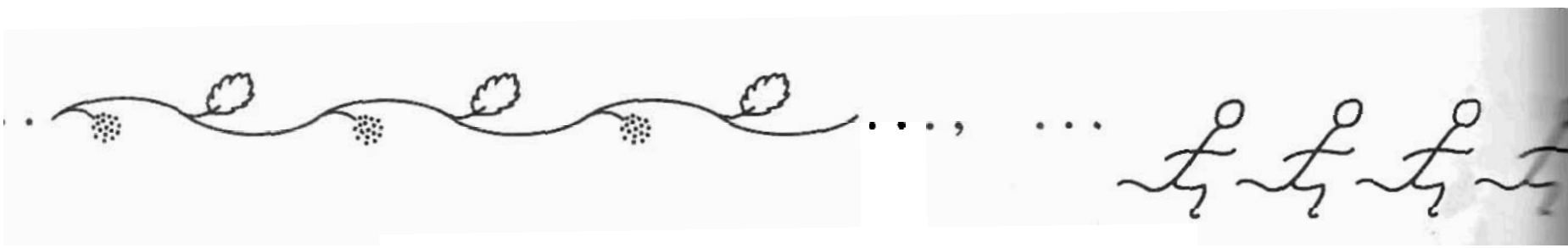
What is Symmetry?

Discuss

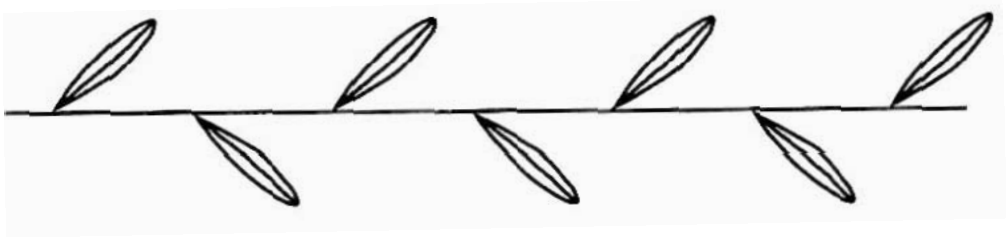
Example

Example

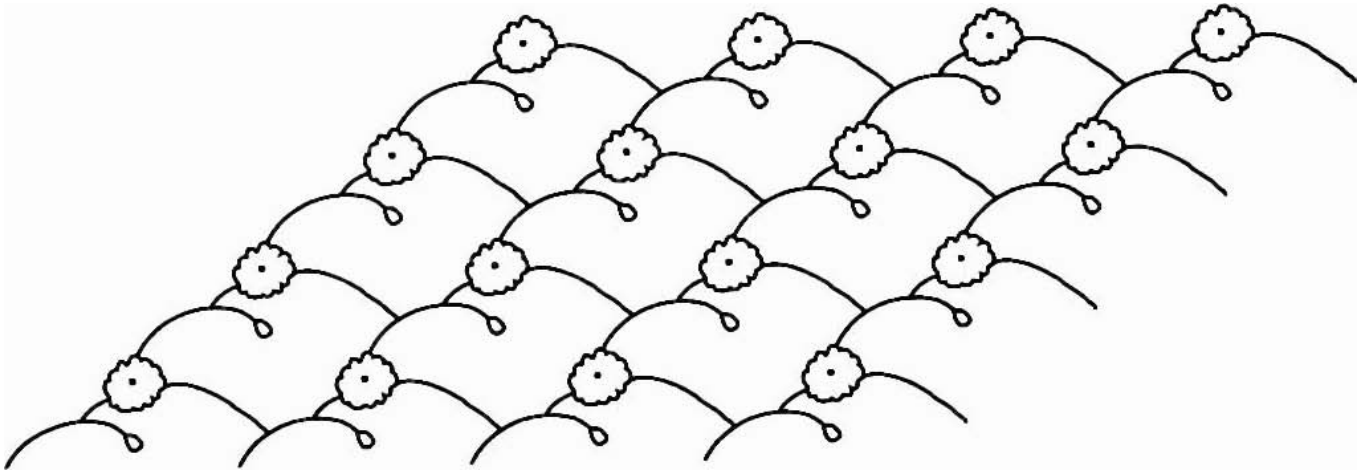
Example



Example

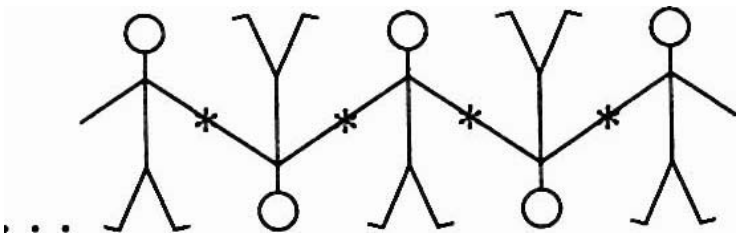


Example



Example

Example



Outline

1. Symmetry
2. Rigid Motions
3. Rigid Motions in the Plane
4. Homework #4
5. Finite Groups of Motions
6. Discrete Groups of Motions
7. Abstract Symmetry
8. The Operation on Cosets
9. Homework #5
10. The Counting Formula
11. Finite Subgroups of the Rotation Group
12. Permutation Representation
13. Symmetric groups

Rigid Motions

A **rigid motion** on the inner product space **V** is a mapping

$$\mathbf{T} : \mathbf{V} \to \mathbf{V}$$

with the property

$$||\mathbf{T}(u) - \mathbf{T}(v)|| = ||u - v||, \quad \forall u, v\mathbf{V}.$$

That is, **T** preserves distance of the images. A simple example is a translation: If **a** is a fixed vector, the function

$$\mathbf{T}(v) := \mathbf{a} + v$$

is obviously a rigid motion:

$$\mathbf{T}(v) - \mathbf{T}(u) = (\mathbf{a} + v) - (\mathbf{a} + u) = v - u$$

What else?

Orthogonal Transformations

Recall what this means:

$$\mathbf{T} \cdot \mathbf{T}^t = \mathbf{I}$$

Therefore for any vector $v \in \mathbb{R}^n$,

$$\langle \mathbf{T}(v), \mathbf{T}(v) \rangle = v^t \cdot \mathbf{T}^t \cdot \mathbf{T} \cdot v = v^t \cdot v = \langle v, v \rangle$$

Thus orthogonal transformations $\mathbf{T}$, $\mathbf{T}\mathbf{T}^t = \mathbf{I}$, preserve distances. Another such motion is obtained by composition: following a translation with an orthogonal mapping. What else? That is it!

Inner product space

An **inner product vector space V** is a V.S. over $\mathbb{R}$ or $\mathbb{C}$ with a mapping

$$\mathbf{V} \times \mathbf{V} \to \mathbf{F}, \quad (u, v) \to \langle u, v \rangle = u \cdot v \in \mathbf{F}$$

satisfying certain conditions. Let us give an example to guide us in what is needed. Let $\mathbf{V} = \mathbb{R}^n$ and define

$$\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \cdot \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = a_1 b_1 + \cdots + a_n b_n = \sum_{i=1}^{n} a_i b_i$$

Note the properties: **bi-additive** ; $v \cdot v$ is a non-negative real number, so we can use $\sqrt{v \cdot v}$ to define the **magnitude** of v.
Question: Could we use the same formula to define an inner product for $\mathbb{C}^n$? Well... $(i) \cdot (i)$ would be -1. Of course the formula still defines a nice bilinear mapping but would not meet our need.

Matrix product and dot product

Let u and v be two vectors of $\mathbb{R}^n$. Their **dot product**

$$u \cdot v = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \cdot \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$$

can be expressed as a **matrix product**

$$u^t v = \begin{bmatrix} a_1 & \cdots & a_n \end{bmatrix} \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$$

Keep in mind

$$u^t v = u \cdot v$$

Dot product

Definition

An inner product vector space is a vector space with a mapping

$$\mathbf{V} \times \mathbf{V} \to \mathbf{F}, \quad (u, v) \to u \cdot v \in \mathbf{F}$$

satisfying:

1. $(u_1 + u_2) \cdot v = u_1 \cdot v + u_2 \cdot v$
2. $(cu) \cdot v = c(u \cdot v)$
3. $\overline{u \cdot v} = v \cdot u$
4. $u \cdot u > 0$ if $u \neq O$

The better notation for this product is

$$u \cdot v = \langle u, v \rangle$$

Examples

Of course, the example above of $\mathbb{R}^n$ is the grandmother of all examples. Let us modify it a bit to get an example for $\mathbb{C}^n$:

$$\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \cdot \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = a_1\overline{b_1} + \cdots + a_n\overline{b_n} = \sum_{i=1}^{n} a_i\overline{b_i}.$$

Note the properties: **additive** ; $v \cdot v$ is a non-negative real number

$$v \cdot v = \sum_{i=1}^{n} a_i\overline{a_i}$$

so we can use $\sqrt{v \cdot v}$ to define the **magnitude** of v. Note the lack of full symmetry.

Example of Function Space

Let us give an example from left field: Let **V** be the vector space of all real continuous functions on the interval $[a, b]$, and define for $f(t), g(t) \in \mathbf{V}$,

$$\langle f(t), g(t) \rangle = f(t) \cdot g(t) = \int_a^b f(t)g(t)dt.$$

An important case: If m, n are integers,

$$\begin{aligned}
\langle \sin nt, \cos mt \rangle &= \int_0^{2\pi} \sin nt \cos mt \; dt = 0 \\
\langle \sin nt, \sin mt \rangle &= \int_0^{2\pi} \sin nt \sin mt \; dt = 0, \; m \neq n \\
\langle \cos nt, \cos mt \rangle &= \int_0^{2\pi} \cos nt \cos mt \; dt = 0, \; m \neq n \\
\langle \sin nt, \sin nt \rangle &= \int_0^{2\pi} \sin^2 nt \; dt = \pi, \; n \neq 0
\end{aligned}$$

Length of a vector

Definition

Let $\mathbf{V}, \langle \cdot, \cdot \rangle$ be an inner product space. If $v \in \mathbf{V}$, the **length** or **norm** of v is the real number $||v|| = \sqrt{\langle v, v \rangle}$.

If $\mathbf{V} = \mathbb{C}^n$, $v = (a, \ldots, a_n)$,

$$||v|| = \left[\sum_{i=1}^{n} |a_i|^2 \right]^{1/2}$$

If $\mathbf{V}$ is the space of real continuous functions on $[0, 1]$ and inner product is that we defined previously,

$$||f(t)||^2 = \int_0^1 f(t)^2 dt.$$

Framework for Geometry

The following assertions permits the construction of 'recognizable' objects in any inner product space:

Theorem

If $\mathbf{V}$ *is an inner product space, then for all* $u, v \in \mathbf{V}$

1. *[Cauchy-Schwarz Inequality]*

$$|\langle u, v \rangle| \leq ||u|| \cdot ||v||$$

2. *[Triangle Inequality]*

$$||u + v|| \leq ||u|| + ||v||.$$

Unitary Operators

Notation: $\mathbf{T}^* = \overline{\mathbf{T}^t}$ conjugate transpose of $\mathbf{T}$

Definition

A linear operator $\mathbf{T}$ of the inner product space $\mathbf{V}$ is called **unitary** if $\mathbf{T}\mathbf{T}^* = \mathbf{T}^*\mathbf{T} = \mathbf{I}$. If $\mathbf{V}$ is a real inner product space, $\mathbf{T}$ is called **orthogonal**.

The rotation operator

$$\mathbf{T}(x, y) = (x \cos\alpha + y \sin\alpha, -x \sin\alpha + y \cos\alpha)$$

is a major example.

If $\mathbf{A}$ is a complex n-by-n matrix and $\mathbf{A}\mathbf{A}^* = \mathbf{A}^*\mathbf{A} = \mathbf{I}$, the column vectors of $\mathbf{A}$ form an orthonormal basis of $\mathbb{C}^n$.
We now develop quickly some basic properties of these operators.

Theorem

Let $\mathbf{T}$ *be a linear operator of the finite-dimensional inner product space* $\mathbf{V}$*. TFAE:*

1. $\mathbf{T}$ *is an unitary operator:* $\mathbf{T}\mathbf{T}^* = \mathbf{T}^*\mathbf{T} = \mathbf{I}$.
2. $\langle \mathbf{T}(u), \mathbf{T}(v) \rangle = \langle u, v \rangle$ *for all* $u, v \in \mathbf{V}$.
3. *For every orthonormal basis* $\mathcal{B} = v_1, \ldots, v_n$ *of* $\mathbf{V}$, $\mathbf{T}(v_1), \ldots, \mathbf{T}(v_n)$ *is also an orthonormal basis of* $\mathbf{V}$.
4. *For some orthonormal basis* $\mathcal{B} = v_1, \ldots, v_n$ *of* $\mathbf{V}$, $\mathbf{T}(v_1), \ldots, \mathbf{T}(v_n)$ *is also an orthonormal basis of* $\mathbf{V}$.
5. $||\mathbf{T}(u)|| = ||u||$ *for every* $u \in \mathbf{V}$.

Proof. $1 \Rightarrow 2, 3, 4, 5$: (Other $\Rightarrow$ LTR)

$$\langle u, v \rangle = \langle \mathbf{T}^*\mathbf{T}(u), v \rangle = \langle \mathbf{T}(u), (\mathbf{T}^*)^*(v) \rangle = \langle \mathbf{T}(u), \mathbf{T}(v) \rangle.$$

$$\delta_{ij} = \langle v_i, v_j \rangle = \langle \mathbf{T}(v_i), \mathbf{T}(v_j) \rangle.$$

Orthogonal Group

- $\mathbf{T}$ is orthogonal operator of $\mathbb{R}^n$ if $\mathbf{T}\mathbf{T}^t = \mathbf{T}^t\mathbf{T} = \mathbf{I}$.
- If $\mathbf{T}_1$ and $\mathbf{T}_2$, then $\mathbf{T}_1\mathbf{T}_2$ is orthogonal: check.

- This shows that the set of orthogonal operators form a subgroup of $GL_n(\mathbb{R})$: the orthgonal group $\mathbf{O}$, or $\mathbf{O}_n$.
- $\det \mathbf{T} \det \mathbf{T}^t = (\det \mathbf{T})^2 = 1$: $\det \mathbf{T} = \pm 1$. The operators with $\det \mathbf{T} = 1$ form a subgroup: orientation preserving.
- The operators $\mathbf{T}$ with $\det \mathbf{T} = 1$ form the subgroup SO_n, called the special orthogonal group

Orthogonal operators of $\mathbb{R}^2$

We have already mentioned rotations, R_α. Let us analyze the possibilities. Let

$$\mathbf{A} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = [v_1|v_2] \quad ||v_1|| = ||v_2|| = 1, \quad v_1 \perp v_2$$

be an orthogonal matrix. This means

$$a^2 + c^2 = 1, \quad b^2 + d^2 = 1, \quad ab + cd = 0$$

We can set $a = \cos\alpha, c = \sin\alpha$ and $b = \cos\beta, d = \sin\beta$ so that

$$ab + cd = \cos\alpha\cos\beta + \sin\alpha\sin\beta = \cos(\alpha - \beta) = 0.$$

This means that $\alpha - \beta = \pm\pi/2$. The two possibilities lead to

$$R_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}, \quad \mathbf{T} = \begin{bmatrix} \cos\beta & \sin\beta \\ \sin\beta & -\cos\beta \end{bmatrix}$$

To analyze

$$\mathbf{T} = \begin{bmatrix} \cos\beta & \sin\beta \\ \sin\beta & -\cos\beta \end{bmatrix}$$

we look at its eigenvalues:

$$\det(\mathbf{T} - x\mathbf{I}) = \begin{bmatrix} \cos\beta - x & \sin\beta \\ \sin\beta & -\cos\beta - x \end{bmatrix} = x^2 - 1$$

So $\lambda = \pm 1$. This means we have an orthonormal basis v_1, v_2, and $\mathbf{T}(v_1) = v_1$, $\mathbf{T}(v_2) = -v_2$.
Thus the line $\mathbb{R}v_1$ is fixed under $\mathbf{T}$, and the perpendicular line $\mathbb{R}v_2$ is flipped about $\mathbb{R}v_1$. These transformations are called **reflections**.

Summary: If $\mathbf{A}$ is an orthogonal 2-by-2 matrix, then if $\det \mathbf{A} = 1$, it is a rotation, and if $\det \mathbf{A} = -1$, it is a reflection.

The group SO_3

Theorem

Let $\mathbf{A} \in SO_3$. *Then there is a basis change so that*

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{bmatrix}.$$

Review te relevant linear algebra

Exercise

Exercise: Prove that the set **M** of rigid motions of $\mathbb{R}^n$ is a group.

The only technical point needed is:

Lemma

If $\mathbf{F} : \mathbb{R}^n \to \mathbb{R}^n$ *is a rigid motion, then* $\mathbf{F}$ *is invertible and* $\mathbf{F}^{-1}$ *is a rigid motion.*

Rigid motion: Main Theorem

Theorem

Any rigid motion $\mathbf{T}$ *of* $\mathbf{V}$ *decomposes into* $\mathbf{T} = \mathbf{S} \circ \mathbf{U}$, *where* $\mathbf{S}$ *is an orthogonal transformation and* $\mathbf{U}$ *is a translation.*

Proof: Set $\mathbf{a} = \mathbf{T}(O)$. Then the function $\mathbf{F}(u) = \mathbf{T}(u) - \mathbf{a}$ is a rigid motion and $\mathbf{F}(O) = O$. It is enough to prove that $\mathbf{F}$ is orthogonal. Note that

$$||\mathbf{F}(u) - \mathbf{F}(O)|| = ||u - O||,$$

so $\mathbf{F}$ preserves lengths, which is the key property of orthogonal transformations. BUT we are NOT assuming that $\mathbf{F}$ is linear, we must prove it.
We first prove that $\mathbf{F}$ preserves dot products:
$\langle \mathbf{F}(u), \mathbf{F}(v) \rangle = \langle u, v \rangle$: We start from the equality and expand both sides

$$
\begin{aligned}
||\mathbf{F}(u) - \mathbf{F}(v)||^2 &= ||u - v||^2 \\
(\mathbf{F}(u) - \mathbf{F}(v)) \cdot (\mathbf{F}(u) - \mathbf{F}(v)) &= (u - v) \cdot (u - v) \\
\underbrace{||\mathbf{F}(u)||^2}_{*} - 2\langle \mathbf{F}(u), \mathbf{F}(v) \rangle + \underbrace{||\mathbf{F}(v)||^2}_{**} &= \underbrace{||u||^2}_{*} - 2\langle u, v \rangle + \underbrace{||v||^2}_{**}
\end{aligned}
$$

Thus proving

$$\langle \mathbf{F}(u), \mathbf{F}(v) \rangle = \langle u, v \rangle.$$

Now we are going to prove that $\mathbf{F}$ is a linear function by first showing that it is additive:

$$
\begin{aligned}
||\mathbf{F}(u+v)-\mathbf{F}(u)-\mathbf{F}(v)||^2 &\stackrel{?}{=} 0 \\
||\mathbf{F}(u+v)||^2+||\mathbf{F}(u)||^2+||\mathbf{F}(v)||^2- &= ||u+v||^2+||u||^2+||v||^2- \\
2\langle \mathbf{F}(u+v),\mathbf{F}(u)\rangle - 2\langle \mathbf{F}(u+v),\mathbf{F}(v)\rangle &= 2\langle (u+v),u\rangle - 2\langle (u+v),v\rangle \\
+2\langle \mathbf{F}(u),\mathbf{F}(v)\rangle &= +2\langle u,v\rangle \\
&= ||(u+v)-u-v||^2 = 0.
\end{aligned}
$$

Scaling, that $\mathbf{F}(cu) = c\mathbf{F}(u)$ for any $c \in \mathbb{R}$, has a similar proof: Expand

$$||\mathbf{F}(cu) - c\mathbf{F}(u)||^2$$

Outline

1. Symmetry
2. Rigid Motions
3. **Rigid Motions in the Plane**
4. Homework #4
5. Finite Groups of Motions
6. Discrete Groups of Motions
7. Abstract Symmetry
8. The Operation on Cosets
9. Homework #5
10. The Counting Formula
11. Finite Subgroups of the Rotation Group
12. Permutation Representation
13. Symmetric groups

Rigid Motions in the Plane

Theorem

Any rigid motion $\mathbf{T}$ *of* $\mathbf{V}$ *decomposes into* $\mathbf{T} = \mathbf{S} \circ \mathbf{U}$*, where* $\mathbf{S}$ *is an orthogonal transformation and* $\mathbf{U}$ *is a translation.*

When $\mathbf{V} = \mathbb{R}^2$:

- Translation by a vector: $t_a(x) = x + a = \begin{bmatrix} x_1 + a_1 \\ x_2 + a_2 \end{bmatrix}$
- Rotation by an angle about the origin:
  $\rho_\theta(x) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$
- Reflection about the x_1-axis:
  $r(x) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_1 \\ -x_2 \end{bmatrix}$
- Compositions: $\rho \circ r$, $\rho \circ r$ $\rho \circ t_a$ etc.

Decomposition of rigid motions

We have shown that every rigid motion $\mathbf{F} : \mathbb{R}^n \to \mathbb{R}^n$ decomposes as

$$\mathbf{F} = \rho \circ t_a,$$

where $\rho \in \mathbf{O}$, the group of orthogonal operators, and t_a is the translation by the vector $\mathbf{a}$.
This decomposition has several properties. Let us highlight some:

- The identity $\rho \circ t_a = t_{\rho(a)} \circ \rho$:

$$\rho(t_a(\mathbf{v})) = \rho(\mathbf{v} + a) = \rho(\mathbf{v}) + \rho(a) = (t_{\rho(a)} \circ \rho)(\mathbf{v})$$

  In particular, the subgroup of translations is normal.

- If $\rho \circ t_a = \rho' \circ t_b$ then $\rho = \rho'$ and $a = b$:

$$\begin{aligned} \rho \circ t_a(\mathbf{v}) &= \rho(\mathbf{v} + a) = \rho(\mathbf{v}) + \rho(a) = \\ \rho' \circ t_b(\mathbf{v}) &= \rho'(\mathbf{v} + b) = \rho'(\mathbf{v}) + \rho'(b) \end{aligned}$$

Thus

$$(\rho - \rho')(\mathbf{v}) = \rho'(b) - \rho(a),$$

an equality that says that the linear transformation $\rho - \rho'$ is constant. But O is the only constant linear transformation, so $\rho = \rho'$ and $\rho(b) = \rho(a)$ and therefore $a = b$ since ρ is invertible.

- $(\rho \circ t_a) \circ (\rho' \circ t_b) = (\rho \circ \rho') \circ t_c, \quad c = \rho'(b) + a.$

$$\begin{aligned}(\rho \circ t_a) \circ (\rho' \circ t_b)(\mathbf{v}) &= \rho(t_a(\rho'(t_b)))(\mathbf{v}) \\ &= \rho(t_a(\rho'(\mathbf{v}) + \rho'(b))) \\ &= \rho \circ \rho'(\mathbf{v}) + \rho(a) + \rho(\rho'(b))\end{aligned}$$

The fact that every rigid motion is written uniquely as $\rho \circ t_a$ and

$$(\rho \circ t_a) \circ (\rho' \circ t_b) = (\rho \circ \rho') \circ t_c, \quad c = \rho'(b) + a,$$

gives rise to a mapping:

Theorem

The mapping φ from the group **M** *of rigid motions to the orthogonal group* **O** *given by*

$$\varphi(\rho \circ t_a) = \rho$$

is a group homomorphism.

The kernel is the subgroup of translations.

Definition

If **G** is a subgroup of **M**, the image $\overline{\mathbf{G}} \subset \mathbf{O}$ of **G** under φ is called the point group of **G**.

This is the group of all $\rho \in \mathbf{O}$ such that there is t_a such that $\rho \circ t_a \in \mathbf{G}$.

Outline

1. Symmetry
2. Rigid Motions
3. Rigid Motions in the Plane
4. **Homework #4**
5. Finite Groups of Motions
6. Discrete Groups of Motions
7. Abstract Symmetry
8. The Operation on Cosets
9. Homework #5
10. The Counting Formula
11. Finite Subgroups of the Rotation Group
12. Permutation Representation
13. Symmetric groups

Homework #4

1. Prove that a linear operator of $\mathbb{R}^2$ is a reflection iff its eigenvalues are 1 and -1, and its eigenvectors are orthogonal.
2. Let D_n denote the dihedral group. Express (see 3.6)

$$x^2yx^{-1}y^{-1}x^3y^3$$

   in the form x^iy^j.
3. List all subgroups of D_4, and determine which are normal.
4. Find all normal subgroups of D_{13}, and determine the quotient groups of D_{13}.

Outline

1. Symmetry
2. Rigid Motions
3. Rigid Motions in the Plane
4. Homework #4
5. **Finite Groups of Motions**
6. Discrete Groups of Motions
7. Abstract Symmetry
8. The Operation on Cosets
9. Homework #5
10. The Counting Formula
11. Finite Subgroups of the Rotation Group
12. Permutation Representation
13. Symmetric groups

Finite Groups of Motions

Theorem (Fixed Point Theorem)

Let $\mathbf{G}$ *be a finite subgroup of the group of rigid motions* $\mathbf{M}$*. Then there is a point* p *which is left fixed by every element of* $\mathbf{G}$*, that is there is a point* p *such that* $\mathbf{g}(p) = p$ *for all* $\mathbf{g} \in \mathbf{G}$*.*

This gives us an opportunity to introduce an important notion in group theory: orbits.
For simplicity suppose that $\mathbf{G}$ are linear transformations of $\mathbb{R}^2$.
For each $x \in \mathbb{R}^2$, the set

$$\mathbf{G}x = \{\mathbf{g}(x) : \mathbf{g} \in \mathbf{G}\}$$

is the orbit of x. Since $\mathbf{G}$ is finite, $\mathbf{G}x$ is a finite set:

$$\mathbf{G}x = \{x_1, \ldots, x_n\}$$

Proof

Note that for any $\mathbf{g} \in \mathbf{G}$

$$\{x_1, \ldots, x_n\} = \{\mathbf{g}(x_1), \ldots, \mathbf{g}(x_n)\}$$

Proof.

Let x be any vector of $\mathbb{R}^2$ and set

$$p = x_1 + \cdots + x_n$$

Then for any $\mathbf{g} \in \mathbf{G}$,

$$\begin{aligned} \mathbf{g}(p) &= \mathbf{g}(x_1) + \cdots + \mathbf{g}(x_n) \\ &= x_1 + \cdots + x_n \\ &= p \end{aligned}$$

□

Center of Gravity and Rigid Motions

Definition

Let $\{x_1, \ldots, x_n\}$ be a set of points of $\mathbb{R}^2$. Their center of gravity is the point

$$p = \frac{1}{n}(x_1 + \cdots + x_n).$$

Proposition

If $\mathbf{F}$ *is a rigid motion then* $\mathbf{F}(p)$ *is the center of gravity* $\{\mathbf{F}(x_1), \ldots, \mathbf{F}(x_n)\}$.

Proof. Volunteer please!

Dihedral group

Volunteer please!

- D_n group of symmetries of the regular n-gon

Finite subgroups

Theorem

Let **G** *be a finite subgroup of the group of rigid motions* **O** *which fix the origin. Then* **G** *is one of the following groups:*

1. $\mathbf{G} = C_n$*: the cyclic group of order n, generated by the rotation* ρ_θ*, where* $\theta = 2\pi/n$.
2. $\mathbf{G} = D_n$*: the dihedral group of order* $2n$*, generated by two elements–the rotation* ρ_θ*, where* $\theta = 2\pi/n$*, and a reflection* r' *about a line through the origin.*

Proof

- If **G** consists of rotations: May assume $\mathbf{G} \neq \{1\}$. Among the rotations in **G**, let $\rho_{\theta_0} \neq 1$ with θ_0 smallest. For any other rotation $\rho_\theta \in \mathbf{G}$, write

$$\theta = m\theta_0 + \alpha, \quad 0 \leq \alpha < \theta_0, m \in \mathbb{Z}.$$

If $\alpha \neq 0$, we would have

$$\rho_\alpha = (\rho_{\theta_0})^{-m}\rho_\theta \in \mathbf{G},$$

which is a contradiction.

This shows **G** is generated by ρ_{θ_0}.

- If **G** contains refections: Change coordinates and assume the standard reflection $r \in \mathbf{G}$.
  Let **H** be the subgroup of rotations in **G**. By the argument above, **H** is a cyclic group C_n generated by the rotation ρ.
  This shows that **G** contains D_n.
  We claim that $\mathbf{G} = D_n$. Let s be any reflection in **G**. Then we know that $s = r\rho'$ for some rotation ρ', which would be an element of **G**.

D_n abstractly

Proposition

The dihedral group D_n is generated by two elements x, y which satisfy the relations

$$x^n = 1, \quad y^2 = 1, \quad yx = x^{-1}y.$$

Proof. The elements $x = \rho_\theta$ and $y = r$ generate D_n by definition of the group. The relations $y^2 = 1$ and $yx = x^{-1}y$ are included in the list of relations for M: They are $rr = 1$ and $r\rho_\theta = \rho_{-\theta}r$. The relation $x^n = 1$ follows from the fact that $\theta = 2\pi/n$, which also shows that the elements $1, x, \ldots, x^{n-1}$ are distinct.

It follows that the elements $y, xy, x^2y, \ldots, x^{n-1}y$ are also distinct and, since they are reflections while the powers of x are rotations, that there is no repetition in the list of elements.

Finally, the relations can be used to reduce any product of x, y, x^{-1}, y^{-1} to the form $x^i y^j$, with $0 \leq i < n$, $0 \leq j < 2$. Therefore the list contains all elements of the group generated by x, y, and since these elements generate D_n the list is complete $\square$

Corollary

The dihedral group D_3 and the symmetric group S_3 are isomorphic.

For $n > 3$, the dihedral and symmetric groups are certainly not isomorphic, because D_n has order $2n$, while S_n has order $n!$.

Outline

1. Symmetry
2. Rigid Motions
3. Rigid Motions in the Plane
4. Homework #4
5. Finite Groups of Motions
6. **Discrete Groups of Motions**
7. Abstract Symmetry
8. The Operation on Cosets
9. Homework #5
10. The Counting Formula
11. Finite Subgroups of the Rotation Group
12. Permutation Representation
13. Symmetric groups

Discrete Groups of Motions of the Plane

The group **M** of motions of the plane is put together from the orthogonal group O and the group of translations.

Definition

A subgroup **G** of the group of motions **M** is called discrete if it does not contains arbitrarily small translations or rotations. More precisely, **G** is discrete if there is some real number $\epsilon > 0$ such that

1. if t_a is a translation in **G**, then $|a| \geq \epsilon$;
2. if ρ_θ is a non trivial rotation in **G**, then $|\theta| \geq \epsilon$.

Plane Lattices

The subgroup of translations is isomorphic to $\mathbb{R}^2$:

$$\mathbf{a}, \mathbf{b} \in \mathbb{R}^2 : t_{\mathbf{a}+\mathbf{b}} = t_{\mathbf{a}} + t_{\mathbf{b}}$$

We are going to study some subgroups of $\mathbb{R}^2$, among them are the subspaces, but these are easy.

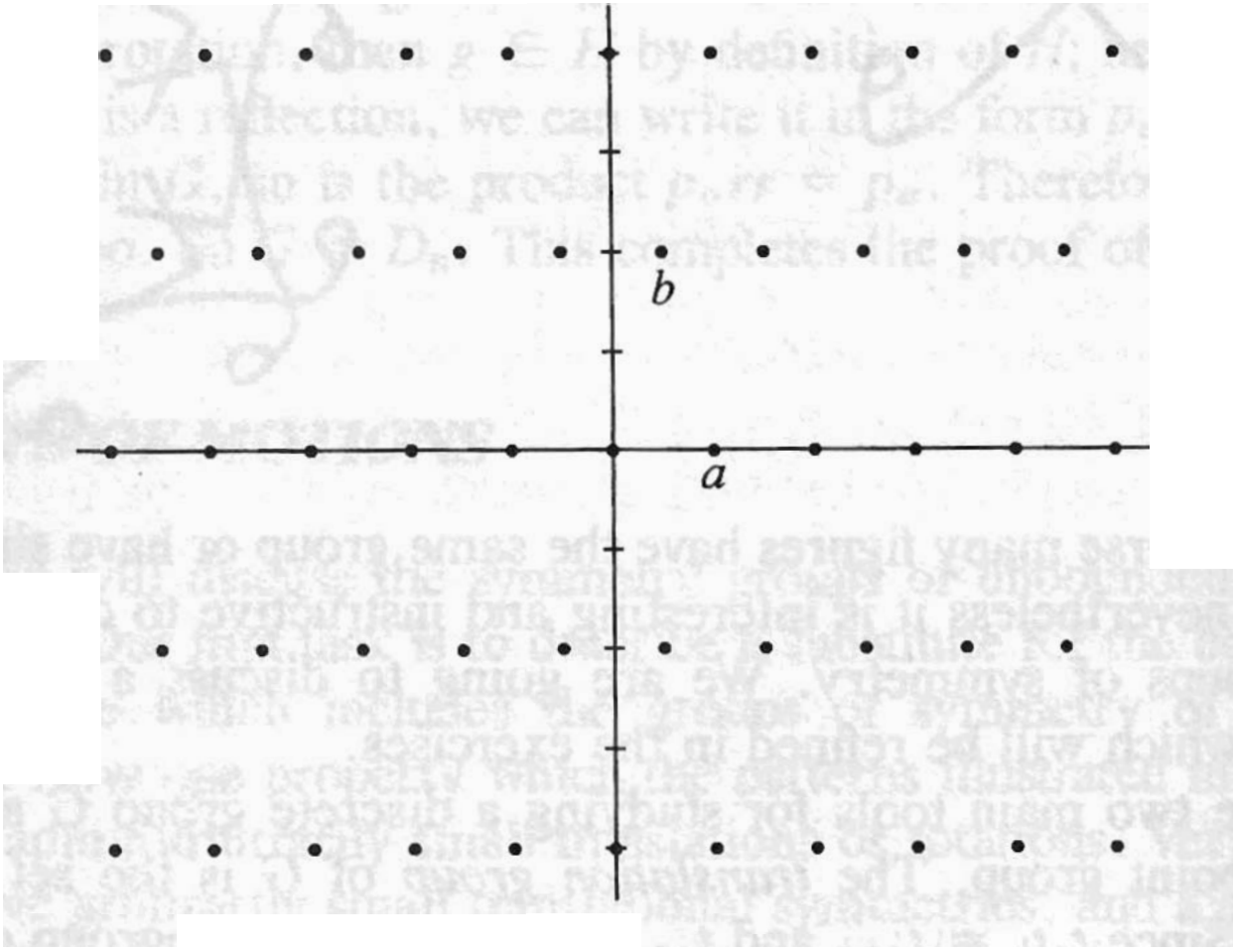
Proposition

Every discrete group L of $\mathbb{R}^2$ has one of these forms :

1. $L = \{0\}$.
2. *L is generated as an additive group by one nonzero vector a :*
$$L = \{ma \mid m \in \mathbb{Z}\}.$$
3. *L is generated by two linearly independent vectors a, b :*
$$L = \{ma + nb \mid m, n \in \mathbb{Z}\}.$$

Groups of the third type are called *plane lattices*,and the generating set (a, b) is called a *lattice basis*.

Example



Proof

We may assume $L \neq (0)$. There are two cases: L contains maximal sets of either 1 or 2 linearly independent sets of vectors.
L is contained in a one-dimensional subspace, $L \subset \mathbb{R}v$. We are going to pick a nonzero element of L of minimal length. For that we need a Lemma.

Lemma

Let L be a discrete subgroup of $\mathbb{R}^2$.

1. *A bounded subset S of $\mathbb{R}^2$ contains only finitely many elements of L.*
2. *If $L \neq (0)$, then L contains a nonzero vector of minimal length.*

Proof

Proof. Volunteer!

Proof of Proposition

- Let $\mathbf{a} \in L$ be nonzero, of minimum length. Then $L \subset \mathbb{R}\mathbf{a}$.
- For $v \in L$, $v = r\mathbf{a}$, for some real number r which we write as

$$r = n + r_0$$

  where n is an integer and $0 \leq r_0 < 1$.
- If $r_0 \neq 0$, $v - n\mathbf{a} = r_0\mathbf{a}$ is an element of L of length less than the length of $\mathbf{a}$.
  The contradiction shows that $L = \mathbb{Z}\mathbf{a}$.

- Consider the other case, that L contains a set of two linearly independent vectors $\mathbf{a}'$ and $\mathbf{b}'$.
- We are going to replace these by better vectors that generate L. First, in the line $\mathbb{R}\mathbf{a}'$ pick the nonzero element of L of least length. By the argument above, $L \cap \mathbb{R}\mathbf{a} = \mathbb{Z}\mathbf{a}$.
- Consider the parallelogram P' of vertices $\{0, \mathbf{a}, \mathbf{b}', \mathbf{a} + \mathbf{b}'\}$. P' is a bounded set so $P' \cap L$ is a finite set. Choose a point $\mathbf{b}$ in this set whose distance to the line $\mathbb{R}\mathbf{a}$ is as small as possible.
- Replace $\mathbf{b}'$ by $\mathbf{b}$ and consider the parallelogram P of vertices $\{0, \mathbf{a}, \mathbf{b}, \mathbf{a} + \mathbf{b}\}$.
- We claim that the only points of L in P are the vertices. Draw a good picture.

Lemma

Let a, b be linearly independent vectors which are elements of a subgroup L of $\mathbb{R}^2$. Suppose that the parallelogram P which they span contains no element of L other than the vertices $0, a, b, a+b$. Then L is generated by a and b, that is,

$$L = \{ma + nb \mid m, n \in \mathbb{Z}\}.$$

Proof. Let v be an arbitrary element of L. Then since (a, b) is a basis of $\mathbb{R}^2$, v is a linear combination, say $v = ra + sb$, where r, s are real numbers. We take out the integer parts of r, s, writing $r = m + r_0$, $s = n + s_0$, where m, n are integers and $0 \leq r_0, s_0 < 1$. Let $v_0 = r_0 a + s_0 b = v - ma - nb$. Then v_0 lies in the parallelogram P, and $v_0 \in L$. Hence v_0 is one of the vertices, and since $r_0, s_0 < 1$, it must be the origin. Thus $v = ma + nb$. This completes the proof of the lemma and the Proposition characterizing plane lattices. □

Proposition

A discrete subgroup of $\mathbf{O}$ *is a finite group.*

This will be a Hourly #1 Question.

Corollary

The point group $\overline{G}$ of a discrete group G is cyclic or dihedral.

Recall how the point group $\overline{G}$ of a group G arises: Every element of **G** can be written as a product $\rho \circ t_a$. The point group of G is the group formed by these ρ.
In other words, $\overline{G}$ is the image of the morphism $G \to \mathbf{O}$ given by $\rho \circ t_a \to \rho$.

Proposition

Let G be a discrete subgroup of **M**, *with translation group $L = L_G$ and point group $\overline{G}$. The elements of $\overline{G}$ carry the group L to itself. In other words, if $\overline{g} \in \overline{G}$ and $a \in L$, then $\overline{g}(a) \in L$.*

Proof. To say that $a \in L$ means that $t_a \in G$. So we have to show that if $t_a \in G$ and $\overline{g} \in \overline{G}$, then $t_{\overline{g}(a)} \in G$.
Now by definition of the point group, $\overline{g}$ is the image of some element g of the group G: $\varphi(g) = \overline{g}$. We will prove the proposition by showing that $t_{\overline{g}(a)}$ is the conjugate of t_a by g.
We write $g = t_b\rho$ or $t_b\rho r$, where $\rho = \rho_\theta$. Then $\overline{g} = \rho$ or ρr, according to the case. In the first case,

$$gt_ag^{-1} = t_b\rho t_a\rho^{-1}t_{-b} = t_bt_{\rho(a)}\rho\rho^{-1}t_{-b} = t_{\rho(a)},$$

as required. The computation is similar in the other case. □

Proposition

Let $H \subset \mathbf{O}$ be a finite subgroup of the group of symmetries of a lattice L. Then

1. *Every rotation in H has order $1, 2, 3, 4,$ or 6.*
2. *H is one of the groups C_n, D_n where $n = 1, 2, 3, 4,$ or 6.*

Proof. The second part of the proposition follows from the first. Let θ be the smallest nonzero angle of rotation in H, and let a be a nonzero vector in L of minimal length. Then since H oprates on L, $\rho_\theta(a)$ is also in L; hence $b = \rho_\theta(a) - a \in L$. Since a has a minimal length, $\mid b \mid \geq \mid a \mid$. It follows that $\theta \geq 2\pi/6$. Thus ρ_θ has order ≤ 6. The case that $\theta = 2\pi/5$ is also ruled out, because then the element $b' = \rho_{\theta^2}(a) + a$ is shorter than a: This completes the proof. $\square$

Let L be a lattice in $\mathbb{R}^2$. An element $v \in L$ is called *primitive* if it is not an integer multiple of another vector in L.

Corollary

Let L be a lattice, and let v be a primitive element of L. There is an element $w \in L$ so that the set (v, w) is a lattice basis.

Now let us go back to our discrete group of motions $G \subset \mathbf{M}$ and consider the rough classification of G accoding to the structure of its translation group L_G. If L_G is the trivial group, then the homomorphism from G to its point group is bijective and G is finite. We examined this case in Section 3.

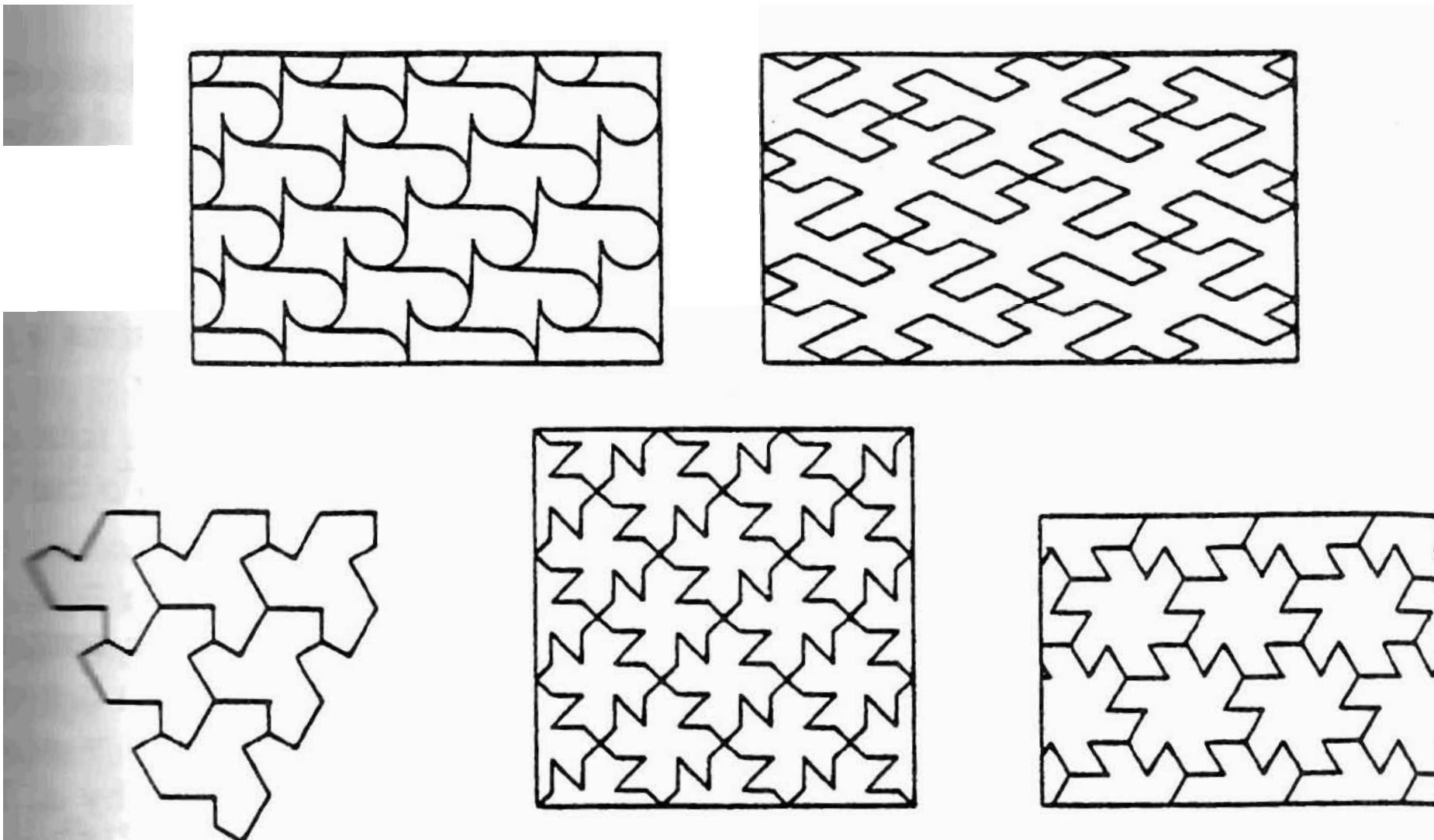
The discrete groups G such that L_G is inifinite cyclic are the symmetry groups of frieze patters. The classification of these groups is left as an exercise.

If L_G is a lattice, then G is called a *two–dimensional crystallographic group*, or a *lattice group*. These groups are the groups of symmetries of wallpaper patterns and of two–dimensional crystals.

The fact that any wallpaper pattern repeats itself in two different directions is reflected in the fact that its group of symmetries will always contain two independent translations, which shows that L_G is a lattice.

It may also contain further elements – translations, reflections, or glides – but the crystallographic groups into 17 types. The classification takes into account not only the intrinsic structure of the group, but also the type of motion that each group element represents. Representative patterns with the various types of symmetry are illustrated in Figure (4.16).
Proposition (4.11) is useful for determining the point group of a crystallographic group. For example, the brick pattern shown below has a rotational symmetry through the angle π about the centers of the bricks. All of these rotations represent the same element ρ_π of the point group $\overline{G}$. The pattern also has glide symmetry along the dotted line indicated. Therefore the point group $\overline{G}$ contains a reflection. By Proposition (4.11), $\overline{G}$ is a dihefral group. On the other hand, it is easy to see that the only nontrivial rotations in the group of G of symmetries are through the angle π. Therefore $\overline{G} = D_2 = \{1,\ \rho_\pi,\ r,\ \rho_\pi r\}$.

Example



Proposition

Let G be a lattice group whose point group contains a rotation ρ through the angle $\pi/2$. Choose coordinates so that the origin is a point of rotation by $\pi/2$ in G. Let a be a shortest vector in $L = L_G$, let $b = \rho(a)$, and let $c = \frac{1}{2}(a + b)$. Denote by r the reflection about the line spanned by a. Then G is generated by one of the following sets: $\{t_a, \rho\}$, $\{t_a, \rho, r\}$, $\{t_a, \rho, t_c r\}$. Thus there are three such groups.

Lemma

Let U be the set of vectors u such that $t_u r \in G$. Then

1. $L + U = U$.
2. $\rho U = U$.
3. $U + rU \subset L$.

Proof. If $v \in L$ and $u \in U$, then t_v and $t_u r$ are in G; hence $t_v t_u r = t_{v+u} r \in G$. This shows that $c + v \in U$ and proves (1). Next, suppose that $u \in U$. Then $\rho t_u r \rho = t_{\rho u} \rho r \rho = t_{\rho u} r \in G$. This shows that $\rho u \in U$ and proves (2). Finally, if $u, v \in U$, then $t_u r t_v r = t_{u+rv} \in G$; hence $u + rv \in L$, which proves (3). □

Outline

1. Symmetry
2. Rigid Motions
3. Rigid Motions in the Plane
4. Homework #4
5. Finite Groups of Motions
6. Discrete Groups of Motions
7. **Abstract Symmetry**
8. The Operation on Cosets
9. Homework #5
10. The Counting Formula
11. Finite Subgroups of the Rotation Group
12. Permutation Representation
13. Symmetric groups

Abstract Symmetry

Definition

Let G be a group and S a set. An *operation* of G on S is a map $G \times S \to S$ which satisfies the following axioms :

1. $1s = s$ for all s, 1 is the identity of G.
2. Associative law : $(gg')s = g(g's)$ for all $g, g' \in G$ and $s \in S$.

A set S with an operation of G is often called a *G–set*.

Example

Let $\mathbf{G} = \mathbf{M}$ be the group of all rigid motions of the plane. Then M operates on the set of points of the plane, on the set of lines in the plane, on the set of triangles in the plane, and so on.

Example

Let $\mathbf{G}$ be the cyclic group $\{1, r\}$ of order 2, with $r^2 = 1$. Then $\mathbf{G}$ operates on the set S of complex numbers, by the rule $r\alpha = \overline{\alpha}$.

Definition

Let S be a G–set. Let s be an element of S. The *orbit* of s in S is the set

$$O_s = \{s' \in S \mid s' = gs \text{ for some } g \in G\}.$$

Example

Let $\mathbf{G} = \mathbf{M}$ be the group of motions and S the set of triangles in the plane. The orbit O_Δ of a given triangle Δ is the set of all triangles congruent to Δ.

The orbits for a group action are equivalence classes for the relation

$$s \sim s' \text{ if } s' = gs \text{ for some } g \in G.$$

Being equivalence classes, the orbits partition the set S:

Proposition

S is a union of disjoint orbits.

The group **G** operates on S by operating independently on each orbit. In other words, an element $g \in \mathbf{G}$ permutes the elements of each orbit and does not carry elements of one orbit to another orbit.

Definition

If S consists of just one orbit, we say that **G** operates *transitively* on S.

Definition

The stabilizer of an element $s \in S$ is the subgroup G_s of G of elements leaving s fixed:

$$G_s = \{g \in G \mid gs = s\}.$$

Example

Consider the action of the group M of rigid motions on the set of points of the plane. The stabilizer of the origin is the subgroup $\mathbf{O}$ of orthogonal operators.

Example

Consider the action of the group M of rigid motions on the set of triangles in the plane. Let Δ be a particular triangle, which happens to be equilateral. Then the stabilizer of Δ is its group of symmetries, a subgroup of M isomorphic to D_3.

Outline

1. Symmetry
2. Rigid Motions
3. Rigid Motions in the Plane
4. Homework #4
5. Finite Groups of Motions
6. Discrete Groups of Motions
7. Abstract Symmetry
8. **The Operation on Cosets**
9. Homework #5
10. The Counting Formula
11. Finite Subgroups of the Rotation Group
12. Permutation Representation
13. Symmetric groups

The Operation on Cosets

- Let H be a subgroup of a group G. The set of left cosets is called the *coset space* and denoted by G/H.
- Though G/H is not a group unless the subgroup H is normal, nevertheless *G operates on the coset space G/H* in a natural way:
  Let g be an element of the group and let C be a coset. Then gC is defined to be the coset

$$gC = \{gc \mid c \in C\}.$$

  Thus if $C = aH$, then gC is the coset gaH.

Proposition

Let S be a G–set, and let s be an element of S. Let H be the stabilizer of s, and let O_s be the orbit of s. There is a natural bijective map

$$\varphi : G/H \longrightarrow O_s$$

defined by $\varphi(aH) = as$. This map is compatible with the operations of G in the sense that $\varphi(gC) = g\varphi(C)$ for every coset C and every element $g \in G$.

Proof. It is clear that map φ, if it exists, will be compatible with the operation of the group.
What is not so clear is that the rule $gH \rightsquigarrow gs$ defines a map at all. Since many symbols gH represent the same coset, we must show that if a and b are group elements and if $aH = bH$, then $as = bs$ too. This is true, because we know that $aH = bH$ if and only if $b = ah$ for some $h \in H$. And when $b = ah$, then $bs = ahs = as$ because h fixes s.
Next, the orbit of s consists of the elements gs, and φ carries gH to gs. Thus φ maps G/H onto O_s, and φ is surjective.
Finally we show that φ is injective. Suppose aH and bH have the same images : $as = bs$. Then $s = a^{-1}bs$. Since H was defined to be the stabilizer of s, this implies that $a^{-1}b = h \in H$. Thus $b = ah \in aH$, and so $aH = bH$. This completes the proof.
□

Proposition

Let S be a G-set, and let $s \in S$. Let s' be an element in the orbit of s, say $s' = as$. Then

(a) *The set of elements g of G such that $gs = s'$ is the left coset*

$$aG_s = \{g \in G \mid g = ah \text{ for some } h \in G_s\}.$$

(b *The stabilizer of s' is a* conjugate subgroup *of the stabilizer of s :*

$$G_{s'} = aG_sa^{-1} = \{g \in G \mid g = aha^{-1} \text{ for some } h \in G_s\}.$$

Outline

1. Symmetry
2. Rigid Motions
3. Rigid Motions in the Plane
4. Homework #4
5. Finite Groups of Motions
6. Discrete Groups of Motions
7. Abstract Symmetry
8. The Operation on Cosets
9. **Homework #5**
10. The Counting Formula
11. Finite Subgroups of the Rotation Group
12. Permutation Representation
13. Symmetric groups

Homework #5: Do 4 Problems

1. Prove that a discrete subgroup of **O** is a finite group.
2. Let $G = D_4$ be the dihedral group of symmetries of the square
   1. What is the stabilizer of a vertex? of an edge?
   2. G acts on the set of two elements consisting of the diagonal lines. What is the stabilizer of a diagonal?
3. Decompose the set $\mathbb{C}^{2\times 2}$ of 2×2 complex matrices for the operation of left multiplication by $GL_2(\mathbb{C})$.
4. Prove that the set of automorphisms of a group is a group. Determine the group of automorphisms of D_4.
5. Prove that if **H** and **K** are subgroups of finite index of a group **G**, then $\mathbf{H} \cap \mathbf{K}$ is also of finite index.

Outline

1. Symmetry
2. Rigid Motions
3. Rigid Motions in the Plane
4. Homework #4
5. Finite Groups of Motions
6. Discrete Groups of Motions
7. Abstract Symmetry
8. The Operation on Cosets
9. Homework #5
10. **The Counting Formula**
11. Finite Subgroups of the Rotation Group
12. Permutation Representation
13. Symmetric groups

The Counting Formula

Let H be a subgroup of G. All the cosets of H in G have the same number of elements : $|\ H\ | = |\ aH\ |$. Since G is a union of nonoverlapping cosets and the number of cosets is the index, which we write as $[G : H]$ or $|\ G/H\ |$, we have the fundamental formula for the order $|\ G\ |$of the group G :

$$|\ G\ | = |\ H\ |\ |\ G/H\ |\ .$$

Proposition

(Counting Formula) *Let S be a G–set and let $s \in S$. Then*

$$|\ G\ | = |\ G_s\cdot\ |\ |\ O_s\ |\ .$$

Equivalently, the order of the orbit is equal to the index of the stabilizer:

$$|\ O_s\ | = [G : G_s].$$

Another counting formula

Proposition

Let $\mathbf{G}$ *be a finite group and* S *a finite* $\mathbf{G}$*-set. If* $O_1, \ldots, O_k$ *are the distinct orbits of* $\mathbf{G}$*,*

$$|S| = |O_1| + \cdots + |O_k|.$$

Each $|O_i|$ *divides* $|\mathbf{G}|$*.*

Conjugation

One of the most useful actions of a group **G** is conjugation. It acts on itself as follows. Conjugation by $a \in \mathbf{G}$

$$x \to a^{-1}xa, \quad x \in \mathbf{G}.$$

- The orbit of x is the set $O_x = \{a^{-1}xa : a \in \mathbf{G}\}$
- The stabilizer of x is the set $C_x(\mathbf{G}) = \{a \in \mathbf{G} : a^{-1}xa\}$. This is the set of all elements of **G** that commute with x.
- The elements x whose orbit O_x have a single element, for instance 1, form the center of **G**. It is a subgroup: $Z(\mathbf{G})$.

The class equation

The counting formula for this action:

Theorem

Let $\mathbf{G}$ *be a finite group. Then*

$$|\mathbf{G}| = \sum |O_x| = |Z(\mathbf{G})| + \sum [\mathbf{G} : C_x(\mathbf{G})].$$

An useful formula

Proposition

Let $\mathbf{H}$ *and* $\mathbf{K}$ *be subgroups of a group* $\mathbf{G}$*. Then*

$$[\mathbf{H} : \mathbf{H} \cap \mathbf{K}] \leq [\mathbf{G} : \mathbf{K}].$$

Proof. Let S denote the coset space $\mathbf{GK}$, and the coset $1\mathbf{K} = s$.

- $|S| = [\mathbf{G} : \mathbf{K}]$, and the stabilizer of s is $\mathbf{K}$.
- Restrict the action of $\mathbf{G}$ on S to an action of $\mathbf{H}$ and decompose S into $\mathbf{H}$-orbits. The stabilizer of s for this action is $\mathbf{H} \cap \mathbf{K}$.
- The $\mathbf{H}$-orbit of s is a subset of S. By the counting formula $|O| = [\mathbf{H} : \mathbf{H} \cap \mathbf{K}]$. Therefore

$$[\mathbf{H} : \mathbf{H} \cap \mathbf{K}] = |O| \leq |S| = [\mathbf{G} : \mathbf{K}].$$

Outline

1. Symmetry
2. Rigid Motions
3. Rigid Motions in the Plane
4. Homework #4
5. Finite Groups of Motions
6. Discrete Groups of Motions
7. Abstract Symmetry
8. The Operation on Cosets
9. Homework #5
10. The Counting Formula
11. **Finite Subgroups of the Rotation Group**
12. Permutation Representation
13. Symmetric groups

Finite Subgroups of the Rotation Group

Theorem

Every finite subgroup G of SO_3 is one of the following:

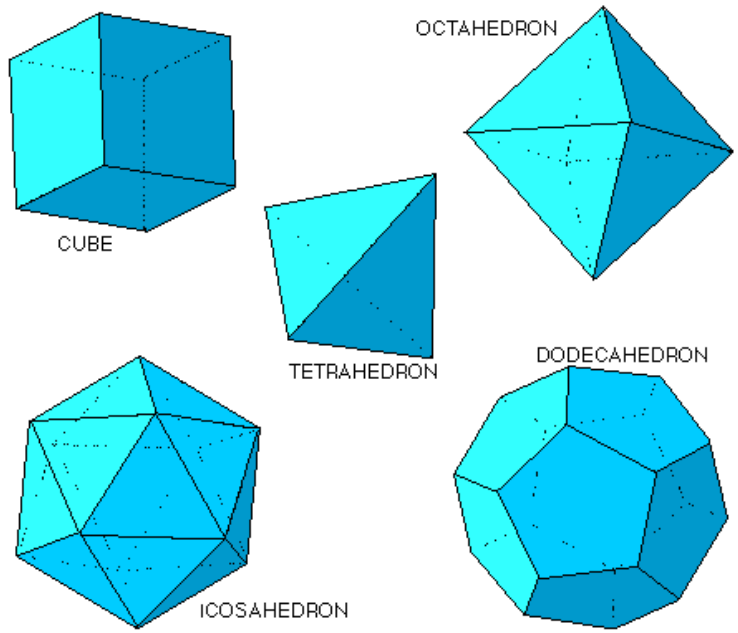
1. C_k *: the* cyclic group *of rotations by multiplies* $2\pi/k$ *about a line ;*
2. D_k *: the* dihedral group *of symmetries of a regular k–gon ;*
3. T *: the* tetrahedral group *of twelve rotations carrying a regular tetrahedron to itself ;*
4. O *: the* octahedral group *of order* 24 *of rotations of a cube, or of a regular octahedron;*
5. I *: the* icosahedral group *of* 60 *rotations of a regular dodecahedron or a regular icosahedron.*

Example

Regular Polyhedra

Regular Polyhedra

also known as Platonic Solids



Kaleidotile was used to help create this image.

There are just five platonic solids.

From equilateral triangles you can make:

with 3 faces at each vertex, a tetrahedron;

Outline

1. Symmetry
2. Rigid Motions
3. Rigid Motions in the Plane
4. Homework #4
5. Finite Groups of Motions
6. Discrete Groups of Motions
7. Abstract Symmetry
8. The Operation on Cosets
9. Homework #5
10. The Counting Formula
11. Finite Subgroups of the Rotation Group
12. **Permutation Representation**
13. Symmetric groups

Permutation Representation

The symmetric group S_n operate on the set $S = \{1, \ldots, n\}$. A permutation representation of a group $\mathbf{G}$ is a homomorphism

$$\varphi : \mathbf{G} \to S_n.$$

Thus, for $\mathbf{g} \in \mathbf{G}$, $\varphi(\mathbf{g})$ is a permutation of S.

Proposition

There is a bijective correspondence

$$\left(\begin{array}{c} \text{operations} \\ \text{of } \mathbf{G} \text{ on } S \end{array} \right) \leftrightarrow \left(\begin{array}{c} \text{homomorphisms} \\ \mathbf{G} \to \text{Perm}(S) \end{array} \right)$$

defined by: Given an operation m define $\varphi : \mathbf{G} \to \text{Perm}(S)$ by the rule $\varphi(\mathbf{g}) = m_{\mathbf{g}}$.

Let us show that φ is a homomorphism. We've already noted that m_g is a permutation. So as dfined above, $\varphi(g) \in \mathrm{Perm}(S)$. The axiom for a homomorphism is $\varphi(xy) = \varphi(x)\varphi(y)$, or $m_{xy} = m_x m_y$, where multiplication is composition of permutations. So we have to show that $m_{xy}(s) = m_x(m_y(s))$ for every $s \in S$. By definition $m_{xy}(s) = (xy)s$ and $m_x(m_y(s)) = x(ys)$. The associative law for group operations shows that $(xy)s = x(ys)$, as required. $\square$

Proposition

The group $GL_2(\mathbb{F}_2)$ of invertible matrices with mod 2 coefficients is isomorphic to the symmetric group S_3.

Proof. Let us denote the field $\mathbb{F}_2$ by F, and the group $GL_2(\mathbb{F}_2)$ by G. We have listed the six elements of G before. Let $V = F^2$ be the space of column vectors. This space consists of the following four vectors : $V = \{0, e_1, e_2, e_1 + e_2\}$. The group G operates on V and fixes 0, so it operates on the set of three nonzero vectors, which form one orbit. This gives us a permutation representation $\varphi : G \longrightarrow S_3$. Now the image of e_1 under multiplication by a matrix $P \in G$ is the first column of P, and similarly the image of e_2 is the second column of P. Therefore P can not operate trivially on these two elements unless it is the identity. This shows that the operation of G is faithful, and hence that the map φ is injective. Since both groups have order 6, φ is an isomorphism. □

Proposition

The group of automorphism of the cyclic group of order p is isomorphic to the multiplicative group $\mathbb{F}_p^\times$ of nonzero elements of $\mathbb{F}_p$.

Proof. The method here is to use the additive group $\mathbb{F}_p^\times$ as the model for a cyclic group of order p. It is generated by the element 1. Let us denote the multipliative group $\mathbb{F}_p^\times$ by G. Then G operates on $\mathbb{F}_p^+$ by left multiplication, and this operation defines an injective homomorphism $\varphi : G \longrightarrow \mathrm{Perm}(\mathbb{F}_p)$ to the group of permutations of the set $\mathbb{F}_p$ of p elements.
Next the group $A = \mathrm{Aut}(\mathbb{F}_p^+)$ of automorphisms is a subgroup of $\mathrm{Perm}(\mathbb{F}_p^+)$. The distributive law shows that multiplication by an element $a \in \mathbb{F}_p^\times$ is an automorphism of $\mathbb{F}_p^+$. It is bijective, and $a(x + y) = ax + ay$. Therefore the image of $\varphi : G \longrightarrow \mathrm{Perm}(\mathbb{F}_p^+)$ is contained in the subgroup A. Finally, an automorphism of $\mathbb{F}_p^+$ is determined by where it sends the generator 1, and the image of 1 can not be zero. Using the operations of G, we can send 1 to any nonzero element. Therefore φ is a surjection from G onto A. Being both injective and surjective, φ is an isomorphism. $\square$

Outline

1. Symmetry
2. Rigid Motions
3. Rigid Motions in the Plane
4. Homework #4
5. Finite Groups of Motions
6. Discrete Groups of Motions
7. Abstract Symmetry
8. The Operation on Cosets
9. Homework #5
10. The Counting Formula
11. Finite Subgroups of the Rotation Group
12. Permutation Representation
13. **Symmetric groups**

Definition

A group G is said to be *simple* if G has no proper normal subgroups.

Theorem

The alternating group A_n is simple if and only if $n \neq 4$.

The proof we shall give is quite elementary. It will be preceded by two lemmas. Recall that if τ is a 2-cycle, $\tau^2 = (1)$ and hence $\tau = \tau^{-1}$.

Lemma

Let r, s be distinct elements of $\{1, 2, \ldots, n\}$. Then A_n ($n \geq 3$) is generated by the 3-cycles

$$\{(rsk) \mid 1 \leq k \leq n,\ k \neq r, s\}.$$

Proof. Assume $n > 3$ (the case $n = 3$ is trivial). Every element of A_n is a product of terms of the form $(ab)(cd)$ or $(ab)(ac)$, where a, b, c, d are distinct elements of $\{1, 2, \ldots, n\}$. Since $(ab)(cd) = (acb)(acd)$ and $(ab)(ac) = (acb)$, A_n is generated by the set of all 3-cycles. Any 3-cycle is of the form $(rsa), (ras), (rab), (sab)$, or (abc), where a, b, c are distinct, and $a, b, c \neq r, s$. Since $(ras) = (rsa)^2$, $(rab) = (rsb)(rsa)^2$, $(sab) = (rsb)^2(rsa)$, and $(abc) = (rsa)^2(rsc)(rsb)^2(rsa)$, A_n is generated by

$$\{(rsk) \mid 1 \leq k \leq n,\ k \neq r, s\}.$$

□

Lemma

If N is a normal subgroup of A_n ($n \geq 3$) and N contains a 3–cycle, then $N = A_n$.

Proof. If $(rsc) \in N$, then for any $k \neq r, s, c$,

$$(rsk) = (rs)(ck)(rsc)^2(ck)(rs) = [(rs)(ck)](rsc)^2[(rs)(ck)]^{-1} \in N.$$

Hence $N = A_n$.

Proof. $A_2 = (1)$ and A_3 is the simple cyclic group of order 3. It is easy to verfify that

$$\{(1),\ (12)(34),\ (13)(24),\ (14)(23)\}$$

is a normal subgroup of A_4. If $n \geq 5$ and N is a nontrivial normal subgroup of A_n, we shall show $N = A_n$ by considering the possible cases.

Case 1. N contains a 3-cycle; hence $N = A_n$.

Case 2. N contains an element σ, the product of disjoint cycles, at least one of which has length $r \geq 4$. Thus $\sigma = (a_1 a_2 \cdots a_r)\tau$ (disjoint). Let $\delta = (a_1 a_2 a_3) \in A_n$. Then $\sigma^{-1}(\delta\sigma\delta^{-1}) \in N$ by normality. But

$$\begin{aligned} \sigma^{-1}(\delta\sigma\delta^{-1}) &= \tau^{-1}(a_1 a_r a_{r-1} \cdots a_2)(a_1 a_2 a_3)(a_1 a_2 \cdots a_r)\tau(a_1 a_3 a_2) \\ &= (a_1 a_3 a_r) \in N. \end{aligned}$$

Hence $N = A_n$.

Case 3. N contains an element σ, the product of disjoint cycles, at least two of which have length 3, so that $\sigma = (a_1 a_2 a_3)(a_4 a_5 a_6)\tau$ (disjoint). Let $\delta = (a_1 a_2 a_4) \in A_n$. Then as above N contains

$$\begin{aligned} & \sigma^{-1}(\delta\sigma\delta^{-1}) \\ = \ & \tau^{-1}(a_4 a_6 a_5)(a_1 a_3 a_2)(a_1 a_2 a_4)(a_1 a_2 a_3)(a_4 a_5 a_6)\tau(a_1 a_4 a_2) \\ = \ & (a_1 a_4 a_2 a_6 a_3). \end{aligned}$$

Hence $N = A_n$ by case 2.

Case 4. N contains an element σ that is the product of one 3-cycle and some 2-cycles, say $\sigma = (a_1 a_2 a_3)\tau$ (disjoint), with τ a product of disjoint 2-cycles. Then $\sigma^2 \in N$ and

$$\sigma^2 = (a_1 a_2 a_3)\tau(a_1 a_2 a_3)\tau = (a_1 a_2 a_3)^2\tau^2 = (a_1 a_2 a_3)^2 = (a_1 a_3 a_2),$$

whence $N = A_n$.

Case 5. Every element of N is the product of (an even number of) disjoint 2-cycles. Let $\sigma \in N$, with $\sigma = (a_1 a_2)(a_3 a_4)\tau$ (disjoint). Let $\delta = (a_1 a_2 a_3) \in A_n$; then $\sigma^{-1}(\delta\sigma\delta^{-1}) \in N$ as above. Now

$$\begin{aligned} \sigma^{-1}(\delta\sigma\delta^{-1}) &= \tau^{-1}(a_3 a_4)(a_1 a_2)(a_1 a_2 a_3)(a_1 a_2)(a_3 a_4)\tau(a_1 a_3 a_2) \\ &= (a_1 a_3)(a_2 a_4). \end{aligned}$$

Since $n \geq 5$, there is an element $b \in \{1, 2, \ldots, n\}$ distinct from a_1, a_2, a_3, a_4. Since $\zeta = (a_1 a_3 b) \in A_n$ and $\xi = (a_1 a_3)(a_2 a_4) \in N$, $\xi(\zeta\xi\zeta^{-1}) \in N$. But

$$\xi(\zeta\xi\zeta^{-1}) = (a_1 a_3)(a_2 a_4)(a_1 a_3 b)(a_1 a_3)(a_2 a_4)(a_1 b a_3) = (a_1 a_3 b) \in N.$$

Hence $N = A_n$.
Since the cases listed cover all the possibilities, A_n has no proper normal subgroups and hence is simple. □