Apprentice Lectures

Daniil Rudenko
LaTeX by Agustin Esteva

July 19, 2024

Contents

Chapter 1

Lecture 1- Combinatorics and Isometries

1.1 Combinatorics

Example.

> How many subsets of $A = \{1, 2, \ldots, n\}$? 2^n.

Proof. (By Induction)

1. If $A = \{1\}$ then there exists $\emptyset$ and $\{1\}$ as subsets of A. Thus there exist $2^1 = 2$ subsets.
2. If $A = \{1, 2, \ldots, n-1\}$, then assume that there exist 2^{n-1} subsets of A.
3. If n, then let $Y = \{1, 2, \ldots, n-1\}$ and $X = \{1, 2 \ldots, n\}$. Evidently, there exists an isomorphism between Y and A, and thus there are 2^{n-1} subsets in Y. Let $f : X \to X \setminus \{n\}$. Now, X is in bijective correspondence with A, and thus there are 2^{n-1} subsets in X. Therefore, there are $2^{n-1} + 2^{n-1} = 2^n$

$\square$

Proof. (With Linear Algebra)
It will suffice to show that $[2^n]$ (the power set of any set with cardinality n, is isomorphic to $\mathbb{F}_2^n$.)
First, to show that $[2^n]$ is a valid vector field of $\mathbb{F}_2$ with multiplication and addition defined as follows: If $X, Y \in [2^n]$, then:

$$X + Y = X \Delta Y = (X \setminus Y) \cup (Y \setminus X) \qquad 1 \cdot X = X \qquad 0 \cdot X = \emptyset$$

1. Commutativity, to prove that $X+Y = Y+X$, it will suffice to show that the symmetric difference is commutative, which it is.

2. Δ is associative.
3. There exists a $\emptyset$ in $[2^n]$ such that $X + \emptyset = X\Delta\emptyset = X$.
4. The additive inverse is $-X = X$. To prove this, note that $-X + X = X\Delta X = \emptyset$.
5. 1 is multiplicative identity by definition.
6. All the rest of the axioms are similarly proved.

$\square$

Definition 1.1.1: Binomial Coefficients

The number of subsets of size k in the set $\{1, 2, \ldots, n\}$, usually denoted by $\binom{n}{k}$

Remark.

> From the previous example, it is evident that
>
> $$\sum_{i=1}^{n} \binom{n}{i} = 2^n$$

Theorem 1.1.2: Binomial Coefficient Identity

$$\binom{n}{k} = \binom{n}{n-k}$$

Proof. Let X be a subset of $A = \{1, 2, \ldots, n\}$ of size k. Let $f : X \to A \setminus X$ be a function and $g : Y \to A \setminus Y$ be a function, where Y is a set in the domain of f. It will suffice to show that $g \circ f$ is a bijection. Let $gf(X_1) = gf(X_2)$. Therefore, because $A \setminus (A \setminus X_1) = X_1$ and $A \setminus (A \setminus X_2) = X_2$, then $X_1 = X_2$, and so $g \circ f$ is injective. Assume that there exists some X such that $X \neq A \setminus (A \setminus X)$. However, this is impossible. $\square$

Remark.

> This result (and the next) lead to an interesting way to represent binomial coefficients:

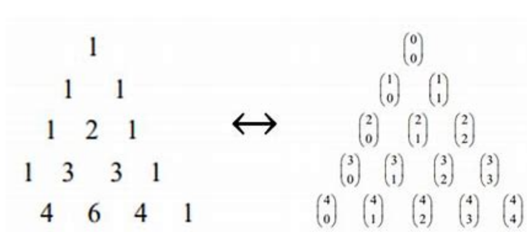


Figure 1.1: Pascal's Triangle for Binom. Coefficients

Theorem 1.1.3: Morgan's Identity

$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$

Proof. Let X be the subsets of size k containing the element n and let Y be the subsets of size k not containing n. Like in Example 1, Y is in bijective correspondence with the subsets of $\{1, 2, \ldots, n-1\}$ of size k. Moreover, X is also in bijective correspondence with subsets of $\{1, 2, \ldots, n-1\}$ of size $k-1$ (since you must take away an element, the sizes of the subsets decreases). $\square$

1.2 Isometries

Definition 1.2.1: Isometry

A map $f : \mathbb{R}^2 \to \mathbb{R}^2$ is an *isometry* if:

1. It is bijective.
2. Distance is preserved, i.e, for all $x, y \in \mathbb{R}^2$, $|xy| = |f(x)f(y)|$

Example.

1. The identity map is an example of an isometry.
2. We call the map $\mathbb{S}_O : \mathbb{R}^2 \to \mathbb{R}^2$ a symmetric difference, as it reflects points across some specified point, O. Thus, $\mathbb{S}_O(X) = Y$, where O is the middle of the segment $[XY]$. Note that $\mathbb{S}_O$ preserves distances as given any $X_1, X_2 \in \mathbb{R}^2$, the triangles $\triangle X_1OX_2 \sim Y_1OY_2$, and thus $|X_1X_2| = |Y_1Y_2|$.

   Remark.

   $\mathbb{S}_O \circ \mathbb{S}_O = \mathrm{Id}$

3. A translation, or a parallel transport, is a function, $T_{\mathbf{v}} : \mathbb{R}^2 \to \mathbb{R}^2$ such that given some vector $\mathbf{v}$ and some $X \in \mathbb{R}^2$, then $T_{\mathbf{v}}(X) = Y$ such that $\overrightarrow{XY} = \mathbf{v}$.

   Remark.

   A vector, $\mathbf{v}$, is defined as follows:

   (a)
   $$\mathbf{v} = (\text{segment} + \text{orientation}) \mod \sim\sim\sim\sim,$$
   where, given any $ABCD \in \mathbb{R}^2$, $\sim$ is defined by:

      i. $|AB| || |CD|$ (equivalent vectors are parallel).
      ii. $|AB| = |CD|$ (equivalent vectors have the same magnitude).
      iii. B, D are on the same side of AC (equivalent vectors have the same orientation).

4. A rotation around some point, $O \in \mathbb{R}^2$, by φ degrees, is a map $R_O^{\varphi}(X) = Y$ such that $|OX| = |XY|$ and there is a counterclockwise rotation from $\overline{OX}$ to $\overline{XY}$ by φ degrees

Fact 1.2.2

If $f, g \in \mathrm{Isom}(\mathbb{R}^2)$, then $f \circ g \in \mathrm{Isom}(\mathbb{R}^2)$.

Proof.

1. The compositions of bijections is a bijection, and thus $f \circ g$ is a bijection.
2. Given any $X_1X_2 \in \mathbb{R}^2$, since g and f preserves distances since it's an isometry, then

$$|(f \circ g)(X_1)(f \circ g)(X_2)| = |fg(X_1)fg(X_2)| = |g(X_1)g(X_2)| = |X_1X_2|.$$

$\square$

Chapter 2

Lecture 2- The Binomial Theorem/Formula and Groups

2.1 The Binomial Formula

Theorem 2.1.1: The Binomial Theorem

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

Before this proof, it will be useful to understand how this works for $(a+b)^3$. To do this, let's decompose the expression:

$$(a+b)^3 = (a+b) \cdot (a+b) \cdot (a+b)$$

This, of course, yields

$$aaa + aab + aba + baa + abb + bba + bab + bbb$$

and this is equal to

$$a^3 + 3a^2b + 3ab^2 + b^3.$$

Note that if we count the brackets in the first expression as say, $1, 2, 3$, thus we have the set $\{1, 2, 3\}$, where each element encodes a pair of brackets, then for the second expression we could denote this as all the possible subsets of $\{1, 2, 3\}$, where if the element appears, an a is placed, and if not, then a b is placed. Thus, the subset $\{1, 3\}$ corresponds to aba and the emptyset corresponds to bbb. Therefore,

$$a^3 + 3a^2b + 3ab^2 + b^3 = \sum_{X \subseteq \{1,2,3\}} \prod_{1 \leq i \leq 3} (\text{an } a \text{ if } i \in X \text{ and } b \text{ if } i \notin X.) = \sum_{X \in \{1,2,3\}} a^{|X|} b^{3-|X|}$$

Proof. As the example above hows,

$$(a+b)^n = (a+b)\cdot(a+b)\cdots(a+b)\{\text{n-times}\} = \sum_{X\subseteq \text{set of } \{1,2,3,\ldots,n\}} a^{|X|}b^{n-|X|} = \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}$$

□

Remark.

> One could pretty easily do binomial expansion using Pascal's Triangle, the coefficients are just the numbers in the triangle.

Corollary 2.1.2

$$2^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n}$$

Proof.

$$2^n = (1+1)^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n}$$

□

Theorem 2.1.3: The Binomial Coefficient Formula

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Before this proof, consider $5 = 5$. This is a trivial statement, but it can mean a lot of things. Do 5 crocodiles equal 5 ducks? That's ridiculous! $5 = 5$ **but not in a unique way.** In fact,

$$\text{permuting a set of } n \text{ obects} = \#\text{ bijections from } \{1,2,\ldots,n\} \text{ to itself} = n! = \mathbb{S}_n$$

Proof. Count the number of permutations in two different ways. The first is by permuting everything using a factorial. The second is to choose k elements out of the n, then seeing how many permutations can occur within those k elements, then seeing how many can occur in the $n-k$ elements. Thus $n! = \binom{n}{k}k!(n-k)!$, and we are done, as rearranging this yields the thesis. □

Corollary 2.1.4

A set of size n has 2^{n-1} even subsets

Proof.

1. If n is even, then $(-1+1)^n = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 0$, and so by moving all the negative terms to the right,

$$\sum_{k=2i}\binom{n}{k} = \sum_{k=2i+1}\binom{n}{k}$$

and thus because there are the same number of even and odd subsets, we get 2^{n-1} subsets.

2. If n is odd, then let $f : 2^A \to 2^A$ such that if $X \in 2^A$, then $f(X) = A \setminus X$, and thus because this map is bijective, then there are the same number of X as $A \setminus (X)$, and since those have different parity, then there are the same number of even and odd sets.

Remark.

> One could also try this using Linear Algebra, as consider the subspace $W \subseteq 2^A = V$ of all the even subsets.Note that because addition was defined on this vector space as Δ, and Δ is mantains parity of evens, then W is a valid subspace. Consider that $|V| = 2^n = 2^{\dim(V)}$. Thus, $|W| = 2^{\dim(W)}$. Consider that $\beta = \{\{1,2\},\{2,3\},\ldots,\{n-1,n\}\}$ is a valid basis of W, and thus we are done.

□

2.2 Introduction to Groups

Example.

> Consider the following two statements:
>
> $$T_{\mathbf{v}} \circ T_{\mathbf{w}} = T_{\mathbf{v}+\mathbf{w}} \qquad S_{O_2} \circ S_{O_2} = T_{2\overrightarrow{O_1O_2}}$$
>
> These proves should be clear geometrically.

Definition 2.2.1: Group

A *group*, G, is a set with an operation $G \times G \to G$ such that $(g_1, g_2) \to g_1 * g_2$ such that:

1. For all $g_1, g_2, g_3 \in G$, $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$.
2. There exists a unit, $e \in G$, suchat that $g * e = e * g = g$.
3. For all $g \in G$, there exists a g', usually denoted as g^{-1}, or then inverse of g, such that $g * g^{-1} = e$.

	Object	Operation $(*)$
1	$\mathbb{Z}$	$+$
2	$\mathbb{R}$	$+$
3	$\mathbb{R} \setminus \{0\}$	$\times$
4	$\text{Isom}(\mathbb{R}^2)$	$\circ$
5	$\mathbb{S}_n$	$\circ$
6	$GL_n(F)$, or Invertible matrices of size $n \times n$	$\times$

Table 2.1: Common Groups

Chapter 3

Lecture 3- Groups and Catalan Numbers

3.1 Groups

Definition 3.1.1: Abelian Group

An *Abelian Group* is a group in which, $*$, the operation of the group, is commutative.

Example.

> For Isom($\mathbb{R}^2$), it is generally not the case that $f \circ g = g \circ f$, as is evidenced by the first example in 2.2

Example.

> More examples of groups:
>
> 1. $G = \{e\}$
> 2. $G = \{e, x\}$ and thus x must be its own inverse. Some examples include $G = \{-1, 1\}, \times$ and $G = \{0, 1\} \subset \mathbb{F}_2, +$
> 3. $G = \{e, x, y\}$

Table for ex 2:

$*$	e	x
e	e	x
x	x	e

Table for ex 3:

$*$	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

Definition 3.1.2: Isomorphism

Let G_1, G_2 be 2 groups. A map: $\varphi : G_1 \to G_2$ is an isomorphism if:

1. φ is a bijection.
2. For all $g_1, g_2 \in G_1$, $\varphi(g_1 *_{G_1} g_2) = \varphi(g_1) *_{G_2} \varphi(g_2)$.

For example, example $G = \{e, x\}$ only has one isomorphism, as the multiplication table is unique, but something like $|G| = 4$, which has 2 multiplication tables, has two isomorphism.

Corollary 3.1.3

The following are properties of any group, G :

1. The identity element is unique.
2. If g' is an inverse such that $g * g' = e$, then $g' * g = e$.
3. Inverses are unique.

Proof. :

1. Let e, e' be identity elements of a group, then $e = e * e' = e$.
2. Let g' be the inverse of g and g'' the inverse of g'.

$$\begin{aligned} g * g' &= e \\ g' * (g * g') &= g' * e \\ (g' * g) * g' &= g' \\ (g' * g) * g' * g'' &= g' * g'' \\ (g' * g) * e &= e \\ g' * g &= e \end{aligned}$$

3. Let g' and g'' be inverses of g, then:

$$
\begin{aligned}
g * g' &= g * g'' \\
g' * (g * g') &= g' * (g * g'') \\
(g' * g) * g' &= (g' * g) * g'' \\
e * g' &= e * g'' \\
g' g''
\end{aligned}
$$

$\square$

3.2 Catalan Numbers

How many ways are there to arrange parenthesis on

$$g_1 * g_2 * g_3 * g_4?$$

1. $(((g_1 * g_2) * g_3) * g_4)$

2. $((g_1 * (g_2 * g_3)) * g_4)$

3. $(g_1 * (g_2 * (g_3 * (g_4))))$

4. $(g_1 * ((g_2 * g_3) * g_4))$

5. $(g_1 * g_2) * (g_3 * g_4)$

Thus, we can let C_{n-1} be the number of ways to arrange parenthesis on $g_1 * g_2 * \cdots * g_n$ (By the exercise above, $C_3 = 5$.)

Fact 3.2.1

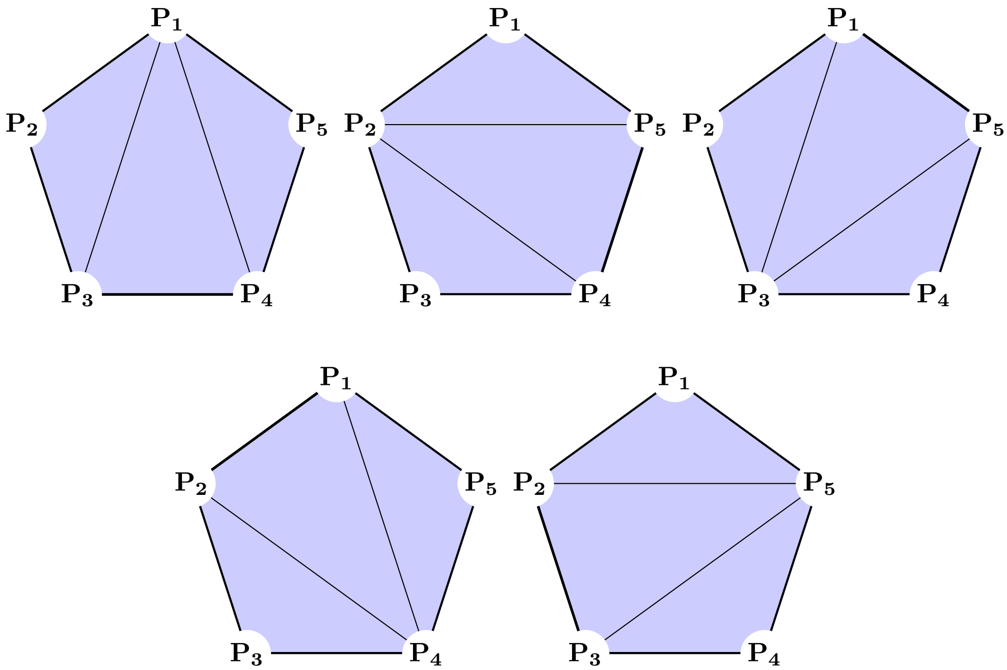
There exists a bijection between the number of ways to put parenthesis in $g_1 * g_2 * \cdots * g_n$ and number of ways to triangulate an $n + 1$ polygon

Remark.

Note that in an $n + 1-$gon, there are $n - 1$ triangles

Example.

For the $n = 4$ case:

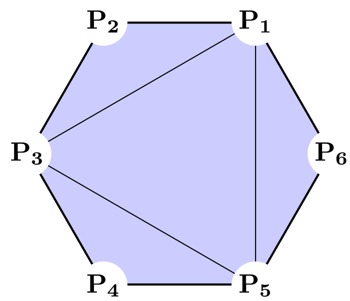


Thus, because there are 5 ways to triangulate a polygon, then there are 5 ways to rearrange the parenthesis.

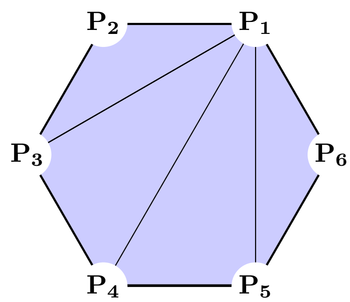
Example.

For the $n = 5$ case, consider a hexagon:

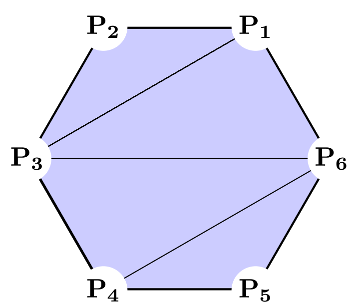
There are two possible combinations of this triangulation:



6 possible combinations of this triangulation:



and 6 more combinations of this triangulation:

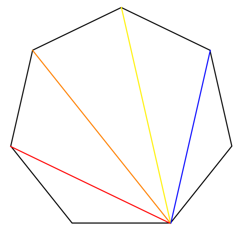


Thus, $C_5 = 14$.

Theorem 3.2.2: Catalan Numbers Formula

$$C_{n-1} = \sum_{i+j=n-1} C_i C_j$$

Proof.



One can create different polygons with each different line, so for example, with the red line, C_5, then with the orange, and so on and on. □

Chapter 4

Lecture 4- Symmetries of Shapes and Modulo Arithmetic

4.1 Symmetries

Definition 4.1.1: A figure

A figure $\mathcal{F}$ is a subset of $\mathbb{R}^2$. $\mathcal{F} \subset \mathbb{R}^2$.

Example.

> $\triangle$

Definition 4.1.2: Symmetry

A symmetry is defined as $\text{Sym}(\mathcal{F}) = \{f \in \text{Isom}(\mathbb{R}^2) | f(\mathcal{F}) = \mathcal{F}\}$

Definition 4.1.3: Subgroup

We define H to be a group, G, if:

1. $e \in H$.
2. For all $h_1, h_2 \in H$, $h_1 * h_2 \in H$.
3. For all $h \in H$, there exists a $h^{-1} \in H$.

Remark.

> Note that symmetries are subgroups of $\text{Isom}(\mathbb{R}^2)$.

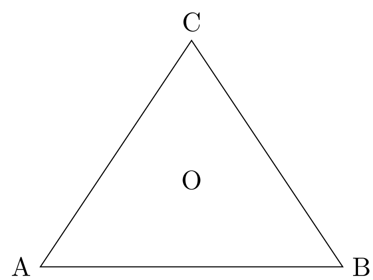
Example.

Various symmetries:

1. $|\text{Sym}(\triangle)| = 6$.
2. $|\text{Sym}(\square)| = 8$.

3. $\text{Sym}(\text{rectangle}) = 4$.
4. $\text{Sym}(\text{pentagon}) = 10$.

But how do we prove, say, that $\text{Sym}(\triangle) = 6$? Consider the following reference:



The key is that any symmetry, $f(\triangle) = \triangle$, will send vertices to vertices, that is $f(\{A, B, C\}) = \{A, B, C\}$. That is to say, f is a bijection from $\{A, B, C\}$ to itself, and so it permutes $\{A, B, C\}$. Therefore, we can construct a map

$$\varphi : \text{Sym}(\triangle) \to \mathbb{S}_n$$

, where $\mathbb{S}_3$ is defined as in Theorem 2.1.3.

Proposition 4.1.4

$\varphi : \text{Sym}(\triangle) \to \mathbb{S}_n$ is an isomorphism

Proof.

1. To first show that φ is a homomorphism, that is, $\varphi(g_1 * g_2) = \varphi(g_1) * \varphi(g_2)$, it is obvious that the composition of symmetries is the same as the symmetry of compositions.

2. To show that φ is surjective, consider first the space of all possible ways to permute $\mathbb{S}_3$:

$$\begin{pmatrix} A & B & C \\ A & B & C \\ & \varphi(\text{Id}) & \end{pmatrix} \quad \begin{pmatrix} A & B & C \\ A & C & B \\ & \varphi(\mathbb{S}_{OA}) & \end{pmatrix} \quad \begin{pmatrix} A & B & C \\ B & A & C \\ & \varphi(\mathbb{S}_{OC}) & \end{pmatrix}$$

$$\begin{pmatrix} A & B & C \\ B & C & A \\ & \varphi(R_O^{240^\circ}) & \end{pmatrix} \quad \begin{pmatrix} A & B & C \\ C & A & B \\ & \varphi(R_O^{120^\circ}) & \end{pmatrix} \quad \begin{pmatrix} A & B & C \\ C & B & C \\ & \varphi(\mathbb{S}_{OC}) & \end{pmatrix}$$

And thus, because every permutation has some symmetry relating to it, then φ is surjective.

3. Before proving that φ is injective, it will be helpful to prove a little lemma and a corollarly:

Lemma 4.1.5

If $A, B, C \in \mathbb{R}^2$ are not on the same line and $f \in \text{Isom}(\mathbb{R}^2)$ such that $f(A) = A$, $f(B) = B$, and $f(C) = C$, then $f = \text{Id}$

Proof. Consider two circles of the same size, C_1 and C_2, who's centers are at A and B, respectively. Consider then a third circle at C, C_3, that is a bit bigger. Then let $x \in C_1 \cap C_2 \cap C_3$, and because $f \in \text{Isom}(\mathbb{R}^3,)$, then it preserves distances, and so $f(x) \in C - 1 \cap C_2 \cap C_3$. Consider just C_1 and C_2, if they touch at just one point, then it is impossible for $f(x)$ to be such point, since C_C doesn't intersect the circle as both points. If they touch at all points, then $C_1 = C_2$ and so $A = $. Therefore, they must touch at two points and $f(x) = x$ with a geometric argument. □

Corollary 4.1.6

If $A, B, C \in \mathbb{R}^2$ are not on the same line and $f, g \in \text{Isom}(\mathbb{R}^2)$ such that $f(A) = g(A)$, $f(B) = g(B)$, and $f(C) = g(C)$, then $f = g$

Proof. Consider that $f(A) = g(A)$, and so $fg^{-1}(A) = A$, and the same for the rest, and so by the lemma, $fg^{-1} = Id$, and thus $f = g$. □

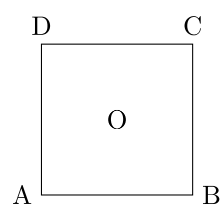
Thus, back to the proof: Suppose $\varphi(g_1) = \varphi(g_2)$, then by the corollary above, $g_1 = g_2$, and so φ is injective.

□

However, this bijection does not hold for something like a square! Specifically, the surjectiveness breaks down, since, for example, there exists the permutation of vertices $\{A, B, C, D\}$ into vertices $\{A, B, D, C\}$, but that is impossible as a symmetry, as is clear by just trying to think of a symmetry which only change two verticies but not the other.

Fact 4.1.7

A symmetry keeps vertices together



Theorem 4.1.8: Sym(P_n) $= 2n$

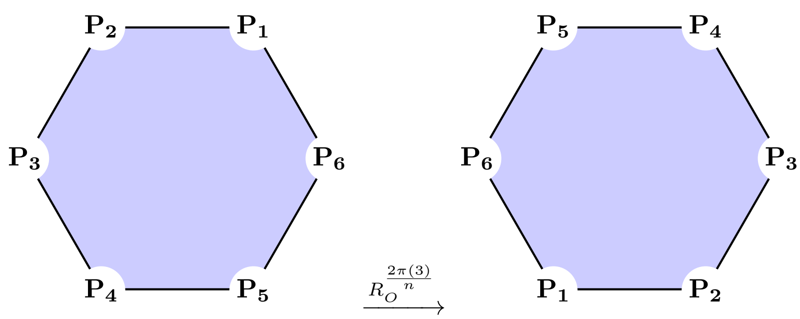
A regular polygon has $2n$ symmetries, were n is the number of vertices of a polygon.

Proof. Consider that a symmetry, f, must send $f(A_i) = \{A_1, A_2, \ldots, A_n\}$. Therefore, if $A_1 = A_k$, then, by the fact above, either:

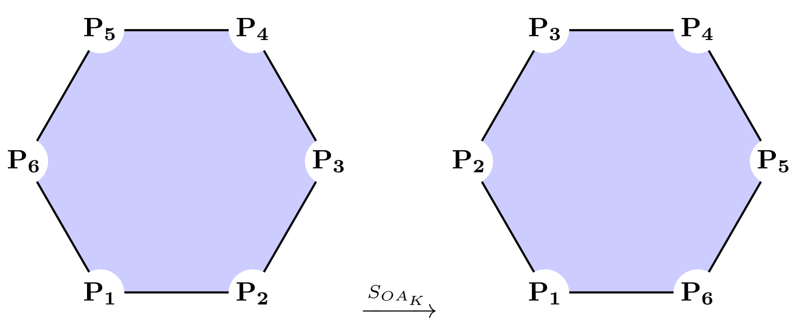
1. $f(A_2) = A_{k-1}$ and $f(A_n) = A_{k+1}$
2. $f(A_2) = A_{k+1}$ and $f(A_n) = A_{k-1}$

(Note that by the corollary above, this is enough to construct the symmetry)

1. In the second case, we are dealing with a rotation by $\frac{2\pi}{n}(k-1)$, or $R_O^{\frac{2\pi}{n}(k-1)}$.



2. In the second case, we can think of it as the same rotation as the first case, and then a symmetry across the A_k line:



Thus, because we can do these two symmetries for any $i \in [n]$, then we get $2n$ symmetries. □

Now, think of a cube, which has 48 symmetries, however, only 24 of which are *orientation preserving* (symmetries not due to reflections). This is 4!, which makes sense, since we are reflecting across the inner diagonals.

4.2 Modulo Arithmetic

Theorem 4.2.1: Division with Remainder Theorem

Let $a, b \in \mathbb{Z}$, then there exists unique $q, r \in \mathbb{Z}$ such that:

$$a = qb + r \qquad 0 \leq r \leq |b|$$

Proof. :

1. Existence: Let $A = \{a - qb \in \mathbb{Z} | a - qb \geq 0\} \neq \emptyset$. By the Minimal Element Principle, since every subset of the integers contains its infemum, then let $r = \inf(A) \in A$. Thus:

   $$r = a - qb \implies a = qb + r$$

   Assume that $r \geq |b|$:

   (a) If $b > 0$, then $r - b \in A$

   (b) If $b < 0$, then $r + b \in A$

   which is a contradiction because both those terms are less than r, the minimum term of A.

2. Uniqueness: Let $a = q_1 b + r_1$ and $a = q_2 b + r_2$, (where $0 \leq r_1, r_2 \leq |b|$). Then $q_1 b + r_1 = q_2 b + r_2$, and thus $|q_1 - q_2|b = |r_2 - r_1|$. Note that this is possible if an only if $|q_1 - q_2| = 0$, which implies that $q_1 = q_2$ and $r_1 = r_2$.)

$\square$

Definition 4.2.2: Congruency Classes

If $a, b \in \mathbb{Z}$, then we say that $a \underset{n}{\equiv} b$ if $n | a - b$ if and only if there exists a $q \in \mathbb{Z}$ such that $a - b = qn$.

Remark.

We denote the class containing a by $[a]$

Example.

In $\mathbb{Z}/5n\mathbb{Z} = [[0], [1], [2], [3], [4]]$.

Chapter 5

Lecture 5- Orientation Preserving Symmetries with $\mathbb{Z}/n\mathbb{Z}$ and Complex Numbers

5.1 Orientation Preserving Symmetries

Definition 5.1.1: A cyclic group of order n

$\mathrm{Sym}^+(\mathbb{P}_n) = \{R_O^{\frac{2\pi}{n}k} | 0 < k < n-1\}$

Lemma 5.1.2

If $a \underset{n}{\equiv} b$ and $c \underset{n}{\equiv} d$, then:

1. $a + b \underset{n}{\equiv} c + d$.
2. $a - c \underset{n}{\equiv} b - d$.
3. $ac \underset{n}{\equiv} bd$.
4. $ka \underset{n}{\equiv} kb$.
5. $a^k \underset{n}{\equiv} b^k$

Proof. :
2) $(a-b) = q_1 n \qquad (b-d) = q_2 n$, and thus $(a-b)-(c-d) = (q_1 - q_2)n$, and thus $(a-b) \underset{n}{\equiv} (c-d)$.

3) $ac \cdot bd = (q_1 n + b)(q_2 n + d) - bd = n[q_1 q_2 n + bq_2 + dq_1]$. $\square$

Example.

What are the last digits of:

1. 9^{100}. Notice that $9 \underset{10}{\equiv} -1$, and thus by the lemma, $9^{100} \underset{10}{\equiv} -1^{100} = 1$.

2. 2^{300}. Notice that

$$\begin{array}{cccccccc} 2^0 & 2^1 & 2^2 & 2^3 & 2^4 & 2^5 & 2^7 & 2^8 \\ 1 & 2 & 4 & 8 & 6 & 2 & 4 & 8 \end{array}$$

and thus consider that $300 \mod 4 = 0$, and thus it is the first one in the sequence, which is 6.

Definition 5.1.3

If $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$, then:

1. $[a] + b = [a + b]$.
2. $[a] - [b] = [a - b]$.
3. $[a] \cdot [b] = [ab]$.

Definition 5.1.4: Ring

A *ring* is has the same axioms as a field, except without there is no inverse required axiom.

Example.

1. $\mathbb{Z}$.
2. $\mathbb{Z}/n\mathbb{Z}$ is a ring without inverses for non-prime n.

Define $\varphi : \mathbb{Z}/n\mathbb{Z} \to \text{Sym}^+(P_n)$ such that if $[k] \in \mathbb{Z}/n\mathbb{Z}$, then $\varphi([k]) \to R_O^{\frac{2\pi k}{n}}$

Proposition 5.1.5

φ is an isomorphism

Proof. :

1. φ is obviously surjective.
2. φ is injective because $|\mathbb{Z}/n\mathbb{Z}| = |\text{Sym}(P_n)|$.
3. φ is a homomorphism because:

$$\varphi([k_1] + [k_2]) = \varphi([k_1 + k_2]) = R_O 6[\frac{2\pi}{n}(k_1 + k_2) = R_O^{\frac{2\pi k_1}{n}} \circ R_O^{\frac{2\pi k_2}{n}}$$

□

5.2 Complex Numbers

Definition 5.2.1: Complex Numbers

The *complex numbers* are defined as $\mathbb{C} = \mathbb{R}^2\{(a, b) \in \mathbb{R}^2\}$. Multiplication and addition is defined as follows:

$$(a, b) + (c, d) = (a + c, b + d)$$

$$(a, b)(c, d) = (ac - bd, ad - bc$$

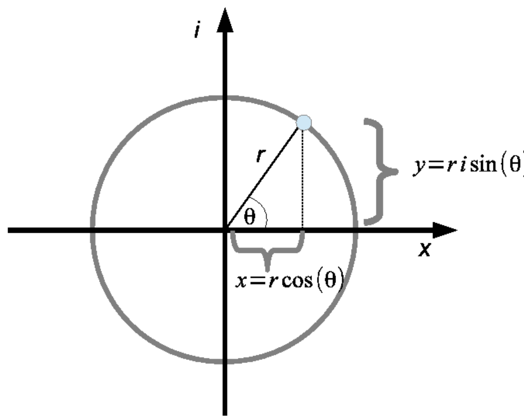


Figure 5.1: Complex Plane

Remark.

> A complex number, (a, b), is usually denoted by $z = (a, b) = a + bi$.

Remark.

> One can check to verify that $\mathbb{C}$ is indeed a field.

Theorem 5.2.2: $i^2 = 1$

We denote $i = (0, 1)$. Thus, by definition:

$$i^2 = (0, 1)(0, 1) = (-1, 0) = -1$$

Remark.

> Note that the only tricky axiom to check in the above remark is the inverse one, as division is tricky with complex numbers. However, as long as $a^2 + b^2 \neq 0$, then we can write $(a + bi)(\frac{a-bi}{a^2+b^2}) = 1$

Definition 5.2.3: —z— and $\arg(z)$

$$r = |z| = \sqrt{a^2 + b^2}$$

$$\phi = \angle = \arg(z)$$

Proposition 5.2.4

$a = |z|\cos(\varphi), b = |z|\sin(\varphi)$, and thus $z = a + bi = |z|(\cos(var\phi) + i\sin(\varphi))$.

Fact 5.2.5

1. $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$
2. $\arg(z_1 z_2) = \arg(z_1) + \arg(z_2)$.

Multiplying complex numbers scales them by multiplying their magnitudes and adds the angles.

Definition 5.2.6: Conjugate Complex Number

Given $z = a + bi \in \mathbb{C}$, we define its *conjugate*, $\overline{z}$, to be $\overline{z} = a - bi$.

Corollary 5.2.7

$\overline{z_1} + \overline{z_2} = \overline{z_1 + z_2}$
$\overline{z_1} \cdot \overline{z_2} = \overline{z_1 z_2}$

Lemma 5.2.8: Powers

$(\cos(\varphi) + i\sin(\varphi))^n = cos(n\phi) + i\sin(n\phi)$

Proof. Apply the above remark n times □

Definition 5.2.9: Exponents

We define $e^{i\varphi} = \cos(\varphi) + i\sin(\varphi)$

Remark.

> From this, we get the identity that:
>
> $$\cos(x) = \frac{e^{ix} + e^{-ix}}{2} \qquad \cos(x) = \frac{e^{ix} - e^{-ix}}{2i}$$

Lemma 5.2.10: Euler's Identity

$e^{i\pi} = -1$

5.3 A Complex Isometry

Theorem 5.3.1: All complex isometries

Let $f : \mathbb{C} \to \mathbb{C}$ be a function. $f(z) = mz + b$ is an isometry if an only if $|m = 1|$.

Proof. Let $f(z) = w$. This is only possible if and only if $z = \frac{w-b}{m}$. Note that because an explicit inverse formula was given, then f is a bijection. Moreover,

$$|f(z_1) - f(z_2)| = |mz_1 + b - mz_2 - b| = |m(z_1 - z_2)| = |z_1 - z_2|.$$

□

Theorem 5.3.2: All $\mathbb{R}^2$ isometries

Any isometry $f : \mathbb{R}^2 \to \mathbb{R}^2$ is either $z = mz + b$ or $z = m\overline{z} + b$ for $|m| = 1$.

Example.

1. $z \to z + b$ (T_b).
2. $z \to -z$ (S_O).
3. $z \to mz$ (R_O^ϕ).
4. $z \to \overline{z}$ $(\mathbb{S}_\mathbb{R})$.

Chapter 6

Lecture 6- Roots of Unity and Classifications of Isometries

6.1 Roots of Unity

Theorem 6.1.1: Fundamental Theorem of Algebra

If $P(x)$ is a polynomial ($P(x) \in \mathbb{P}[x]$), then it has a complex root

Example.

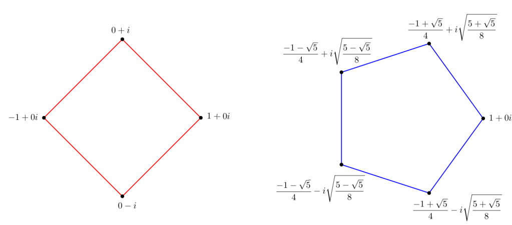
Consider $x^n - a = 0$. Let

$$a = r(\cos(\varphi) + i\sin(\varphi)) \qquad x = R((\cos(\Theta) + i\sin(\Theta))$$

It is evident that $R = \sqrt{n}$ and $\Theta = \frac{\varphi}{n} + 2\pi\frac{k}{n}$, for $0 \le k \le n-1$.

Example.

With the same example as above, consider $a = 1$. Then if $\varepsilon_k = \cos(\frac{2\pi k}{n}) + i\sin(\frac{2\pi k}{n}) = e^{\frac{2\pi i k}{n}}$, then $\mu_0 = \{\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}\}$ are the verticices of $n-$regular polygons



The 4^{th} roots of unity **The 5^{th} roots of unity**

Figure 6.1: Roots of Unity

Example.

> If $n = 3$, then $x^3 - 1 = 0$, and so $(x-1)(x^2+x+1) = 0$, and thus $x = \{1, \frac{-1\pm\sqrt{3}}{2}\}$

Theorem 6.1.2

$\mathbb{Z}/n\mathbb{Z}$ is isomorphic to μ_n.

Proof. Let $\varphi : [k] \to \varepsilon_k$.

1. $$\varepsilon_k \varepsilon_\ell = (\cos(\frac{2\pi k}{n}) + i\sin(\frac{2\pi k}{n}))(\cos(\frac{2\pi \ell}{n}) + i\sin(\frac{2\pi \ell}{n})) = \cos(\frac{2\pi(k+\ell)}{n}) + i\sin(\frac{2\pi(k+\ell)}{n}) = \varepsilon_{k+\ell}$$

2. This is obviously bijective since $|\mu_0| = |\mathbb{Z}/n\mathbb{Z}|$.

$\square$

Theorem 6.1.3: Classifications of Isometries

Every isometry $f : \mathbb{C} \to \mathbb{C}$ is one of the following:

1. $z \to mz + b$ (orientation-preserving).
2. $z \to m\overline{z} + b$ (orientation-reversing).

Proof. Let f be an isometry and consider $f(0)$, $f(1)$, and $f(i)$. Define $f_1(z) = f(z) - f(0)$, and notice that

$$\begin{aligned} &f_1(0) = 0 \\ &f_1(1) = 1 \implies |1-0| = |f_1(1) - f_1(0)| = |f_1(1)| = 1 \end{aligned}$$

Define:
$$f_2(z) = \frac{f(z) - f(0)}{f(1) - f(0)} \implies f(0) = 0, \quad f(1) = 1$$

Thus, there are two cases:

1. If $z = \frac{f(z)-f(0)}{f(1)-f(0)}$, then $f(z) = (f(1) - f(0))z + f(0)$.
2. If $\overline{z} = \frac{f(z)-f(0)}{f(1)-f(0)}$, then $f(z) = (f(1) - f(0))\overline{z} + f(0)$.

$\square$

Theorem 6.1.4: Classification of Orientation Preserving Isometries

$\mathrm{Isom}(\mathbb{R}^2)$ is a subgroup, and every element in Isom^+ is either:

1. An identity.
2. A translation.
3. A rotation.

Proof. 1. Consider that if $f_1, f_2 \in \mathrm{Isom}^+(\mathbb{R}^2)$, then $f_1 \circ f_2 = m((m)z + b') + b' = mm'z + (m'b + b')$, $f_I = f(z) = mz$, $m = 1$.

2. $f(z) = z + b$ is a translation.
3. $f(z) = mz + b$ is a rotation, with a fixed point at $z_0 = \frac{b}{1-m}$

□

Theorem 6.1.5: Chasle's Theorem

Every isometry $f : \mathbb{R}^2 \to \mathbb{R}^2$ is one of the following:

1. Identity
2. Rotation
3. $T_{\mathbf{v}}$
4. $\mathbb{S}_\ell$
5. $\mathbb{S}_\ell T_{\mathbf{v}}$

Corollary 6.1.6

$$R_{O_1}^{\varphi_1} \circ R_{O_2}^{\varphi_2} = \begin{cases} R_{O_3}^{\varphi_1+\varphi_3} & \varphi_1 + \varphi_2 \neq 2\pi k \\ T_{\mathbf{v}} & \varphi_1 + \varphi_2 = 2\pi k \end{cases}$$

Proof. Consider the following functions:

$$z \to e^{i\varphi_1} z + b_1 \qquad z \to e^{i\varphi_2} z + b_2$$

and thus by multiplying, $e^{i(\varphi_1+\varphi_2)z+(b_1 e^{i\varphi_2}+b_2)}$. □

Theorem 6.1.7: Napoleon's Theorem

Given a $\triangle ABC$ and creating equilateral triangles on each edge and having the center points be O_A, O_B, O_C, then $\triangle O_A O_B O_C$ is a regular triangle.

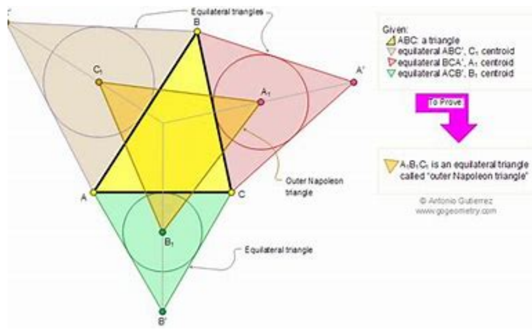


Figure 6.2: Napoleon's Theorem

s

Definition 6.1.8: Similarities

A function $f : \mathbb{R}^2 \to \mathbb{R}^2$ is a *similarity* if there exists a $k \in \mathbb{R}$ such that for all $A, B \in \mathbb{R}^2$,

$$|f(A)f(B)| = k|AB|$$

Example.

> Given $H_O^\lambda : \mathbb{R}^2 \to \mathbb{R}^2$, with $\lambda \neq 0$ such that $H_O^\lambda(X) = Y$ with $\lambda\overrightarrow{OX} = \overrightarrow{OY}$

Chapter 7

Lecture 7- Fundamental Theorem of Arithmetic and Euler's Function for $\mathbb{Z}/n\mathbb{Z}$.

7.1 Prime Numbers and FTA.

Recall the integer remained theorem:

Fact 7.1.1

For all $a, b \in \mathbb{Z}$, with $b \neq 0$, there exists unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r \leq |b|$.

Remark.

> We say that $b|a$ if and only if there exists a $q \in \mathbb{Z}$ such that $a = bq$. Moreover, we say that $a_1 \underset{n}{\equiv} a_2$ if and only if $n|(a_1 - a_2)$

Definition 7.1.2: Greatest Common Divisor

The *greatest common divisor*, or *gcd*, between $a, b \in \mathbb{Z}$, is $\gcd(a, b) = (a, b) = \max\{d \in \mathbb{N} | d|a, d|b\}$

Proposition 7.1.3

1. $(a, b) = (a - b, b)$.
2. $(a, b) = (b, a)$.
3. $(3, 0) = 3$.

Theorem 7.1.4: Euclid's Algorithm

1. If $b = 0$, then $(a, b) = a$.
2. Use fact 7.1.1 to write $(a, b) = (q_1 b + r_1, b) = (r_1, b) = (b, r_1)$. If $r_1 = 0$, then $(a, b) = b$.
3. Use fact 7.1.1 to write $(b, r_1) = (q_2 r_1 + r_2, r_1)$, and keep going until $r_n = 0$, and thus $(a, b) = r_{n-1}$. Note that this process terminates eventually because integers eventually decrease down to 0.

Corollary 7.1.5

Suppose $a, b \in \mathbb{Z}$ with $(a, b) = d$, then there exists $u, v \in \mathbb{Z}$ such that $d = ua + vb$.

Proof. This comes from the fact that in Euclid's Algorithm, $d = \langle r_{n-1}, r_n \rangle$, and so on and on. $\square$

Example.

(31,22)

$$\begin{aligned}(31, 22) &= (9, 22)\\ &= (9, 4)\\ &= (1, 4)\end{aligned}$$

And thus $(31, 22) = 1$. Moreover, we can write 1 as

$$1 = 9 - (2 \cdot 4) = (9 - 2 \cdot (22 - 9 \cdot 2)) = 5 \cdot 9 - 2 \cdot 22 = 5(31 - 22) - 2(22) = 5(31) - 7(22)$$

Definition 7.1.6: Coprime

We say that $a, b \in \mathbb{Z}$ are *coprime*if $(a, b) = 1$.

Remark.

By the above corollary, $a, b \in \mathbb{Z}$ are coprime if and only if there exist $u, v \in \mathbb{Z}$ such that $1 = ua + vb$.

Definition 7.1.7: Prime

We say that $p \in \mathbb{N}$ is prime if an only if p has exactly two divisors, namely, 1 and p.

Theorem 7.1.8

Every $n \in \mathbb{Z}$ is a product of primes

Proof. induct □

Proposition 7.1.9

There exists an infinite amount of prime numbers

Proof. Assume there exists N primes. Therefore, consider $a = p_1 p_2 \cdots p_N + 1$. By the above theorem, there exists some p_i prime such that $p_i | a$. However, this is a contradiction, as any prime dividing a would result with remainder 1. □

Theorem 7.1.10

For any $a \in \mathbb{Z}$, either $p|a$ or $(p, a) = 1$.

Theorem 7.1.11

The following statements hold:

1. If $ma \underset{n}{\equiv} mb$ and $(m, n) = 1$, then $a \underset{n}{\equiv} b$.
2. If $n|(ma)$ and $(m, n) = 1$, then $n|a$.
3. If $p|(ab)$, then $p|a$ or $p|b$.

Proof.

1. Because $ma \underset{n}{\equiv} mb$ implies that $n|(a-b)m$, then by (2), we have that $n|(a-b)$, and thus $a \underset{n}{\equiv} b$
2. Because $(m, n) = 1$, then

$$1 = um + vn \qquad \Longrightarrow \qquad a = uma + vna$$

   Because the RHS is divisible by n $(n|(ma))$, then $n|a$.
3. If $p|a$, we are done. If not, assume $p \not| b$, then we have, by Theorem 7.1.10, that $p|a$, which is a contradiction.

□

Theorem 7.1.12: Fundamental Theorem of Arithmetic

If $a \in \mathbb{Z}$ and $a \neq 0$, then we can write $a = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}$ in 1 distinct way (up to the ordering of the factors)

Proof.

1. Already proven in Theorem 7.1.8.
2. Assume

$$a = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k} = s_1^{n_1} \cdot s_2^{n_2} \cdots s_k^{n_k}.$$

   If $q_s \notin \{p_1, \dots, p_k\}$, then q_s is coprime with all p. Because $q_s | p_1 \cdots p_k$, then by Theorem 7.1.11.3, we are done.

□

7.2 $\mathbb{Z}/n\mathbb{Z}$ Rings

Recall that $\mathbb{Z}/n\mathbb{Z}$ is a ring.
Define $R^* = \{x \in R | \exists y \in R; xy = 1\}$. Note that R^* is therefore an Abelian Group.

Remark.

> Note that R is a field if and only if for all $x \in R$ such that $x \neq 0$, we have that $x \in R^*$.

Theorem 7.2.1: When is $[a]$ Invertible?

$[a] \in (\mathbb{Z}/n\mathbb{Z})^*$ if and only if $(an) = 1$, that is, a, n coprime.

Proof. Consider that $[a]$is invertible if and only if there exists a $[b] \in \mathbb{Z}/n\mathbb{Z}$ such that $[a][b] = 1$, which exists if and only if there exists a b such that $n|((a-b)-1)$, which exists if an only if there exists $b, q \in \mathbb{Z}$ such that $(a-b)-1 = qn$, and thus $1 = ab - qn$. $\square$

Example.

> What is $[22]^{-1}$ in $\mathbb{Z}/31\mathbb{Z}$? Consider that $1 = 5(31) - 7(22)$, and thus $[1] = [5][31] - [7][22] = [-7][22]$, and so $[22]^{-1} = [-7] = [24]$.

Corollary 7.2.2

1. $|\mathbb{Z}/n\mathbb{Z}| = \varpi(n)$ (Euler's function). Note that $|\mathbb{Z}/p\mathbb{Z}| = p - 1$ where p is prime.
2. $\mathbb{Z}/p\mathbb{Z}$ is a field.

Theorem 7.2.3: Euler's Theorem

Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ such that $(a, n) = 1$, then $a^{\varphi(n)} \underset{n}{\equiv} 1$.

Proof. Suppose $(\mathbb{Z}/n\mathbb{Z}) = \{[a_1], [a_2], \ldots, [a_{\varphi(n)}]\}$.
Let $A = \{[a][a_1], [a][a_2], \ldots, [a][a_{\varphi(n)}]\}$. I claim that these are the same set, up to the order of the elements. This holds because (1) the first question on PSET 3 and (2) because for any $i \neq j \in [\varphi(n)]$, we have that $[a][a_i] = [a][a_j]$, then $[a_i] = [a_j]$. Therefore:

$$[a_1], [a_2], \ldots, [a_{\varphi(n)}] = [a][a_1], [a][a_2], \ldots, [a][a_{\varphi(n)}]$$

, and thus

$$[1] = [a]^{\varphi(n)}$$

$\square$

Theorem 7.2.4: Fermat's Last Theorem

If p is a prime and $(a, p) = 1$, then $a^{p-1}\underset{p}{n}1$

Corollary 7.2.5

(Wilson's Theorem) Let p be a prime and $p \geq 3$, then $(p-1)! \underset{n}{-1}$.

Proof. Consider that

$$[(p-1)!] = [p-1][p-2]\cdots[2][1] = [1][p-1]\prod_{1<x<p-1}[x][x]^{-1} = -1 \cdot 1$$

Consider that $[x] = [x]^{-1}$ when $[x^2] = 1$ when $p|x^2 - 1$, and thus $p|x - 1$ or $p|x + 1$, and thus either $[x] = [1]$ or $[x] = -1$. Therefore, the last equality holds. $\square$

Chapter 8

Lecture 8- Fields and Polynomials, Inversions

8.1 Fields and Polynomials

Example.

Examples of Fields:

1. $\mathbb{C}, \mathbb{R}, \mathbb{Q}$;
2. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$, where inverses are defined by multiplying by conjugates: $\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2}$.
3. $\mathbb{F}_2$.

Definition 8.1.1: Characteristics of Fields

1. We say a field, F, has *characteristic zero* if

$$\underbrace{1+1+\cdots+1}_{n \text{ times}} \neq 0, \qquad \forall n \in \mathbb{N}$$

Remark.

With such a field we can build an injective map $\mathbb{Q} \to F$ by sending

$$\frac{n}{m} \to \underbrace{(1+1+\cdots+1)^{-1}}_{m \text{ times}} \underbrace{(1+1+\cdots+1)}_{n \text{ times}}$$

Therefore, we get a notion of *Inclusion of Fields*, which implies that a 'copy' of $\mathbb{Q}$ is found in every field of characteristic zero.

2. We say a field, F, has *characteristic* p, if there exists some $N \in \mathbb{N}$ such that

$$\underbrace{1+1+\cdots+1}_{n \text{ times}} = 0.$$

Remark.

We know the smallest such n must be prime, as otherwise, either factor of n would be the one contributing the zero, which is a contradiction, since if its a factor, then its smaller than n. Thus, we can build an injective map $\mathbb{Z}/p\mathbb{Z} \to F$ by sending

$$[k] \to \underbrace{1+1+\cdots+1}_{k \text{ times}},$$

and thus we get the notion that $\mathbb{F}_p \subset F$.

Theorem 8.1.2

Suppose F is a finite field, then $|F|^p = p^n$ for some $n \in \mathbb{N}$.

Proof. F cannot have characteristic 0, as it is finite, and thus $\mathrm{char}(F) = p$ for some p prime. Notice then that F is a vector space of $\mathbb{F}_p$, and we know also that because $\dim(F) < \infty$, then $\dim(F) = n$ for some $n \in \mathbb{N}$. Therefore, we know that $F \cong F_p^n$, and thus $|F| = |F_p^n| = p^n$. $\square$

Definition 8.1.3: Polynomial

A *polynomial* with coefficients in F is a sequence $(a_0, a_1, \dots)$ with each $a_i \in F$ such that there exists some $N \in \mathbb{N}$ with all $n \geq N$ yielding $a_n = 0$. Addition and multiplication are defined as follows:

$$+ : ((a_0, a_1, \dots) + (b_0, b_1, \dots) = (a_0 + b_0, a_1 + b_1, \dots)$$

$$\times : (a_0, a_1, \dots) \times (b_0, b_1, \dots) = (a_0 b_0, a_0 b_1 + a_1 b_0, \dots)$$

Fact 8.1.4

A polynomial is a ring

Proof. While tedious, it is useful to note that the identity element is

$$1 = (1, 0, 0, \dots),$$

and to arrive at a usual notion of a polynomial, simply use the fact that:

$$x = (0, 1, 0 \dots)$$

and thus

$$x^n = (\underbrace{0, 0, \dots, 1}_{n+1 \text{ times}}, 0, \dots)$$

$\square$

8.2 Inversions

Definition 8.2.1: Inversion

Let S be a circle of radius R and with a center at O. Then we define as inversion to be the map $I_S : \mathbb{R}^2 \setminus \{O\} \to \mathbb{R}^2 \setminus \{O\}$ such that $I_S(X) = Y$ if:

1. $Y \in$ line connecting O, X.
2. $|OX||OY| = R^2$.

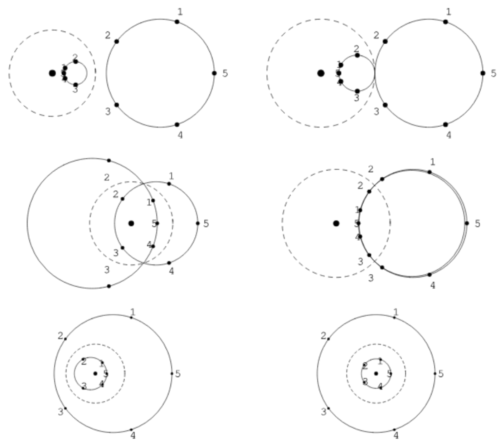


Figure 8.1: Inversion

Proposition 8.2.2

1. Points on S are fixed;
2. Points inside of S are mapped outside, and vice-versa;
3. $I_S^2 = \text{Id}$;
4. If $A, B \in \mathbb{R}^2$, then
$$\frac{|OA}{OI(B)} = \frac{|OB|}{|OI(A)|}$$
i.e, Figure 8.2 below;
5. Lines containing O are unchanged under inversions;
6. Lines not containing O are sent to circles with A, B, O on the circle;
7. Circles not containing O are sent to circles containing O.

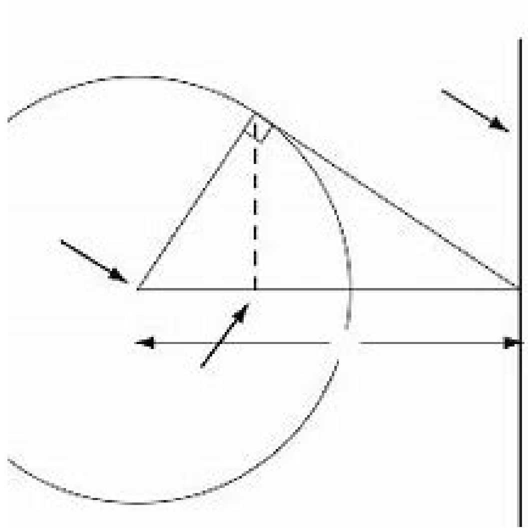


Figure 8.2: Triangle Inversion

Definition 8.2.3: Riemann Sphere

A *Riemann sphere*, or a *projective line over* $\mathbb{C}$, *is* $\mathbb{C} \cup \{\infty\} = \tilde{\mathbb{C}} = \mathbb{P}'_{\mathbb{C}}$.

Remark.

A line in $\mathbb{R}^2$ is mapped to a line $\cup\{\infty\}$, and

$$I_S(\infty) = 0, \qquad I_S(0) = \infty.$$

Chapter 9

Lecture 9- Roots of Polynomials, Lagrange Interpolation, and Mobius Groups

9.1 Roots of Polynomials

Theorem 9.1.1: Polynomial Division with Remainder Theorem

If $A(x), B(x) \in F[x]$, and $Q(x) \neq 0$, then there exists unique polynomials $R(x), Q(x)$ such that $A(x) = Q(x)B(x) + R(x)$ and $0 < \deg(R(x)) < \deg(B(x))$.

Proof. The proof follows exactly the same as Theorem 4.2.1, but just with polynomials and degrees. □

Definition 9.1.2: Roots

Given that $P(x) \in F[x]$ and $x_0 \in F$, we say that x_0 is a *root* of $P(x)$ if $P(x_0) = 0$.

Definition 9.1.3: Polynomial Divisions

Suppose $A(x), B(x) \in P(x)$, then we say that $A(x)|B(x)$ if and only if there exists a $Q(x) \in F[x]$ such that $B(x) = A(x)B(x)$.

Lemma 9.1.4

Suppose that $P(x) \in F[x]$, then $x_0 \in F$ is a root of $P(x)$ if and only if $(x - x_0)|P(x)$.

Proof.

- ($\implies$:) Divide $P(x)$ by $(x - x_0)$ with remainder. Then $P(x) = Q(x)(x -$

$x_0) + R(x)$, and thus $P(x_0) = 0 = Q(x_0)(x_0 - x_0) + R(x)$, and thus $R(x) = 0$, meaning that there is no remainder, and thus $(x - x_0)|P(x)$.

- ($\Longleftarrow$:) If $(x - x_0)|P(x)$, then $P(x) = (x - x_0)Q(x)$, and thus, $P(x_0) = 0$.

□

Corollary 9.1.5

:

1. Suppose $P(x) \in F[x]$ and $\deg(P(x)) = n$, then $P(x)$ has at most n roots.
2. If $P(x) \in F[x]$ has roots $x_1, \ldots, x_n$ and is of degree n, then we can write:

$$P(x) = (x - x_1)P_1(x) = (x - x_0)(x - x_2)P_2(x) = \cdots = a_n(x - x_1)\cdots(x - x_n)$$

3. If $P(x) = a_n(x - x_1)\cdots(x - x_n)$, then

$$\frac{-a_{n-1}}{a_n} = x_1 + \cdots + x_n, \frac{\pm a_{n-k}}{a_n} = \sum_{1<<k} x_1 \cdots x_k, \qquad (-1)^n \frac{a_1}{a_n} = x_1 \cdots x_n$$

4. Let $P(x), Q(x) \in F[x]$ and $\deg(P, Q) \leq n$ and let there exist $(n+1)$ distinct $x_1, \ldots, x_{n+1} \in F$ such that $P(x_i) = Q(x_j)$, then $P = Q$.

Proof. Proofs mostly use previous lemma. □

Theorem 9.1.6

Let F be an infinite field. If for all $a \in F$, $P(a) = Q(a)$, then $P = Q$.

Proof. Let P, Q, have degree n, then because there exists more than $n + 1$ such $a \in F$ (since it is infinite), by the last part of the corollary, we are done. □

9.2 Lagrange Interpolation

Theorem 9.2.1: Lagrange Interpolation Theorem

Let $x_0, x_1, \ldots, x_n$ and $y_0, y_1, \ldots, y_n$ be elements of F. Then There exists a unique $P(x) \leq F[x]$ such that $P(x_1) = y_1, \ldots, P(x_n) = y_n$ of $\deg(P) < n - 1$

Remark.

> Intuitively, this says that if we have n points, say 3, we can create a unique polynomial of degree $n - 1$, say a quadratic, that passes through all those points

Proof. Uniqueness by Corollary. Consider

$$P(x) = y_1 \frac{(x-x_2)(x-x_3)\cdots(x-x_n)}{(x_1-x_2)(x_1-x_3)\cdots(x_1-x_n)} + y_2 \frac{(x-x_1)(x-x_3)\cdots(x-x_n)}{(x_2-x_1)(x_2-x_3)\cdots(x_2-x_n)} + \cdots + y_n \frac{(x-x_1)(x-x_2)\cdots(x-x_n}{(x_n-x_1)(x_n-x_2)\cdots(x_n-}$$

□

Example.

Fermat's Little Theorem:

1. $$\mathbb{F}_3 : \qquad x^2 - [1] = (x-[1])(x-[2])$$

2. $$\mathbb{F}_5 : \qquad x^4 - [1] = (x-[1])(x-[2])(x-[3])(x-[4])$$

3. $$\mathbb{F}_p : \qquad x^{p-1} - [1] = (x-[1])(x-[2])\cdots(x-[p-1])$$

9.3 Mobius Groups and Fractional Linear functions

Definition 9.3.1: Mobius Group

Consider the group of bijections $\mathbb{P}'_{\mathbb{C}} \to \mathbb{P}'_{\mathbb{C}}$, then we define a *Mobius Group* to be the subgroup generated by $\mathrm{Sym}(\mathbb{R}^2)$ and inversions.

Definition 9.3.2: Fractional Linear Functions

A *fractional linear function* is a map $f : \mathbb{P}'_{\mathbb{C}} \to \mathbb{P}'_{\mathbb{C}}$ such that $f(z) = \frac{az+b}{cz+d}$ given that $ad - bc \neq 0$ and

1. If $c = 0$, then we have that $z \to \frac{az}{d} + \frac{b}{d}$ and $\infty \to \infty$.
2. If $c \neq 0$, then we have that $f(\frac{-d}{c}) = \infty$ and $f(\infty) = \frac{a}{c}$.

Theorem 9.3.3

Fractional linear functions form a group (denoted by $PGL_Q(\mathbb{C})$.)

Chapter 10

Lagrange's Theorem and The Gauss Theorem for Cyclic Groups

10.1 Lagrange's Theorem

Theorem 10.1.1: Lagrange's Theorem

Let G be a finite group and let $a \in G$, then $a^{|G|} = e$.

Corollary 10.1.2

Fermat's Little Theorem: Consider any $a \in (\mathbb{Z}/p\mathbb{Z})^*$, then $[a]^{p-1} = [1]$ if and only if $p|a^{p-1}$

Proof. Let $a \in G$, and let $G = \{g_1, g_2, \ldots, g_n\}$. Consider a graph where $g_i \to g_j$ if there is an edge whenever $g_i = ag_j$. Note that for every vertex, there exists a unique outgoing and incoming edge. Therefore, the group creates various loops. For example, $g_1, ag_1, a^2g_1, \ldots, a^{k-1}g_1$ is a loop where each element is distinct and $a^k g_1 = g_1$. Define

$$k := \{S_{\geq 1} : a^S = e\} =: \mathrm{ord}(a)$$

, then $|G| = k(\#\text{cycles})$, and thus $a^k = a^{|G|} = e$ for any $a \in G$. $\square$

Corollary 10.1.3

Let $a \in G$ and G be finite, then $\mathrm{ord}(a)||G|$.

Corollary 10.1.4

If $|G| = p$, then $G \cong (\mathbb{Z}/p\mathbb{Z}, +)$

Proof. The map sends $[k] \to a^k$. □

10.2 Cyclic Groups and Gauss' Theorem

Definition 10.2.1: Cyclic Groups

A group G is cyclic if it is generated by 1 element, i.e, there exists an $a \in G$ such that for all $g \in G$, g is a power of a.

Proposition 10.2.2

If G is cyclic, then either $G \cong (\mathbb{Z}, +)$ or $G \cong (\mathbb{Z}/n\mathbb{Z}, +)$

Theorem 10.2.3: Gauss' Theorem

If $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic, then it is isomorphic to $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$.

Lemma 10.2.4

Consider the cyclic group of order n, $\mathbb{Z}/n\mathbb{Z}$. Then there exists $\varphi(d)$ number of elements with order d.

Proof. This proof is mostly done by exploring examples, but an important corollary is

$$n = \sum_{d|n} \varphi(d)$$

□

Proof. Proof for Gauss consists of showing that $\Psi(p-1) \neq 0$, where Ψ is the number of elements of order d in $\mathbb{F}_p^*$. □

Definition 10.2.5: Action

An *action* of a group G on a set X is a map

$$G \times X \to X$$

such that $(g, x) \to gx$. that satisfies $g_1(g_2x) = (g_1g_2)x$ and $(e, x) = x$.

Remark.

> Every element in G defines a bijection $X \to X$ by $x \to gx$.

Chapter 11

Lecture 11- Quadratic Residuals and Projective Geometry

11.1 Quadratic Residuals

Definition 11.1.1: Quadratic Residue

We say that $[a] \in \mathbb{F}_p$ is *quadratic residue* if there exists an x such that $a\underset{\equiv}{p}x^2$.

Example.

1. If $p = 5$, then QR: $[1]\underset{\equiv}{5}[1]$, $[4]\underset{\equiv}{5}[2]$.
2. If $p = 7$, then QR: $[1]\underset{\equiv}{7}[1]$, $[2]\underset{\equiv}{7}[4]$, $[4]\underset{\equiv}{7}[2]$.

Definition 11.1.2: Legendre Symbol

Chapter 12

Lecture 12

Definition 12.0.1: Determinants

The *determinant* of a matrix, $\det(A)$, where $A \in M_{n\times n}$ is defined as follows,

$$\det(A) = \sum_{\sigma \in S_n} \text{sign}(\sigma) a_{1,\sigma(1)} a_{2,\sigma(2)}, \ldots, a_{n,\sigma(n)}$$

Example.

> Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, then $\det(A) = ad - bc$

Example.

> Let $A = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$, then $\det(A) = aei + bfg - ceg + cdh - bdi - afh$

Proposition 12.0.2

Let $A, B \in M_{n\times n}$, then $\det(AB) = \det(A \det(B)$.

Definition 12.0.3: Alternating Polynomials

We say that a polynomial in $n-$variables, $P(x_1, \ldots, x_n)$ is *alternating* if for any permutation, $\sigma \in \mathbb{S}_n$,

$$P(x_1, \ldots, x_n) = \text{sgn}(\sigma) P(x_{\sigma(1)}, \ldots, x_{\sigma})$$

Example.

For $n = 2$, consider $P(x_1, x_2) = x_1 - x_2$.

Definition 12.0.4: Alternation of a Polynomial

Let $P(x_1, \ldots, x_n)$ be a polynomial, then we define

$$\mathrm{Alt}(P) = \sum_{\sigma \in \mathbb{S}_n} \mathrm{sgn}(\sigma) P(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

Example.

Consider $P(x_1, x_2, x_3) = x_1$, then

$$\mathrm{Alt}(x_1) = x_1 - x_2 - x_3 - x_1 + x_2 + x_3 = 0$$

Example.

Consider $P(x_1, x_2) = x_1 x_2$, then

$$\mathrm{Alt} = x_1x_2 - x_1x_2 - x_3x_2 - x_1x_3 + x_2x_3 + x_1x_3 = 0$$

Example.

Consider $P(x_1, x_2) = x_1 - x_2$, then

$$\mathrm{Alt}(x_1 - x_2) = (x_1 - x_2) - (x_2 - x_1) - (x_3 - x_2) + \cdots = x_1 - x_2 - x_2 + x_1 - x_3 + x_2 - x_1 + x_3 + x_2 - x_3 + x_3 - x_1 =$$

Fact 12.0.5

$\mathrm{Alt}(P(x_1, \ldots, x_n))$ is always an alternating polynomial

Remark.

Suppose $\alpha_1 > \alpha_2 \cdots > \alpha_n$ is a decreasing sequence of natural numbers, then consider

$$x_1^{\alpha_1}, \ldots, x_2^{\alpha_n},$$

then define

$$A_\alpha := \mathrm{Alt}(x_1^{\alpha_1}, \ldots, x_2^{\alpha_n}) = \det \left(\begin{bmatrix} x_1^{\alpha_1} & x_2^{\alpha_1} & \ldots & x_n^{\alpha_1} \\ x_1^{\alpha_2} & x_2^{\alpha_2} & \ldots & x_n^{\alpha_2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{\alpha_n} & x_2^{\alpha_n} & \ldots & x_n^{\alpha_n} \end{bmatrix} \right).$$

Let

$$\delta := (n-1, n-2, \ldots, 1, 0),$$

then

$$A_\delta = \det \left(\begin{bmatrix} x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1} \\ x_1^{n-2} & x_2^{n-2} & \ldots & x_n^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & \ldots & x_n \\ 1 & 1 & 1 & 1 \end{bmatrix} \right) = \prod_{i<j} (x_i - x_j)$$

This is famously known as the *Vandermonde determinant.*

Definition 12.0.6: Schur Polynomial

Let $\lambda = \{\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_{n-1} \geq \lambda_n\}$, where $\lambda_i = \alpha_i - (n-i)$, and α is defined as above be a partition of some natural number. Then we define the *Schur polynomial* to be

$$S_\lambda = \frac{A_{\lambda+\delta}}{A_\delta}$$

Theorem 12.0.7

Schur polynomials are symmetric