Inverse Problems in Algebra and Topology
International Spring School in Mathematics
University of Sharjah

Sam Smith
Saint Joseph's University
Philadelphia

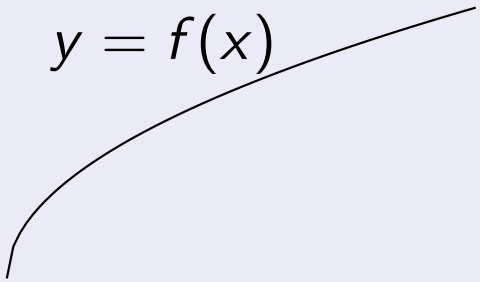
March 2019

What is an inverse problem?

Mathematical Construction

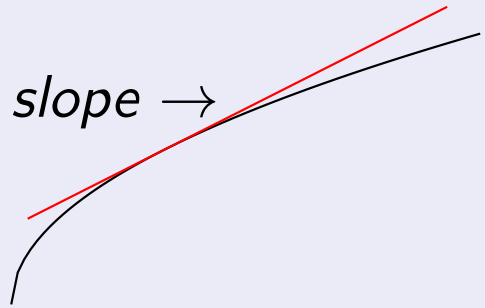
function

$y = f(x)$



derivative

$f'(x) = slope \rightarrow$



Inverse Problem for Derivatives

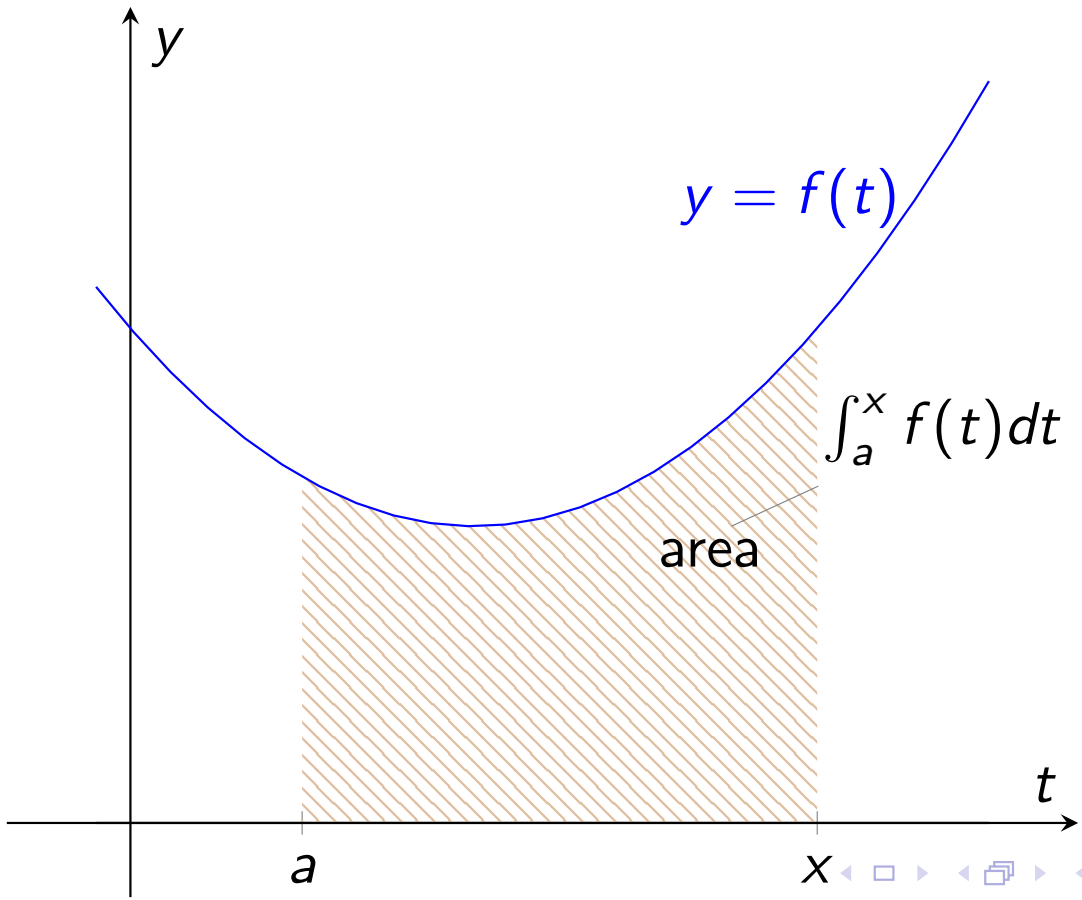
Is every continuous function the derivative of some function?

Answer

Yes!

Theorem (Fundamental Theorem of Calculus I)

Let $f(x)$ be continuous. Let $F(x) = \int_a^x f(t)dt$. Then $F'(x) = f(x)$.



Refining the Inverse Problem

Definition (Elementary Antiderivatives)

A function $f(x)$ has an **elementary antiderivative** $F(x)$ if $F'(x) = f(x)$ and $F(x)$ can be expressed in terms of exponentials, logarithms, trigonometric functions, and trigonometric inverse functions.

Refined Inverse Problem

Which functions have elementary antiderivatives?

Elementary Antiderivatives

Examples (Integral Calculus)

function	antiderivative	method
$4\sin(3x)$	$-4/3\cos(3x)$	u-substitution
$x\ln(x)$	$x\ln(x) - x$	parts
$\frac{x^2}{\sqrt{1-x^2}}$	$\frac{1}{2}\left(\sin^{-1}(x) - x\sqrt{1-x^2}\right)$	trig substitution
$\frac{2x+5}{x^2+4x+5}$	$\ln(x^2+4x+5) + \tan^{-1}(x+2)$	partial fractions
$\frac{xe^{2x}}{(2x+1)^2}$	$\frac{e^{2x}}{8x+4}$	parts

Integration in Finite Terms

1835

Joseph Liouville gives a characterization of functions with elementary antiderivatives. The result is phrased in terms of extensions of differential algebras. The Liouville Principle implies that only certain sums of logarithms of simple functions will have elementary antiderivatives.

Theorem (Liouville)

The function e^{-x^2} does not have an elementary antiderivative.

1969

Robert Henry Risch solves the decision problem for elementary antiderivatives. The Risch algorithm decides whether a given function has an elementary antiderivative and computes the antiderivative when it exists.

Comparison of Functions

Examples

Elementary Antiderivative	No Elementary Antiderivative
$\sin(3x)$	$\sin(x^3)$
e^{-x}	e^{-x^2}
xe^x	$\frac{e^x}{x}$
$\frac{\ln(x)}{x}$	$\frac{x}{\ln(x)}$
$\frac{xe^{2x}}{(2x+1)^2}$	$\frac{xe^x}{(2x+1)^2}$

Group Theory

Definition

A *group* is a set G with an operation $a \cdot b$ satisfying

(i) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associativity)

(ii) there is $e \in G$ with $e \cdot a = a \cdot e$ for all $a \in G$ (identity)

(iii) for each $a \in G$ there is $a^{-1} \in G$ with $a \cdot a^{-1} = a^{-1} \cdot a = e$ (inverses)

Examples (Finite Groups)

cyclic groups:

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}, + \mod n.$$

finite abelian groups:

$$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k} = \{(a_1, \ldots, a_k) \mid a_i \in \mathbb{Z}_{n_i}\}.$$

multiplicative group of integers mod n:

$$U(n) = \{k \in \mathbb{Z}_n \mid (k, n) = 1\}$$

Examples (Finite Groups continued)

semi-direct product:

$$\mathbb{Z}_n \rtimes U(n) = \{(m,k) \mid \in \mathbb{Z}_n, k \in U(n)\}$$

$$\text{multiplication:} (m_1,k_1)\cdot(m_2,k_2) = (m_1 + k_1 m_2, k_1 k_2).$$

symmetric group:

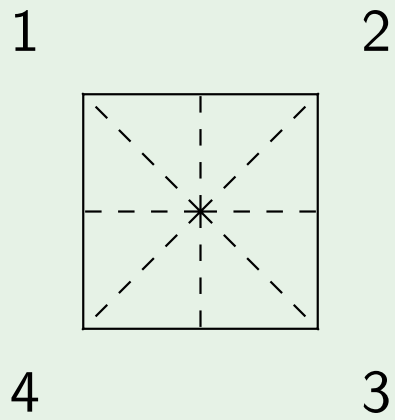
$$S_n = \text{ permutations of } \{1,2,\ldots,n\}$$

$$\text{elements: } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 8 & 5 & 4 & 3 & 6 & 7 \end{pmatrix} = (12)(3876)(45)$$

$$\text{multiplication: } (12)(3876)(45)\cdot(143)(28)(567) = (1532748)$$

Examples (Finite Groups continued)

D_4 = symmetries of the square



$$D_4 = \{e, (1234), (13)(24), (1432), (14)(23), (12)(34), (24), (13)\}$$
$$= \langle a, b \mid a^4 = b^2 = e, bab = a^{-1} \rangle, \quad a = (1234), b = (13)$$

dihedral group: D_n = symmetries of the regular n-gon

$$D_n = \langle a, b \mid a^n = b^2 = e, bab = a^{-1} \rangle$$

Automorphism Groups

Definition

Given a group G define $\mathrm{Aut}(G)$ to be the set of all automorphisms of G with multiplication given by composition of functions.

$\mathrm{Aut}(\mathbb{Z}_n) \cong U(n)$

An automorphism $\psi\colon \mathbb{Z}_n \to \mathbb{Z}_n$ is determined by $\psi(1) \in \mathbb{Z}_n$ where $(\psi(1), n) = 1$.

Theorem (Gauss)

Write the prime factorization of n in the form $n = 2^{n_0} p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ where $n_0 \geq 0$, each $n_i \geq 1$ and the p_i are odd primes. If $n_0 \geq 2$ then

$$U(n) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{n_0-2}} \oplus \mathbb{Z}_{(p_1-1)p_1^{n_1-1}} \oplus \cdots \oplus \mathbb{Z}_{(p_k-1)p_k^{n_k-1}}.$$

Otherwise, $U(n) \cong \mathbb{Z}_{(p_1-1)p_1^{n_1-1}} \oplus \cdots \oplus \mathbb{Z}_{(p_k-1)p_k^{n_k-1}}$.

Cayley's Theorem

Definition

Given a group G and an element $h \in G$, write $L_h \colon G \to G$ for the *left-multiplication* function

$$L_h(g) = h \cdot g \quad \text{for} \quad g \in G.$$

Theorem (Cayley)

Every finite group G is isomorphic to a subgroup of the permutation group S_n for some n.

Proof.

We take $n = |G|$ and view S_n as the group $S_n = \mathrm{Perm}(G)$ of permutations of the set G. Define $L \colon G \to \mathrm{Perm}(G)$ by $L(g) = L_g$. It is now easy to check that G is a one-to-one homomorphism of groups. Thus $G \cong L(G) \subseteq S_n$. $\square$

Automorphism Groups continued

$\mathrm{Aut}(S_3) \cong S_3$

An automorphism $\psi\colon S_3 \to S_3$ must permute the three elements of order 2, namely $(12), (23), (13)$. Further, any such permutation gives an automorphism.

$\mathrm{Aut}(S_4) \cong S_4$

An automorphism $\psi\colon S_4 \to S_4$ preserves the subgroup $T = \{e, (12)(34), (13)(24), (14)(23)\}$. Consider the generating cycles $(12), (23), (34)$. We have 6 choices for $\psi(12) = (ij)$. We then have $\psi(34) = (st)$ is the disjoint cycle. This leaves 4 choices for $\psi(23)$.

$\mathrm{Aut}(D_n) \cong \mathbb{Z}_n \rtimes U(n)$

Recall $D_n = \langle a, b \mid a^n = b^2 = e, bab = a^{-1} \rangle$. Given $(i, j) \in \mathbb{Z}_n \oplus U(n)$ we define $\psi_{ij}(a) = a^j$ and $\psi_{ij}(b) = ba^i$.

Inverse Problem for Automorphism Groups

Question:

Is every finite group isomorphic to $\mathrm{Aut}(G)$ *for some finite group* G*?*

Answer: No!

Let $n \geq 1$. Then $\mathbb{Z}_{2n+1}$ is not isomorphic to $\mathrm{Aut}(G)$ for any finite group G.

Some Terminology

subgroup: subset $H \subseteq G$ closed under multiplication and inverses

normal subgroup: subgroup H with $ghg^{-1} \in H$ for all $g \in G, h \in H$.

center of G: $Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$

$Z(G)$ is a normal subgroup of G

quotient group: Given H a normal subgroup of G define

$G/H = \{gH \mid g \in G\}$ where $gH = \{gh \mid h \in H\}$ is the left coset.

multiplication: $aH \cdot bH = abH$

Two Easy Lemmas

Lemma 1

Any subgroup of a cyclic group is cyclic

Proof.

Let $m = \min\{k \mid a^k \in H\}$. Then $H = \langle a^k \rangle$. □

Lemma 2

If $G/Z(G)$ is cyclic then G is abelian.

Proof.

Write $G/Z(G) = \langle aZ(G) \rangle$. Then elements $g, h \in G$ can be written $g = a^k z_1$ and $b = a^m z_2$ for some $k, m \geq 0$ and $z_1, z_2 \in Z(G)$. Then

$$gh = a^k z_1 a^m z_2 = a^{k+m} z_1 z_2 = a^m z_2 a^k z_1 = hg.$$

□

Conjugation Action and Inner Automorphisms

Given $g \in G$ we obtain an automorphism

$$\varphi_g \in \mathrm{Aut}(G) \text{ where } \varphi_g(h) = ghg^{-1}.$$

The assignment $g \mapsto \varphi_g$ gives a homomorphism

$$\varphi \colon G \to \mathrm{Aut}(G).$$

We have

$$\ker(\varphi) = Z(G).$$

The group $G/Z(G)$ is called the group of inner automorphisms $\mathrm{Inn}(G)$ of G and we have

$$\mathrm{Inn}(G) \cong G/Z(G) \hookrightarrow \mathrm{Aut}(G).$$

A Negative Result

Theorem

Let $n \geq 1$. Then the cyclic group $\mathbb{Z}_{2n+1}$ is not isomorphic to $\mathrm{Aut}(G)$ for any finite group G.

Proof.

Suppose $\mathrm{Aut}(G) \cong \mathbb{Z}_{2n+1}$. Then $\mathrm{Inn}(\mathrm{G})$ is cyclic by Lemma 1. Thus G is abelian by Lemma 2.

Since G is abelian, the map $\psi\colon G \to G$ given by $\psi(a) = a^{-1}$ is an automorphism of G. If there exists an element a in G with $a \neq a^{-1}$ then ψ has order $= 2$. This is a contradiction: $\mathbb{Z}_{2n+1}$ has odd order.

Suppose every element $a \in G$ satisfies $a = a^{-1}$. Then $G \cong \mathbb{Z}_2^m$ for some $m > 1$. But then

$\mathrm{Aut}(G) = \mathrm{GL}(m, 2) =$ invertible $m \times m$ matrices with coefficients in $\mathbb{Z}_2$

It is an easy exercise to prove:

$$|\mathrm{GL}(m, 2)| = (2^m - 1)(2^m - 2)\cdots(2^m - 2^{m-1}).$$

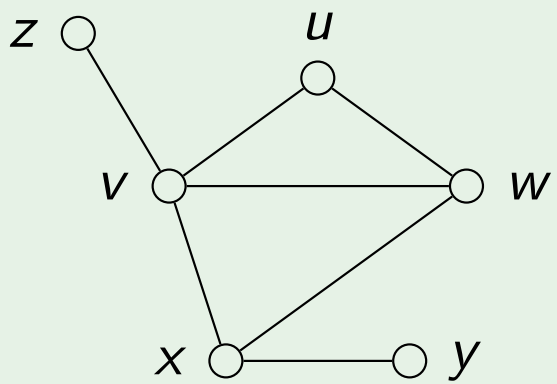
In particular, $\mathrm{GL}(m, 2)$ has an even number of elements. □

Graph Theory

Definition

A *graph* Γ is a set V of vertices together with a set E of edges where each element of E is a two element set $\{v_1, v_2\}$ of vertices.

Example (A Simple Graph)



$$V = \{u, v, x, y, z\}$$

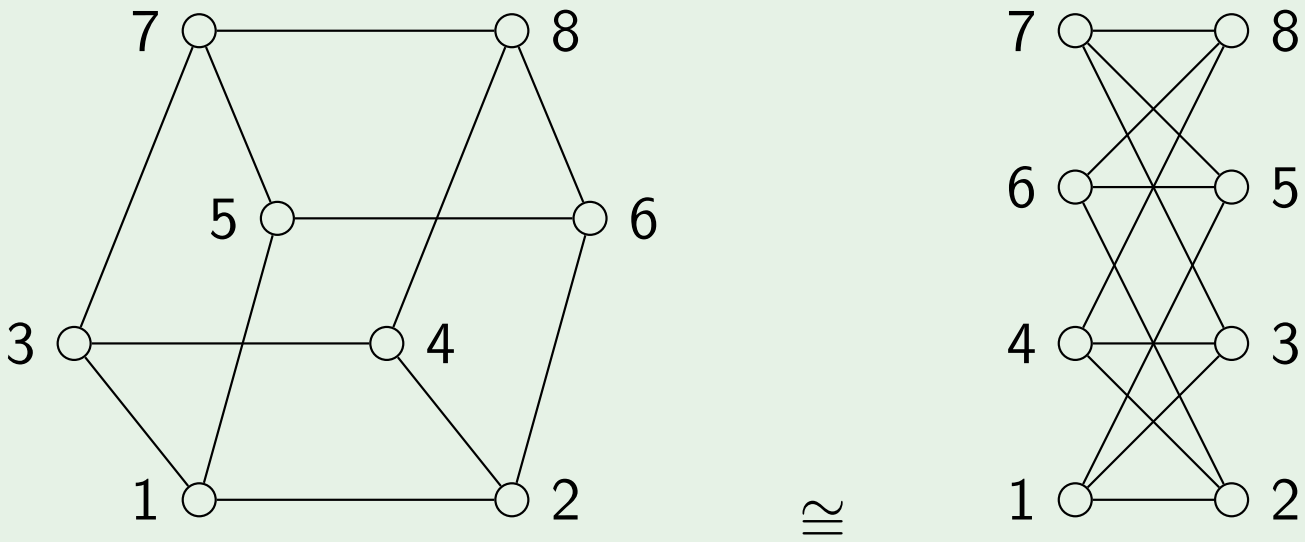
$$E = \{\{u, v\}, \{u, w\}, \{v, w\}, \{v, x\}, \{v, z\}, \{w, x\}, \{x, y\}\}$$

Graph Isomorphisms

Definition

An *isomorphim* from graph Γ_1 with V_1 and edges E_2 to graph Γ_2 with V_2 and E_2 is one-to-one correspondence $f : V_1 \to V_2$ such that $\{v_1, v_2\} \in E_1$ if and only if $\{f(v_1), f(v_2)\} \in E_2$ for all $v_1, v_2 \in V_1$.

Example (A Graph Isomorphism)



Graph Automorphisms

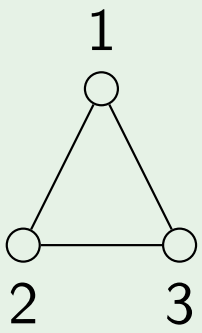
Definition

Given a graph Γ, let $\mathrm{Aut}(\Gamma)$ denote the set of all graph isomorphisms from Γ to Γ.

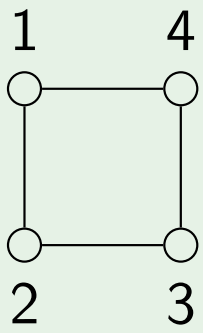
Theorem

$\mathrm{Aut}(\Gamma)$ *is a group under composition of functions.*

Examples (Graph Automorphism Groups)



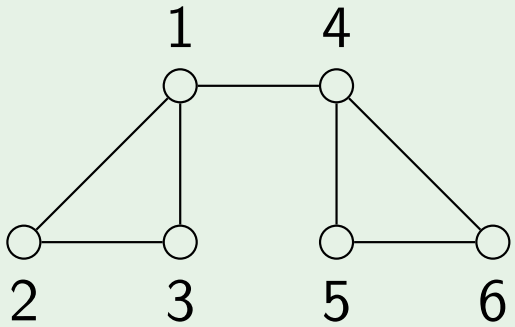
$\mathrm{Aut}(\Gamma) \cong S_3$.



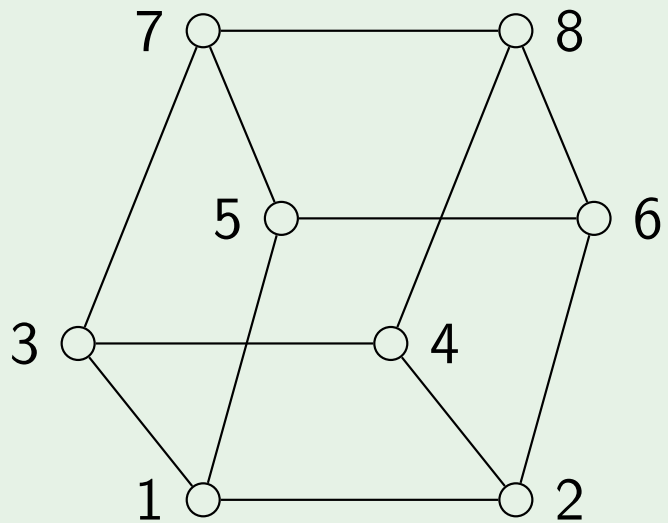
$\mathrm{Aut}(\Gamma) \cong D_4$.

Graph Automorphism Examples continued

Examples



$$\mathrm{Aut}(\Gamma) = \{e, (23), (56), (14)(25)(36), (14)(26)(35),$$
$$(23)(56), (14)(2635), (14)(2536)\} \cong D_4$$



$$\mathrm{Aut}(\Gamma) \cong S_4 \times \mathbb{Z}_2$$

Inverse Problem for Graph Automorphisms

Question

Is every finite group G isomorphic to $\mathrm{Aut}(\Gamma)$ for some simple graph Γ?

Answer

Yes!

Theorem (Frucht, 1939)

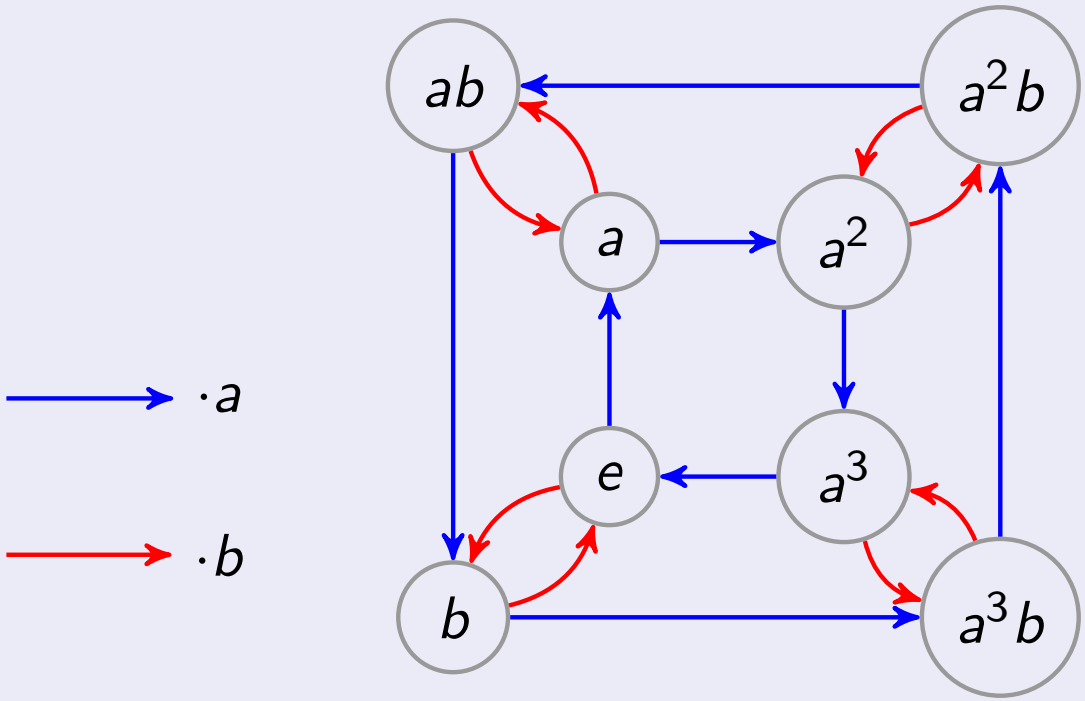
Given a finite group G there exists a simple graph Γ with $\mathrm{Aut}(\Gamma) \cong G$.

Proof of Frucht's Theorem

Definition (Cayley Graph of a Group)

Let G be a finite group with generating set $S = \{s_1, \ldots, s_n\}$ satisfying $e \notin S$. The *Cayley graph* $\mathcal{G}$ of G corresponding to S is the colored, directed graph with vertex set $V = G$, color set $C = \{c_1, \ldots, c_n\}$ and directed edges $E = \{(g, g \cdot s_k) \mid g \in G, s_k \in S\}$. The edge $(g, g \cdot s_k)$ has color c_k.

Cayley Graph of $D_4 = \langle a, b \mid a^4 = e, b^2 = e, ab = ba^3 \rangle$



Proof of Frucht's Theorem continued

Definition (Automorphism Group of a Colored, Directed Graph)

Given a colored, directed graph $\mathcal{G}$ let $\mathrm{Aut}^{cd}(\mathcal{G})$ denote the group of all automorphisms ψ of $\mathcal{G}$ such that

(i) (v_1, v_2) is in E if and only if $(\psi(v_1), \psi(v_2))$ is in E and

(ii) if (v_1, v_2) has color c then $(\psi(v_1), \psi(v_2))$ has color c also.

Theorem

Let G be a finite group and $\mathcal{G}$ denote the Cayley graph corresponding to some generating set S. Then $G \cong \mathrm{Aut}^{cd}(\mathcal{G})$.

Proof.

Let $\psi \in \mathrm{Aut}^{cd}(\mathcal{G})$ and $g \in G$ and $s_k \in S$. We have

$$(g, gs_k) \in E \Longrightarrow (\psi(g), \psi(gs_k)) \in E.$$

Since ψ is color-preserving we have $\psi(gs_k) = \psi(g)s_k$.

Proof of Frucht's Theorem continued

Proof continued ($\mathrm{Aut}^{cd}(\mathcal{G}) \cong G$).

We have shown

$$\psi(gs_k) = \psi(g)s_k$$

for all $s_k \in S$. It follows easily that

$$\psi(gs_{k_1} \cdots s_{k_m}) = \psi(g)s_{k_1} \cdots s_{k_m}$$

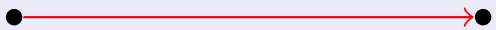
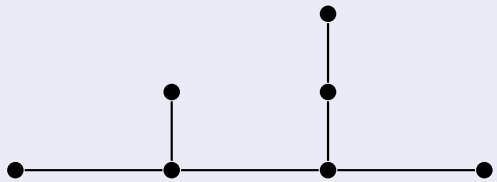
for any product of elements of S. Since S generates G we conclude

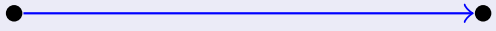
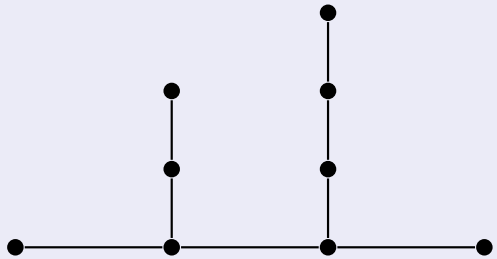
$$\psi(gh) = \psi(g)h \text{ for all } g, h \in G.$$

Thus $\psi = L_{g_0} : G \to G$ is left-multiplication by $g_0 = \psi(e)$. The result now follows as in the proof of Cayley's Theorem. □

Proof of Frucht's Theorem: Last Step

Replacing Colored, Directed Edges with Simple Ones

Replace  by 

Replace  by 

etc

Starting with a colored, directed graph $\mathcal{G}$ we obtain a simple graph Γ with

$$\mathrm{Aut}^{cd}(\mathcal{G}) = \mathrm{Aut}(\Gamma).$$

□

Galois Theory

Fields

A *field* F is a set with a commutative operations of $+$ and $\cdot$ such that every nonzero element has a multiplicative inverse.
Examples: $\mathbb{Z}_p$ for p prime, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

Extension Fields

A field E containing a field F and extending the operations of F is called an *extension field* of F. Given a field F and an element $\alpha \in E$, an extension of F, we write $F(\alpha)$ for the smallest extension field of F containing F and α. Example: $\mathbb{C} = \mathbb{R}(i)$ where $i = \sqrt{-1}$.

Irreducible Polynomials

A polynomial $f(x)$ with coefficients in a field F is *irreducible* over F if $f(x)$ cannot be factored (nontrivially) as $f(x) = g(x)h(x)$
Examples: $f(x) = x^5 - 2$ is irreducible over $\mathbb{Q}$ but not over $\mathbb{R}$
$g(x) = x^2 + 1$ is irreducible over $\mathbb{R}$ but not over $\mathbb{C}$

Splitting Fields

Definition (Splitting Field)

Let $f(x)$ be irreducible over F. The *splitting field* E of $f(x)$ is the smallest extension field of F such that $f(x)$ factors as a product of linear polynomials over E.

Examples (Splitting Fields)

(1) $f(x) = x^2 + 1$ irreducible over $\mathbb{R}$. The splitting field for $f(x)$ is $\mathbb{C} = \mathbb{R}(i)$. Note that $f(x) = (x - i)(x + i)$ in $\mathbb{C}$.

(2) $f(x) = x^2 - 2$ irreducible over $\mathbb{Q}$. The splitting field for $f(x)$ is $\mathbb{Q}(\sqrt{2})$. Note that $f(x) = (x - \sqrt{2})(x + \sqrt{2})$ in $\mathbb{R}$

(3) $f(x) = x^5 - 2$ irreducible over $\mathbb{Q}$. Let $\alpha = 2^{\frac{1}{5}}$ and $\omega = e^{\frac{2\pi i}{5}}$ so that $\alpha^5 = 2$ and $\omega^5 = 1$. The splitting field for $f(x)$ is $\mathbb{Q}(\alpha, \omega)$. Note that $f(x) = (x - \alpha)(x - \omega\alpha)(x - \omega^2\alpha)(x - \omega^3\alpha)(x - \omega^4\alpha)$ in $\mathbb{Q}(\alpha, \omega)$.

Galois Groups

Definition (Galois Group of an Irreducible Polynomial)

Let $f(x)$ be irreducible over F. Let E denote the splitting field for $f(x)$. The *Galois group* $G(f)$ is the group of automorphisms of E that fix F.

Theorem

Suppose $f(x)$ has degree n. Then $G(f)$ is a subgroup of S_n.

Proof.

Recall $E = F(\alpha_1, \ldots, \alpha_n)$ where the α_k are the roots of $f(x)$. An automorphism of E that fixes F is determined by its action on the roots of $f(x)$. □

Example

Let $f(x) = x^2 + 1$ irreducible over $\mathbb{R}$. The splitting field is $\mathbb{C} = \mathbb{R}(i)$. One nontrivial automorphism: $i \mapsto -i$. The Galois group $G(f) \cong \mathbb{Z}_2$.

Galois Groups continued

Example

Let $f(x) = x^5 - 2$ irreducible over $\mathbb{Q}$. The splitting field is $\mathbb{Q}(\alpha, \omega)$ with $\alpha = 2^{\frac{1}{5}}$ and $\omega = e^{\frac{2\pi i}{5}}$. Generators of the Galois group $G(f)$:

$$\psi: \qquad \alpha \mapsto \alpha\omega, \qquad \omega \mapsto \omega$$

$$\phi: \qquad \alpha \mapsto \alpha, \qquad \omega \mapsto \omega^2$$

Check that $\psi^5 = \phi^4 = 1$ and that $\phi \circ \psi \circ \phi^{-1} = \psi^4$. We conclude

$$G(f) \cong \mathbb{Z}_5 \rtimes U(5).$$

Galois Groups for Irreducible Quintics

An Inverse Problem

Which finite groups occur as $G(f)$ for $f(x)$ a degree 5 polynomial irreducible over $\mathbb{Q}$?

Lemma

If $f(x)$ is irreducible of degree n over $\mathbb{Q}$ then $G(f) \subseteq S_n$ and $n \mid |G(f)|$.

Proof.

Let E be the splitting field for $f(x)$ over $\mathbb{Q}$. Then we have extensions:

$$E \longrightarrow \frac{\mathbb{Q}(x)}{\langle f(x) \rangle} \xrightarrow{n} \mathbb{Q}.$$

Galois Groups of Irreducible Quintics continued

Corollary

The possible orders for $G(f)$ for $f(x)$ of degree 5 over $\mathbb{Q}$ are $5, 10, 20, 60, 120$.

Proof.

The order of $G(f)$ must be a multiple of 5 and divide $5! = 120$. Further, S_5 has no subgroups of order 30 or of order 40. □

Theorem

The finite groups occurring as $G(f)$ for $f(x)$ an irreducible quintic over $\mathbb{Q}$ are:

$$\mathbb{Z}_5, \quad D_5, \quad \mathbb{Z}_5 \rtimes U(5), \quad A_5, \quad \text{and} \quad S_5$$

Two Useful Results

Theorem (The Discriminant)

Let $f(x)$ be irreducible over $\mathbb{Q}$ with roots $r_1, \ldots, r_n$ in some extension field. Define

$$D(f) = \prod_{j>k} (r_j - r_k)^2.$$

Then $D(f) \in \mathbb{Q}$ and $D(f)$ is a perfect square in $\mathbb{Q}$ if and only if $G(f) \subseteq A_n$.

Theorem (Dedekind)

Let $f(x)$ be monic and irreducible over $\mathbb{Q}$ and suppose $f(x)$ factors into polynomials of degrees $n_1, \ldots, n_k$ over $\mathbb{Z}_p$ for some prime p. Then $G(f)$ contains a permutation with cycle decomposition having factors of length $n_1, \ldots, n_k$.

Galois Groups of Irreducible Quinitics

Group	Polynomial	Comments
$\mathbb{Z}_5 \rtimes U(5)$	$x^5 - 2$	proved above
S_5	$7x^5 - 21x + 3$	three real roots $D(f)$ not a perfect square
A_5	$x^5 + 20x + 16$	one real root $D(f)$ a perfect square Dedekind $\Longrightarrow$ a 3-cycle
D_5	$x^5 - 5x + 12$	one real root $D(f)$ a perfect square no 3-cycle
C_5	$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 3$	5 real roots $r_k^2 = r_{(k+1) \bmod 5} + 2$

Inverse Galois Problem

Open Question

Does every finite group occur as the Galois group of an irreducible polynomial over $\mathbb{Q}$?

Significant Partial Results

Hilbert: S_n and A_n occur as Galois groups for any n

Shafarevich: Every finite solvable group occurs as a Galois group

Thompson: The Monster group occurs as a Galois group

Two Inverse Problems in Topology

Self-Equivalences

Given a topological space X we have a group

$$\mathcal{E}(X) = \text{group of homotopy self-equivalences of } X$$

and a topological monoid

$$\mathrm{Aut}(X) = \text{space of all homotopy self-equivalences of } X$$

Inverse Problems

- Is every finite group G isomorphic to $\mathcal{E}(X)$ for some space X?
- Is every topological monoid A isomorphic to $\mathrm{Aut}(X)$ for some space X?

Thank You!!