APAM2021
Chulalongkorn University
June 17-18, 2021

Future Development and Applications of Algebra

Teerapong Suksumran
Department of Mathematics
Faculty of Science
Chiang Mai University

Outline of the talk

Introduction
- Importance of pure mathematics

Applications of algebra
- Geometry
- Topology
- Algebra
- Analysis

Future development
- Problems related to group presentation
- Problem related to Galois groups

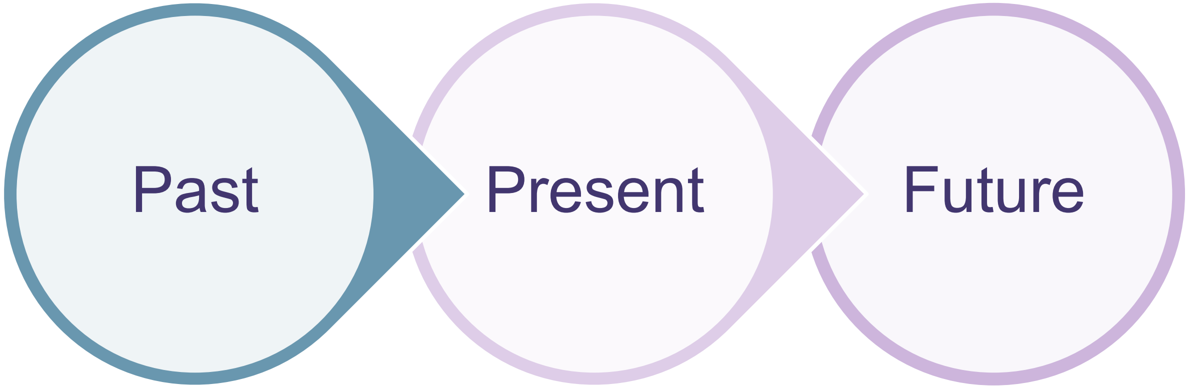
Pure mathematics

Inspiration
- Beautifulness
- Previous incomplete results

Sources of problems
- Pure/Applied mathematics
- Sciences

Backgrounds
- Techniques of proving
- Basic knowledge in algebra, analysis, topology, geometry, combinatorics, etc.

ไม่มีใครทำนายอนาคตได้ถูกต้อง 100%



Prime numbers and applications

Euclid of Alexandria (335 – 265 BC)

The study of prime numbers

↓

The RSA public key encryption

Group (Representation) theory in physics

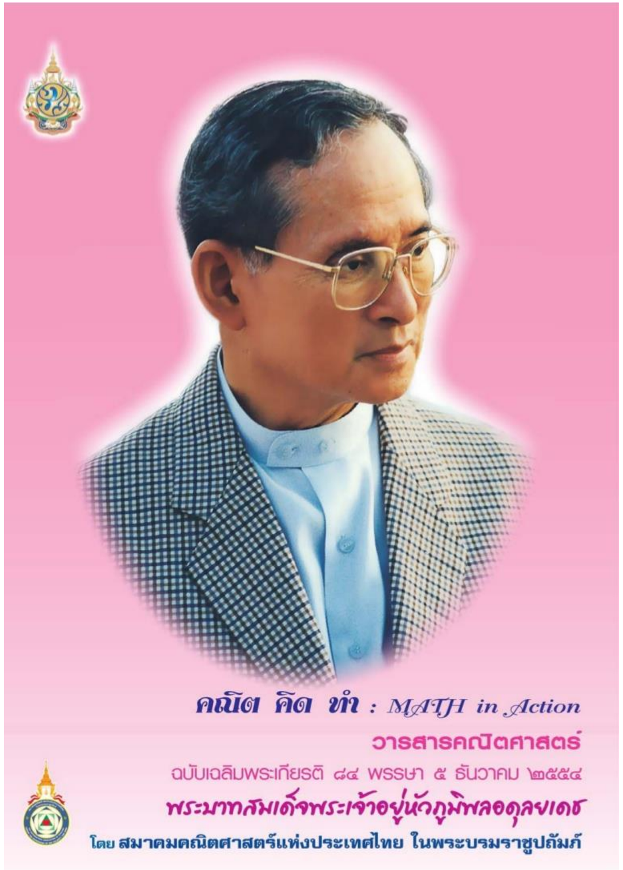
"We may as well cut out group theory. That is a subject which will never be of any use in physics."

James Jeans

การอภิปรายปรับปรุงแผนการเรียนวิชาคณิตศาสตร์ สำหรับหลักสูตรฟิสิกส์ มหาวิทยาลัยพรินซ์ตัน (Princeton University) ระหว่างเจมส์ จีนส์ (James Jeans) และ ออสวอล์ด เว็บเลน (Oswald Veblen) ในปีค.ศ. 1910

Group (Representation) theory in physics

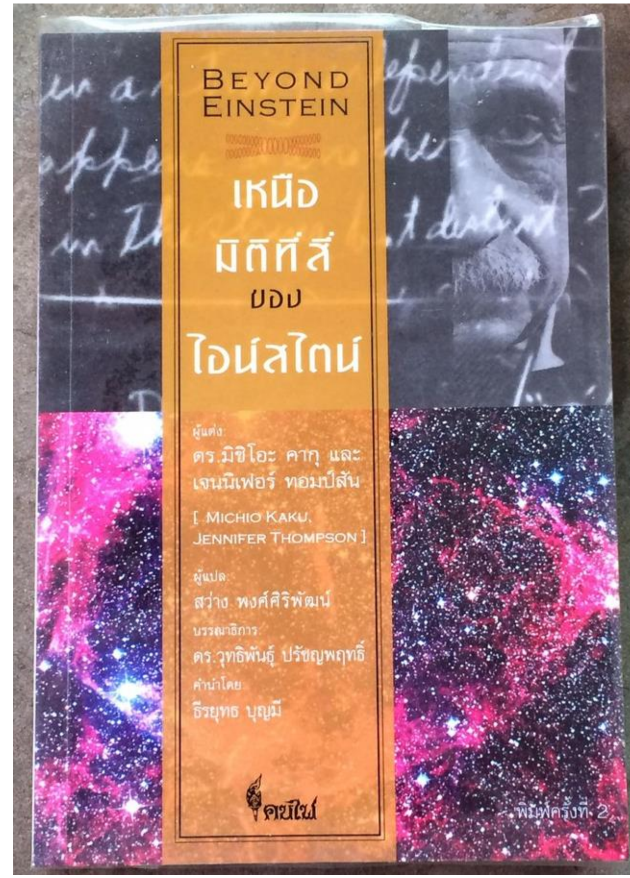
“บทเรียนที่ได้จากเรื่องเล่าข้างต้นคือ เราควรรู้ว่าอนาคตของวิทยาศาสตร์นั้นเป็นเรื่องที่ไม่มีใครสามารถทำนายได้ถูกต้อง และในทำนองเดียวกันก็ไม่มีใครที่สามารถระบุได้ว่า คณิตศาสตร์เรื่องใดจะมีบทบาทและความสำคัญเพียงใดในวิทยาศาสตร์เรื่องนั้นหรือเรื่องนี้ เพราะทั้งวิทยาศาสตร์และคณิตศาสตร์ต่างก็กำลังเจริญเติบโตตลอดเวลา ดังนั้น ความสัมพันธ์และความผูกพันระหว่างกันจึงมีมากและจะมีเพิ่มต่อไปอย่างไม่มีที่สิ้นสุด”



บทบาทและความสำคัญของคณิตศาสตร์ในวิทยาศาสตร์ (Role and Importance of Mathematics in Science) โดย ศาสตราจารย์ ดร. สุทัศน์ ยกส้าน

Lie groups and physics

“...เมื่อ Lie Groups ได้ถูกพัฒนาขึ้นเรียบร้อยแล้ว โดยทั้งหมดถูกพัฒนาขึ้นจากโครงสร้างทางคณิตศาสตร์ที่เป็นนามธรรมล้วน ๆ นักคณิตศาสตร์ต่างพากันคิดว่า ในที่สุดพวกเขาได้ค้นพบสาขาของความรู้ซึ่งนักฟิสิกส์จะไม่สามารถนำไปใช้ประโยชน์ได้ในทางปฏิบัติ (...) พวกเขาเข้าใจผิด หนึ่งศตวรรษให้หลัง ทฤษฎีเกี่ยวกับ Lie groups ซึ่งดูไร้ประโยชน์นั้น ได้กลายมาเป็นรากฐานให้กับเอกภพทางกายภาพทั้งหมด!”

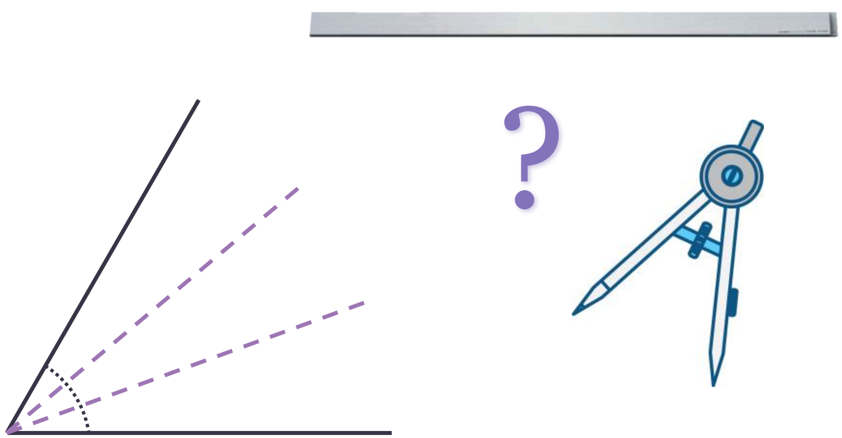


เหนือมิติที่ 4 ของไอน์สไตน์ (Beyond Einstein: The Cosmic Quest for the Theory of the Universe) เขียนโดยดร.มิชิโอะ คากุและเจนนิเฟอร์ ทอมป์สัน แปลโดยสว่าง พงศ์ศิริพัฒน์

Trisecting an angle

Problem 1

Is it possible using only straightedge and compass to trisect any given angle θ?



Not always possible!

Criterion for trisecting an angle

A polynomial of degree 3 in $\mathbb{Q}[x]$ is *reducible* (i.e., can be expressed as a product of two polynomials in $\mathbb{Q}[x]$ of positive degree) if and only if it has a root in $\mathbb{Q}$.

Theorem 2

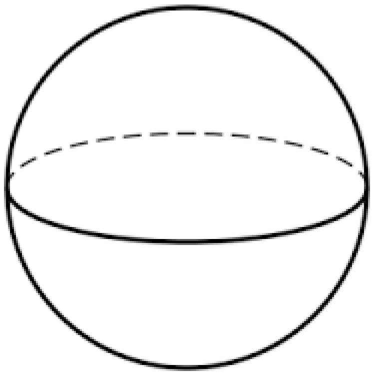
If $\cos\theta \in \mathbb{Q}$, then the angle θ can be trisected by straightedge and compass if and only if $4x^3 - 3x - \cos\theta$ is reducible over $\mathbb{Q}$.

For example, $\pi/3$ cannot be trisected since $4x^3 - 3x - 1/2$ is not reducible over $\mathbb{Q}$ (it has no rational root).

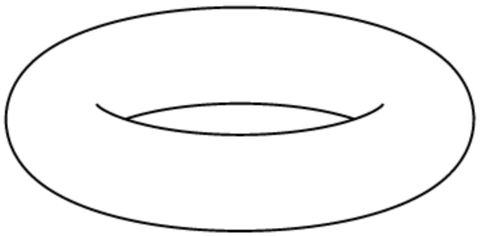
Modern Algebra With Applications, William J. Gilbert and W. Keith Nicholson

Please answer the following question

Determine whether the following surfaces are the same from the topological viewpoint (i.e., are homeomorphic):



Sphere, S^2



Torus, T

NO!

because one has no hole and the other has a hole.

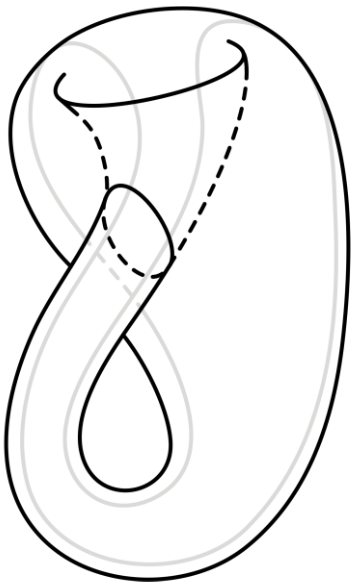
Please answer the following question

Determine whether the following groups are the same from the algebraic viewpoint (i.e., are isomorphic):

- The trivial group $\{e\}$
- The direct group $\mathbb{Z}\times\mathbb{Z}$

NO! because their sizes are different.

Fundamental groups



Topological space, X

construction of path homotopy classes of loops

$$\pi_1(X, x_0)$$

Fundamental group of X

Topological invariant via the notion of a group

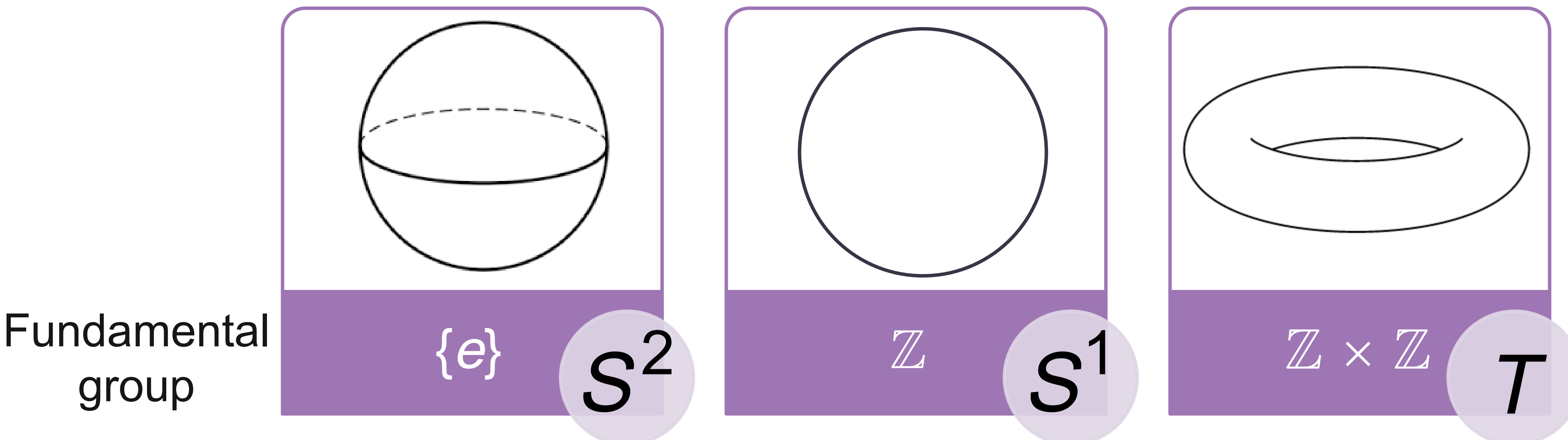
Theorem 3

If X and Y are homeomorphic topological spaces, then their fundamental groups are isomorphic.

Hence, if $\pi_1(X, x_0) \not\cong \pi_1(Y, y_0)$, then X and Y are not homeomorphic.

Topology, James Munkres

Non-homeomorphic spaces



Quadratic formula

A polynomial $p(x) = ax^2 + bx + c$ in $\mathbb{R}[x]$ with $a \neq 0$ may have no root, or one root, or two roots, given by

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

In this case, every quadratic polynomial in $\mathbb{R}[x]$ is solvable by radicals.

Solvability by radicals

A polynomial in $\mathbb{R}[x]$ is *solvable by radicals* if we can obtain all its roots by adjoining n^{th} roots (for various n) to $\mathbb{R}$. That is, each root of the polynomial can be written as an expression involving elements of $\mathbb{R}$ combined by the operations of addition, subtraction, multiplication, division, and extraction of roots.

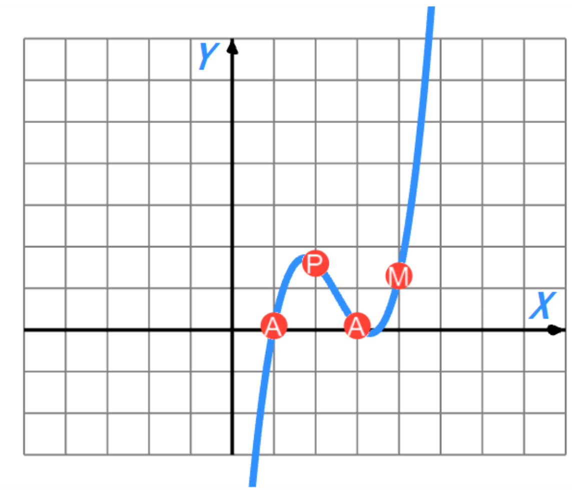
Polynomials with degree ≤ 5

Polynomials of degree	Solvable by radicals	Name/Formula	Time around
2	Yes	Quadratic formula	1600 BC
3	Yes	Cardano's formula	1543
4	Yes	Ferrari's method	1545
5	No	Abel & Galois	1826-1831

Question 4

Is every polynomial of degree 5 in $\mathbb{R}[x]$ solvable by radicals?

Galois groups



Polynomial in $\mathbb{R}[x]$, f

construction of splitting field of f over $\mathbb{R}$.

Gal(f)

Galois group of f

Solvability by radicals via the notion of a group

A group G is *solvable* if G has a series of subgroups

$$\{e\} = N_0 \subset N_1 \subset \cdots \subset N_k = G,$$

where, for each i with $0 \leq i \leq k - 1$, N_i is normal in N_{i+1} and N_{i+1}/N_i is abelian.

Theorem 5

A polynomial f with coefficients in $\mathbb{R}$ is solvable by radicals if and only if the Galois group $\mathrm{Gal}(f)$ is solvable.

For example, $f(x) = x^5 - 8x + 2$ is not solvable by radicals since $\mathrm{Gal}(f) \cong S_5$, which is not a solvable group.

Fields and Galois Theory, John M. Howie

Inequality related to integrals

If *f* and *g* are continuous real-valued functions on the closed interval [0,1], then

$$\left|\int_0^1 f(t)g(t)\,dt\right| \leq \sqrt{\int_0^1 f(t)^2\,dt}\,\sqrt{\int_0^1 g(t)^2\,dt}.$$

Cauchy-Schwarz Inequality

Theorem 6

If a and b are vectors in a real inner product space, then

$$\langle a,b\rangle^2 \leq ||a||^2||b||^2, \qquad (*)$$

where $||c|| = \langle c,c\rangle^{1/2}$.

Proof. Consider the quadratic function

$$||xa + b||^2 = ||a||^2x^2 + 2\langle a,b\rangle x + ||b||^2$$

in the variable x. Clearly, $(*)$ holds when $a = 0$ or $b = \lambda a$. Therefore, assume that a and b are linearly independent with $a \neq 0$. Hence, $||xa + b||^2 > 0$ for all $x \in \mathbb{R}$ and so the discriminant $4(\langle a,b\rangle^2 - ||a||^2||b||^2)$ is less than 0. □

Proofs from THE BOOK, Martin Aigner and Günter M. Ziegler

Cauchy-Schwarz Inequality

The inequality

$$\left|\int_0^1 f(t)g(t)dt\right| \leq \sqrt{\int_0^1 f(t)^2 dt}\sqrt{\int_0^1 g(t)^2 dt}$$

follows since the space of continuous real-valued functions on [0,1] forms a real inner product space whose inner product is given by

$$\langle f, g\rangle = \int_0^1 f(t)g(t)dt.$$

Conformal self-maps of the disk

Let $D = \{z \in \mathbb{C} : |z| < 1\}$ be the open unit disk. A continuously differentiable function $f: D \to \mathbb{C}$ is *analytic* if

$$\frac{\partial f}{\partial \bar{z}} = 0$$

at every point of D.

An analytic function $f: D \to D$ that is bijective is called a *conformal self-map* of D. Some examples are the following:

1. $z \mapsto \omega z$
2. $z \mapsto \dfrac{z - a}{1 - \bar{a}z}$,

where ω is a fixed unimodular complex and a is a fixed element in D.

Conformal self-maps of the disk

Theorem 7

If f is a non-identity conformal self-map of D, then f has at most two fixed points.

Proof. By a certain result in the literature, there are complex numbers a *and* ω with $a \in D$, $|\omega| = 1$ such that

$$f(z) = \omega \frac{z-a}{1-\bar{a}z}$$

for all $z \in D$. If z_0 is a fixed point of f, then z_0 must be a root of the quadratic equation $\bar{a}z^2 + (\omega - 1)z - a\omega = 0$, which has at most two roots, in the case $a \neq 0$. If $a = 0$, we have 0 is the unique fixed point of f. $\square$

Rough definition of free groups

Let X be a non-empty set and let X^{-1} be a set that has a bijection from X to X^{-1} such that $X \cap X^{-1} = \varnothing$. A string of elements from $X \cup X^{-1}$ is called a *word*. A *reduced word* is a word not containing subwords of the form xx^{-1} or $x^{-1}x$.

The *free group* on X, denoted by $F(X)$, consists of the set of reduced words on X, together with an empty word 1, and the operation of concatenation:

$$(x^{\alpha_1}x^{\alpha_2}\cdots x^{\alpha_m})(y^{\beta_1}y^{\beta_2}\cdots y^{\beta_n}) = x^{\alpha_1}x^{\alpha_2}\cdots x^{\alpha_m}y^{\beta_1}y^{\beta_2}\cdots y^{\beta_n}.$$

Groups defined by presentation

Let G be a group, let S be a non-empty set, and let R be a set of words on S. We say that $\langle S \mid R \rangle$ is a *presentation* of G if

$$G \cong F(S)/N,$$

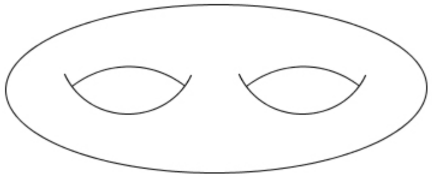
where N is the normal closure of R in $F(S)$.

Group	Presentation
$\mathbb{Z}$	$\langle a \mid \varnothing \rangle$
$\mathbb{Z} \times \mathbb{Z}$	$\langle a, b \mid a^{-1}b^{-1}ab = 1 \rangle$
Dihedral group of order $2n$	$\langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$

Fundamental groups

Here are some fundamental groups defined by presentation.

Space	Presentation of fundamental group
Unit circle in $\mathbb{R}^2$	$\langle a \mid \varnothing \rangle$
Torus	$\langle a, b \mid a^{-1}b^{-1}ab = 1 \rangle$
Double torus	$\langle a, b, c, d \mid a^{-1}b^{-1}abc^{-1}d^{-1}cd = 1 \rangle$
Projective plane in $\mathbb{R}^2$	$\langle a \mid a^2 = 1 \rangle$
Figure eight	$\langle a, b \mid \varnothing \rangle$



Double torus

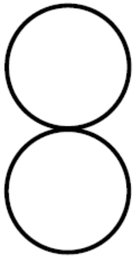


Figure eight

Dehn’s problems

By “algorithm” we mean a procedure, given by a finite number of instructions, that produces an answer after a finite number of steps, without ever leaving any doubt as to the next step.

The Word Problem

Let G be a group given by a finite presentation $\langle S \mid R \rangle$. Is there an algorithm that decides whether a given word is equivalent to the identity in G?

The Isomorphism Problem

Is there an algorithm that determines whether a pair of finite presentations define isomorphic groups?

Galois groups

Let E be an extension field of $\mathbb{Q}$. The *Galois group* of E over $\mathbb{Q}$ is defined as

$$\mathrm{Gal}(E/\mathbb{Q}) = \{\text{automorphisms of } E \text{ fixing all elements of } \mathbb{Q}\}.$$

Open Problem (Noether)

Determine which finite groups can occur as Galois groups over $\mathbb{Q}$.

Partial answers:

- every solvable group
- certain kinds of simple groups

Contemporary Abstract Algebra, Joseph A. Gallian

Questions & Answers

Thank you very much!