Field Theory, Group Theory, and the Abel Ruffini Theorem

Xiwen Guo (advised by Brett Hungar)

*The Ohio State University

Background

This semester emphasized how algebraic structures (fields, groups, and their categorical generalizations) underpin classical problems, demonstrating the power of abstraction in unifying seemingly disparate mathematical ideas. Through this framework, we connected theoretical constructs like minimal polynomials and composition series to profound results such as the unsolvability of higher-degree equations.

Fields

Definition 1 *A **field** is a set F equipped with two operations, addition and multiplication, such that:*

- *Addition is associative:* $(a+b)+c = a+(b+c)$
- *Multiplication is associative:* $(ab)c = a(bc)$
- *Addition is commutative:* $a+b = b+a$
- *Multiplication is commutative:* $ab = ba$
- *There is a unit, 1, satisfying:* $1 \cdot a = a \cdot 1 = a$
- *There is a zero, 0, satisfying:* $0 + a = a + 0 = a$
- *There are inverses: for all* $a \neq 0$*, there is an element* a^{-1} *satisfying* $a^{-1} \cdot a = 1$
- *There are negatives: for all* a*, there is an element* $-a$ *satisfying* $a + (-a) = 0$
- *The distributive law holds:* $a(b+c) = ab + ac$ *for all* $a, b, c \in F$*.*

Example 2

- *rational numbers* $\mathbb{Q}$
- *real numbers* $\mathbb{R}$
- *complex numbers* $\mathbb{C}$ *are fields.*
- *rational functions (eg things in the form* $\frac{x^2+4x+3}{2x-10}$*)*
- *finite fields (eg,* $\mathbb{F}_5 = \{0,1,2,3,4\}$ *with multiplication and addition mod 5)*
- *The integers* $\mathbb{Z}$ *do not form a field because not all nonzero elements have multiplicative inverses.*

Definition 3 *The **minimal polynomial** of an algebraic element* α *over a field* F *is the unique polynomial* $p(x)$ *with leading coefficient 1 of the lowest degree such that* $p(\alpha) = 0$*.*

Example 4 *Examples of things like* $\sqrt{2}$*,* i*,* $\sqrt[3]{2}$*,* ζ *(which solves something like* $x^2 + x + 1$ *or also* $x^3 - 1$*)*

- *The minimal polynomial of* $\sqrt{2}$ *over* $\mathbb{Q}$ *is* $x^2 - 2$*.*
- *The minimal polynomial of* i *(where* $i^2 = -1$*) over* $\mathbb{Q}$ *is* $x^2 + 1$*.*
- *The minimal polynomial of* ζ *(a primitive third root of unity) over* $\mathbb{Q}$ *is* $x^2 + x + 1$*, since* ζ *satisfies* $x^3 - 1 = (x-1)(x^2+x+1)$*.*

Definition 5 *The **splitting field** of a polynomial is the smallest field containing all its roots, over which the polynomial factors completely into linear terms.*

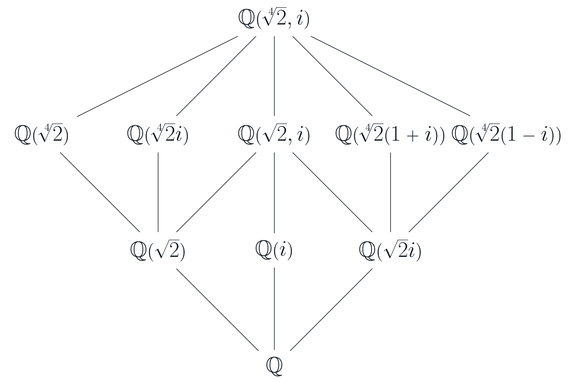
Example 6 *The roots of* $x^3 - 2$ *are:*

$$\sqrt[3]{2}, \quad \sqrt[3]{2}\zeta, \quad \sqrt[3]{2}\zeta^2$$

The field $\mathbb{Q}(\sqrt[3]{2})$ *contains only the real root* $\sqrt[3]{2}$*, but not the complex roots* $\zeta\sqrt[3]{2}$ *and* $\zeta^2\sqrt[3]{2}$*. To include the complex roots, we must adjoin* ζ *to* $\mathbb{Q}(\sqrt[3]{2})$*, giving the splitting field* $\mathbb{Q}(\sqrt[3]{2}, \zeta)$*.*

Field Extension Diagram

A *subfield* of a field is a subset that contains 0, 1, is closed under addition and multiplication, and contains inverses and negatives of its elements. We can create a diagram of a field and its subfields; below is an example of such a diagram for $\mathbb{Q}(\sqrt[4]{2}, i)$ (the splitting field for $x^4 - 2$).



Automorphisms

Definition 7 *A **field automorphism** of a field* F *is a function* $f : F \to F$ *satisfying:*

$$f(a+b) = f(a) + f(b); \qquad f(a \cdot b) = f(a) \cdot f(b), \quad \forall a, b \in F$$
$$f(1) = 1; \qquad f(0) = 0$$

Example 8 ***Complex conjugation*** *f(a + bi) = a - bi*
This function preserves both addition and multiplication:

$$f((a+bi)+(c+di)) = (a+c) - (b+d)i = f(a+bi) + f(c+di),$$

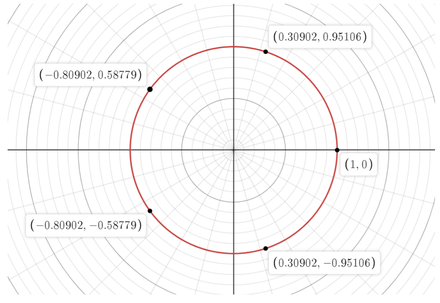
and

$$f((a+bi)(c+di)) = f(ac - bd + (ad+bc)i) = ac - bd - (ad+bc)i = f(a+bi)f(c+di).$$

Thus, f *is a field automorphism.*

If we compose two field automorphisms, then the composition is also a field automorphism. For example, there is a field automorphism f of $\mathbb{Q}(\zeta)$ (where $\zeta^5 = 1$) given by $f(\zeta) = \zeta^2$. Below, we see how the composite of f with itself is also a field automorphism:

$$f = \begin{cases} \zeta \mapsto \zeta^2 \\ \zeta^2 \mapsto \zeta^4 \\ \zeta^3 \mapsto \zeta \\ \zeta^4 \mapsto \zeta^3 \end{cases} \qquad f \circ f = \begin{cases} \zeta \mapsto \zeta^2 \mapsto \zeta^4 \\ \zeta^2 \mapsto \zeta^4 \mapsto \zeta^3 \\ \zeta^3 \mapsto \zeta \mapsto \zeta^2 \\ \zeta^4 \mapsto \zeta^3 \mapsto \zeta \end{cases} = \begin{cases} \zeta \mapsto \zeta^4 \\ \zeta^2 \mapsto \zeta^3 \\ \zeta^3 \mapsto \zeta^2 \\ \zeta^4 \mapsto \zeta \end{cases}$$



A picture of the five solutions to $\zeta^5 = 1$

Groups

Definition 9 *A **group** is a set* G *equipped with a binary operation* $\cdot$ *that satisfies the following properties:*

- ***Associativity****: For all* $a, b, c \in G$*, we have* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$*.*
- ***Unital****: There exists an element* $1 \in G$ *such that for all* $a \in G$*, we have* $1 \cdot a = a \cdot 1 = a$*.*
- ***Invertible****: For every* $a \in G$*, there exists an element* $a^{-1} \in G$ *such that* $a \cdot a^{-1} = a^{-1} \cdot a = 1$*.*

Example 10

- S_n*: The group of all permutations of* n *elements with composition as the operation. For example:*

$$S_3 = \{\textit{identity}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}.$$

- D_n*: The group of symmetries of a regular* n*-sided polygon. For example,* D_5 *is the symmetries of the regular pentagon (consisting of five rotations and five reflections)*

- C_n*: The group of integers modulo* n *under addition, generated by a single element. For example:*

$$C_5 = \{0,1,2,3,4\}, \quad \textit{where } 3+4 = 2 \ (\textit{mod } 5).$$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

- *The collection of field automorphisms of a field forms a group under function composition*

Abel-Ruffini Theorem

Theorem 11 (Abel-Ruffini) *There is not general solution to fifth degree polynomials (and higher) with radicals, addition, and multiplication.*

The proof of this theorem using Galois theory uses the connection between fields and their corresponding groups of automorphisms. The structure of the automorphism group can be used to determine if the field is built out of radical extensions.

References

[1] David S. Dummit and Richard M. Foote. *Abstract algebra*. 3rd ed. New York: Wiley, 2004.