Fields and Galois Theory

MATH 370, YALE UNIVERSITY, SPRING 2019

These are lecture notes for MATH 370b, "Fields and Galois Theory," taught by Asher Auel at Yale University during the spring of 2019. These notes are not official, and have not been proofread by the instructor for the course. They live in my lecture notes respository at

https://github.com/jopetty/lecture-notes/tree/master/MATH-370.

If you find any errors, please open a bug report describing the error and label it with the course identifier, or open a pull request so I can correct it.

Contents

Syllabus

Instructor	Asher Auel, asher.auel@yale.edu
Lecture	TR 11:35 AM – 12:50 PM in LOM 215
Peer Tutor	Arthur Azvolinsky, arthur.azvolinsky@yale.edu
Section	Math Lounge
Exams	Midterm 1: Febuary 19; Midterm 2: April 9; Final: May 3.
Textbook	James S. Milne. *Fields and Galois Theory (v4.60).* 2018

The main object of study in Galois theory are roots of single variable polynomials. Many ancient civilizations (Babylonian, Egyptian, Greek, Chinese, Indian, Persian) knew about the importance of solving quadratic equations. Today, most middle schoolers memorize the "quadratic formula" by heart. While various incomplete methods for solving cubic equations were developed in the ancient world, a general "cubic formula" (as well as a "quartic formula") was not known until the 16th century Italian school. It was conjectured by Gauss, and nearly proven by Ruffini, and then finally by Abel, that the roots of the general quintic polynomial could not be solvable in terms of nested roots. Galois theory provides a satisfactory explanation for this, as well as to the unsolvability (proved independently in the 19th century) of several classical problems concerning compass and straight-edge constructions (e.g., trisecting the angle, doubling the cube, squaring the circle). More generally, Galois theory is all about symmetries of the roots of polynomials. An essential concept is the field extension generated by the roots of a polynomial. The philosophy of Galois theory has also impacted other branches of higher mathematics (Lie groups, topology, number theory, algebraic geometry, differential equations).

This course will provide a rigorous proof-based modern treatment of the main results of field theory and Galois theory. The main topics covered will be irreducibility of polynomials, Gauss's lemma, field extensions, minimal polynomials, separability, field automorphisms, Galois groups and correspondence, constructions with ruler and straight-edge, theory of finite fields. The grading in Math 370 is very focused on precision and correct details. Problem sets will consist of a mix of computational and proof-based problems.

Your final grade for the course will be determined by

$$\max \left\{ \begin{array}{l} 20\% \text{ homework} + 25\% \text{ midterm } 1 + 25\% \text{ midterm } 2 + 30\% \text{ final} \\ 20\% \text{ homework} + 25\% \text{ midterm } 1 + 15\% \text{ midterm } 2 + 40\% \text{ final} \\ 20\% \text{ homework} + 15\% \text{ midterm } 1 + 25\% \text{ midterm } 2 + 40\% \text{ final} \end{array} \right\}.$$

References

[Mil18] James S. Milne. *Fields and Galois Theory (v4.60).* 2018.

1 January 15, 2019

"Daddy, the bears is wubbing his back!"

Noah Auel

Asher's kids came up and they are soooooo cuuuuuuttteeeeee! That's so adorable. He also says that the course is really fun but honestly the kids are by far my favorite part of the course so far. Hi Noah! Sorry your great-grandfather died :(

1.1 What is Galois Theory?

Galois theory is an explanation of a trajectory we started in grade school. We start with the positive integers $\mathbb{Z}_{>0}$ and we learn to make bijections (bijections between apples on the table and positive integers). Then we discovered (or invented) the concept of zero which led us to $\mathbb{N}$. Then we started using negative numbers to arrive at $\mathbb{Z}$, and from there on to $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ and so on. Each jump is necessitated by wanting or needing to solve some kind of equation. Galois theory mainly focuses on that last jump from $\mathbb{R}$ to $\mathbb{C}$.

1.2 Moving from $\mathbb{R}$ to $\mathbb{C}$

We usually think of $\mathbb{C}$ in the presentation of $\mathbb{C} = \mathbb{R}[i] = \{x + iy \mid x, y \in \mathbb{R}\}$. This value i is a root of the equation $x^2 + 1$, one we can't solve with just real numbers. One could ask "what is so special about this polynomial?" Why is i the thing that builds complex numbers? What about $x^2 + x + 1$? That is also rather fundamental, with roots $\omega = (-1 \pm \sqrt{-3})/2$. If you draw the unit circle in the complex plane, these roots divide the circle into three pieces along with $(1, 0)$. We could form an object $\mathbb{R}[\omega]$ and call that the complex numbers. We don't use this construction because $\mathbb{R}[\omega] = \mathbb{C}$, since

$$x + y\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = \left(x - \frac{1}{2}y\right) + \frac{\sqrt{3}}{2}yi,$$

by associativity via the substitution $x' = x - \frac{1}{2}y$ and $y' = \frac{\sqrt{3}}{2}y$. These transformations are always solvable, so the two systems are in fact equivalent.

> **Exercise 1.1.** Let $f : x \mapsto ax^2 + bx + c$ where $a, b, c \in \mathbb{R}$ where $b^2 - 4ac < 0$. Prove that $\mathbb{C} = \mathbb{R}[\alpha]$ where α is a root of f.

But even if you do choose to ordain $x^2 + 1$ as special, there's still nothing special about i since it factors into $(x + i)(x - i)$. Then there are really two roots, $+i$ and $-i$. We have arbitrarily chosen i over $-i$, probably because it was invented by nineteenth century

German mathematicians living in the Northern Hemisphere. Algebraically, there is no way to distinguish between i and $-i$. However moving *between* the roots is special: it's a map $\sigma\colon \mathbb{C} \to \mathbb{C} : x + iy \mapsto x - iy$ called an $\mathbb{R}$-automorphism of $\mathbb{C}$, meaning that restricting σ to $\mathbb{R}$ is the identity. It's also a (unital) ring homomorphism, so $\sigma(z_1 + z_2) = \sigma(z_1) + \sigma(z_2)$ and $\sigma(z_1 \cdot z_2) = \sigma(z_1) \cdot \sigma(z_2)$ and $\sigma(1) = 1$.

There are more such automorphisms! We already saw that we can write complex numbers as $\mathbb{C} = \mathbb{R}[\omega]$. We could create the map $\sigma\colon x + y\omega \mapsto x + y\bar{\omega}$. Notice that all these automorphisms are doing is exchanging the roots of the generating polynomials. We can check that this is in fact a valid automorphism by look at what it does to i.

$$\sigma\colon i = \frac{1}{\sqrt{3}} + \frac{2}{\sqrt{3}}\omega \mapsto \frac{1}{\sqrt{3}} + \frac{2}{\sqrt{3}}\bar{\omega} = -i,$$

so it's actually just complex conjugation! In fact, $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\mathrm{id}_{\mathbb{C}}, \sigma\}$.

Example 1.1. Notice that $|\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})| = 2 = \dim_{\mathbb{R}} \mathbb{C} = [\mathbb{C} : \mathbb{R}]$. We'll be seeing a lot of this later.

This shows that the special part of the complex numbers is not i or ω, but rather complex conjugation. This is actually the defining property of the complex numbers irrespective of how you define them.

Proposition 1.1. *More generally, given a field F and a polynomial $f(x) = ax^2 + bx + c$ for some $a, b, c \in F$ satisfying $f(x)$ has no root in F then there exists a field k with the following properties:*

1. *F is a subfield of k;*
2. *$\dim_F k = [k : F] = 2$;*
3. *$|\mathrm{Aut}_F k| = 2$; and*
4. *the polynomial f is separable which for us means that $b^2 - 4ac \neq 0$. This is called the quadratic extension of F.*

This will lead us to a new σ which will exchange the roots analogously to conjugation. We'll also need that the characteristic of F is not 2, since otherwise the quadratic formula doesn't work since we divide by $2a$. Implicit in the quadratic formula is the statement that $k = F[\sqrt{b^2 - 4ac}]$.

1.3 Going Cubic

We have a similar story for cubic equations where $f(x) = x^3 + px - q$ (the negative is there for historical reasons). This also leads us to the cubic formula. The Babylonians

discovered the quadratic formula, and Italian mathematicians in the 16^{th} century developed the cubic formula,

seriously, just look it up.

because they had these betting games where two mathematicians had to compete to find the roots of a cubic equation. Eventually, a guy named Cardano and his students started winning everything and then one of his students defected to a competitor. The important part is that this formula is a nested formula of certain finitely many operations depending just on the coefficients. There is a similar story for quartic equations.

Theorem 1.1 (Abel-Ruffini)**.** *Given a general polynomial $f \in \mathbb{Q}[x]$ with $\deg(f) \geq 5$, there is no explicit closed form formula for the roots of f only depending on taking nested roots.*

Galois theory is about understanding polynomials by looking at the symmetry of their roots.