Math 418: Abstract Algebra II

Lecture: MWF 1:00-1:50pm
1047 Sidney Lu Mech. Eng. Bldg.

Instructor: Andy Hardt
Computing Applications Bldg. 69B
ahardt@illinois.edu

Textbook: Dummit & Foote, Abstract Algebra, 3rd. Edition

Today: course overview

This is a second course in abstract algebra (after 417)
We will cover three main topics

1) Rings and factorization
2) Field theory & Galois theory
3) Algebraic geometry

leads into

---

1) <u>Ring theory</u> (first two weeks)

Let R be an <u>integral domain</u>: commutative ring with 1 and with no zero-divisors

E.g.: $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$,

$$\mathbb{Z}[\sqrt{\underset{\in \mathbb{Z}}{D}}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}$$

<u>Unit</u>: $x \in R$ s.t. $x^{-1} \in R$ (in $\mathbb{Z}$, ± 1)

<u>Irreducible</u>: if $r = ab$, then a or b is a unit
(in $\mathbb{Z}$, prime #'s, but different for general R)

R has unique factorization if $\forall r \in R$, r can be written

$$r = \underbrace{r_1 \cdots r_k}_{\text{irred.}}$$

and this factorization is unique up to rearrangement & units

E.g.:

a) $R = \mathbb{Z}$

$$6 = 2 \cdot 3 = 3 \cdot 2 = (-2)(-3) = (-3)(-2)$$

b) $R = \mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$

$$6 = (1+i)(1-i) \cdot 3 = \underbrace{\cdots}_{\text{rearrangements \& units}}$$

c) $R = \mathbb{Z}[\sqrt{-5}]$

$$6 = \underbrace{2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})}_{\text{all irred! (see h/w)}}$$

---

2) Galois theory (bulk of the course)

Arose from attempts to solve one of the most classical problems, the solution of polynomial eqns. by radicals

Quadratic formula (antiquity): $ax^2+bx+c=0$ has sol'ns

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

Cubic formula (Cardano? 1545): x^3+px+q has sol'ns

$$x = \sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}$$

for compatible choices of the cube roots

Quartic formula (Ferrari, 1540)
(relies on cubic formula)

What about the quintic equation?

$$x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$$

Thm (Ruffini 1799, Abel 1824): There is no (general) "quintic formula" by radicals.

Galois (1830): New, far-reaching proof of Abel-Ruffini

- Provides specific polys that are not solvable by radicals

Main idea: stop asking <u>what</u> the roots are and start asking <u>where</u> they live?

Def: A <u>field extension</u> E/F is a pair of fields $F \subseteq E$.

Def: The <u>splitting field</u> of a poly. p w/ coeffs. in F is the "smallest" ext. field E of F containing all roots of p.

Fundamental Thm. of Galois Theory: In this setting, $\exists$ a group called the Galois group of p whose structure gives detailed information about E/F, and thus p.

Galois' proof of Abel-Ruffini:

- p is solvable by radicals $\leftrightarrow$ $\mathrm{Gal}(p)$ is a solvable gp.
- There exist (many) polys. w/ Galois gp. S_n
- S_n is not solvable for $n \geq 5$

<u>3) Algebraic geometry</u> (last few weeks)

Study of <u>shape</u> of sol'ns to (multivar.) poly. eqns. (over $\mathbb{C}$)

E.g.: Want to study sol'ns of $xy + xz = 1$

Can either study

I = ideal in $\mathbb{C}[x,y,z]$ generated by $xy + xz - 1$

or

$V = \{(x,y,z) \in \mathbb{C}^3 \mid xy + xz = 1\} \subseteq \mathbb{C}^3$

Hilbert's Nullstellensatz: There is a direct correspondence between these two approaches.