Template

Sam Lowe

October 27, 2021

Contents

1 Section 1

Lecture 1

Motivation: how do we solve polynomials? In solving the polynomial $9x^2 - 4 = 0$, we can add, subtract, multiply, divide, and take roots.

Field extension

The solution to our polynomial came in pairs; $\pm 2/3$. Notice the symmetry that these roots come in pairs.

Q sits inside R which sits inside C. However, "between" Q and R, we have $\mathbb{Q}(\sqrt{2})$. We can also thing of the field $\mathbb{Q}(i)$ as sitting between Q and C.

In general, we can solve quadratics with the quadratic formula

$$x = \frac{-b \pm \sqrt{\Delta}}{2a}$$

where $\Delta = b^2 - 4ac$. Notice that again we have symmetry that interchanges these two square roots.

Degree 2 polynomials are solvable in radicals; all we have to do in addition to solving degree 2 polynomial equations over a field, we only have to include additional numbers - roots - of the form $\sqrt{b^2 - 4ac}$. Here, we're including *roots of numbers that we already have.*

Cardano: $x^3 + px + q = 0$

$$\sqrt[3]{\alpha + \sqrt{\beta}} + \sqrt[3]{\alpha - \sqrt{\beta}}$$

where $\alpha = \frac{-q}{2}$ and $\beta = \frac{q^2}{4} + \frac{p^3}{27}$.

Theorem (Abel-Ruffini) For any $n \geq 5$ there is a polynomial of degree n that is not solvable in radicals.

One example is $x^5 - x - 1 = 0$.

This theorem does **not** say there are no solutions, or that no polynomials of degree 5 or greater cannot be solved by radicals. It only says that those roots do not conform to a certain form.

The idea behind this proof is:

1. Solvability in radicals means that we give ourselves ("pass to a field extension") a finite sequence of nth roots. For example, in the quadratic example, we went from $\mathbb{Q} \to \mathbb{Q}(\sqrt{\Delta})$. In the cubic example, we went from $\mathbb{Q} \to \mathbb{Q}(\sqrt{\beta}) \to \mathbb{Q}(\sqrt{\beta}, \sqrt{\alpha})$
2. These roots have symmetries: $\sqrt{\Delta} \to -\sqrt{\Delta}$, or $\sqrt[3]{\alpha + \sqrt{\beta}} \to \sqrt[3]{\alpha + \sqrt{\beta}}e^{2\pi i/3}$ (note the third root of unity!)
3. So we can show that a polynomial is not solvable in radicals by showing that the symmetries of its roots are not of this iterated, cyclic nature.

A **ring** is a set R equipped with two binary operations, denoted $(a, b) \to a+b$ (addition) and $(a, b) \to a \times b = a \cdot b = ab$ (multiplication).

Both of these operations are associative $a(bc) = (ab)c$ and unital ($a + 0 = a$, $1 \times a = a \times 1 = a$).

Addition is commutative and has inverses; $a + b = b + a$ and $a + (-a) = 0$.

Multiplication distributes over addition on both sides $c(a + b) = (a + b)c = ac + bc$.

A ring R is called commutative if its multiplication operation is commutative.

Examples:

$\mathbb{Z}$ is a ring with the usual addition and multiplication.

$\mathbb{Z}/n\mathbb{Z}$ is a ring with addition mod n and multiplication mod n. ($a \equiv bmodn$ if $n \mid b - a$)

Exercise: these are well-defined and make $\mathbb{Z}/n\mathbb{Z}$ a ring.

Example: $\mathbb{Z}/1\mathbb{Z}$ is the singleton ring.

Exercise: $0r = 0$ for all $r \in R$, R a ring, implies that $0 = 1$ iff $R = \{0\}$.

Example: $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$

Example: $\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$

Example: $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 4\}$

Interestingly, in $\mathbb{Z}/4\mathbb{Z}$, $2 \times 2 = 0$, so it fails to have multiplicative inverses.

A commutative ring with $0 \neq 1$ is a field if it has multiplicative inverses for nonzero elements. $\mathbb{Z}, \{0\}$, and $\mathbb{Z}/4\mathbb{Z}$ fail to be fields.

$\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields.

The set $M_n(\mathbb{R})$ of $n \times n$ matrices a non-commutative ring for $n \geq 2$ under entrywise addition and standard matrix multiplication. (The entries can come from any set, not just from $\mathbb{R}$.)

Proposition $\mathbb{Z}/n\mathbb{Z}$ is a field iff n is prime.

Lemma Given $m \in \mathbb{Z}$, $\overline{m}$ has a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$ if and only if m and n are relatively prime.

In a field, $ab = 0$ if and only if a or b is 0.

Conversely, if m and n are relatively prime, then $rm + sn = 1$ for some integers r and s (Bézout's identity), so $rm \equiv 1 mod n$, i.e. $\overline{r} \cdot \overline{m} = 1$.

Example $F_4 = \{0, 1, \omega, \overline{\omega}\}$

$1, \omega, \overline{\omega}$, are roots of $x^3 - 1$.