Motivation and Introduction

Main purpose of this course is to study Galois theory — a field that arose in trying to study roots of polynomials.

Consider $f(x) = ax^2 + bx + c$. If we want to find a general, closed-form expression for the roots of the function, we complete the square.

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

We found these roots by by the coefficients, $\mathbb{Q}$, addition, subtraction, multiplication, division, and square root (raising to the 1/2 power: see Math 310 notes, Page 104). Naturally, this leads us to ask whether we can do this for cubic polynomials with the same operations. Obviously, we have to change from 1/2 power to the 1/3 power, but Cardano showed that it was possible to solve a cubic and quartic equation using these traditional operations and radicals.

Évariste Galois invented his theory to prove there is no such closed formula by radicals for any polynomial of degree 5 or above.

For example, $x^5 - x + 1$ does not have roots given by radicals.

Example: A Solvable Polynomial

Consider the polynomial $f(x) = x^2 - 2$. We know that the roots of this polynomial are $\pm\sqrt{2}$. From this, we want to create a set $K(f)$ that satisfies the following rules:

- $\mathbb{Q} \subseteq K(f)$.
- $K(f)$ must contain the roots of f.
- $K(f)$ must be closed under the traditional operations: $+, -, \times, /$
- $K(f)$ must be the smallest field that satisfies the above three requirements.

Claim: $K(f) = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

- $\mathbb{Q} \subseteq K(f)$, because we can set $b = 0$.
- $\sqrt{2} = 0 + (1)(\sqrt{2})$, $-\sqrt{2} = 0 + (-1)(\sqrt{2})$
- Let $a + b\sqrt{2}$ and $c + d\sqrt{2}$ be elements of $K(f)$. Then,
  - $(a + b\sqrt{2}) \pm (c + d\sqrt{2}) = (a \pm c) + (b \pm d)\sqrt{2}$
  - $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$
  - Set $c + d\sqrt{2} \neq 0$

$$\begin{aligned}\frac{a + b\sqrt{2}}{c + d\sqrt{2}} &= \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{c^2 - 2d^2}\\ &= \frac{1}{c^2 - 2d^2}\left((ac - 2bd) + (bc - ad)\sqrt{2}\right)\\ &= \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2}\sqrt{2}\end{aligned}$$

- $K(f)$ is indeed the smallest set.
  - Note that $K(f)$ is a $\mathbb{Q}$-vector space, with basis $\{1, \sqrt{2}\}$. Therefore, $\dim_{\mathbb{Q}} K(f) = 2$. $K(f)$ is known as the "splitting field" of f.

We want to consider a bijective function $\varphi : K(f) \to K(f)$ with the following properties:

- $\varphi(r) = r$ for every $r \in \mathbb{Q}$
- $\varphi(x + y) = \varphi(x) + \varphi(y)$
- $\varphi(xy) = \varphi(x)\varphi(y)$

We denote the collection of all such φ as $\text{Aut}(K(f)/\mathbb{Q})$. This is a group under the operation $\circ$ (composition). Specifically, we have

$$\begin{aligned}\varphi(a + b\sqrt{2}) &= \varphi(a) + \varphi(b)\varphi(\sqrt{2})\\ &= a + b\varphi(\sqrt{2}).\end{aligned}$$

Notice

$$\begin{aligned}\left(\varphi(\sqrt{2})\right)^2 - 2 &= \varphi\left(\left(\sqrt{2}\right)^2 - 2\right)\\ &= \varphi(0)\\ &= 0.\end{aligned}$$

Therefore, $\varphi(\sqrt{2}) = \pm\sqrt{2}$. Therefore, we have that the elements of $\text{Aut}(K(f)/\mathbb{Q})$ as the following:

$$\begin{aligned}\varphi_0 &: a + b\sqrt{2} \mapsto a + b\sqrt{2}\\ \varphi_1 &: a + b\sqrt{2} \mapsto a - b\sqrt{2}\\ \varphi_1 \circ \varphi_1 &= \varphi_0\end{aligned}$$

Thus,

$$\begin{aligned}\text{Aut}(K(f)/\mathbb{Q}) &= \{\varphi_0, \varphi_1\}\\ &\cong \mathbb{Z}/2\mathbb{Z}\end{aligned}$$

Example: A Harder Polynomial

Let $f(x) = (x^2 - 2)(x^2 - 3)$. Our roots are $\{\pm\sqrt{2}, \pm\sqrt{3}\}$. We want to form $K(f)$ with the same properties. Let

$$\begin{aligned}K(f) &= \mathbb{Q}(\sqrt{2}, \sqrt{3})\\ &= \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}.\end{aligned}$$

Just as with our previous example, $K(f)$ is a vector space over $\mathbb{Q}$, with basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$, so $\dim_{\mathbb{Q}} K(f) = 4$.

Now, we want $\text{Aut}(K(f)/\mathbb{Q})$. If $\varphi \in \text{Aut}(K(f)/\mathbb{Q})$, then

$$\begin{aligned}\varphi(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a + b\varphi(\sqrt{2}) + c\varphi(\sqrt{3}) + d\varphi(\sqrt{6})\\ &= a + b\varphi(\sqrt{2}) + c\varphi(\sqrt{3}) + d\varphi(\sqrt{2})\varphi(\sqrt{3}).\end{aligned}$$

Thus, we need to know $\varphi(\sqrt{2})$ and $\varphi(\sqrt{3})$. So,

$$\begin{aligned}f(\varphi(\sqrt{2})) &= \left(\left(\varphi(\sqrt{2})\right)^2 - 2\right)\left(\left(\varphi(\sqrt{2})\right)^2 - 3\right)\\ &= 0\end{aligned}$$

and the same is the case with $\varphi(\sqrt{3})$. So,

$$\begin{aligned}\varphi(\sqrt{2}) &\in \{\pm\sqrt{2}, \pm\sqrt{3}\}\\ \varphi(\sqrt{3}) &\in \{\pm\sqrt{2}, \pm\sqrt{3}\}.\end{aligned}$$

Suppose $\varphi(\sqrt{2}) = \sqrt{3}$. Then,

$$\begin{aligned}\left(\left(\varphi(\sqrt{2})\right)^2\right) &= (\sqrt{3}^2 - 1)\\ &= 0\\ &= (\varphi(2) - 3)\\ &= -1. \perp\end{aligned}$$

Thus,

$$\begin{aligned}\varphi(\sqrt{2}) &\in \{\pm\sqrt{2}\}\\ \varphi(\sqrt{3}) &\in \{\pm\sqrt{3}\},\end{aligned}$$

and we have the maps as:

$$\begin{aligned}\varphi_0 &: \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto \sqrt{3}\\ \varphi_1 &: \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto \sqrt{3}\\ \varphi_2 &: \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}\\ \varphi_3 &: \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}\end{aligned}$$

Example: A Cubic Polynomial

Consider the function $f(x) = x^3 - 2$. The function has one real root, $r_1 = \sqrt[3]{2}$, and two complex roots. Let's examine $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$; r_2 and r_3 are not in $Q(\sqrt[3]{2})$. We could instead consider $\mathbb{Q}(\sqrt[3]{2}, r_1, r_2)$.

$$\begin{aligned}x^3 - 2 &= (x - r_1)(x^2 + r_1 x + r_1^2)\\ r_2 &= \frac{-r_1 + \sqrt{r_1^2 - 4r_1^2}}{2}\\ &= r_1\frac{-1 + \sqrt{-3}}{2}\\ &= r_1\zeta_3\\ r_3 &= r_1\frac{-1 - \sqrt{-3}}{2}\\ &= r_1\zeta_3^2\end{aligned}$$

However, including r_2 and r_3 is excessive — all we need is $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Therefore, the basis of this vector space is $\{1, r_1, r_1^2, \zeta_3, \zeta_3 r_1, \zeta_3 r_1^2\}$ (note that $\zeta_3^2 = -1 - \zeta_3$). Therefore, $\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2}, \zeta_3) = 6$, and $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) = K(f)$.Additionally, we have $\operatorname{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\varphi_0\}$, but $\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2}) = 3$. For the full field extension, we need to find $\varphi(\sqrt[3]{2})$ and $\varphi(\zeta_3)$.

$$\begin{aligned}\varphi(\sqrt[3]{2}) &\in \{r_1, \zeta_3 r_1, \zeta_3^2 r_1\}\\ \varphi(\zeta) &\in \{\zeta_3, \zeta_3^2\}\\ \varphi_0 &: r_1 \mapsto r_1, \zeta_3 \mapsto \zeta_3\\ \varphi_1 &: r_1 \mapsto \zeta_3 r_1, \zeta_3 \mapsto \zeta_3\\ \varphi_2 &: r_1 \mapsto r_1, \zeta_3 \mapsto \zeta_3^2\\ \varphi_3 &: r_1 \mapsto \zeta_3^2 r_1, \zeta_3 \mapsto \zeta_3\\ \varphi_4 &: r_1 \mapsto \zeta_3 r_1, \zeta_3 \mapsto \zeta_3^2\\ \varphi_5 &: r_1 \mapsto \zeta_3^2 r_1, \zeta_3 \mapsto \zeta_3^2\end{aligned}$$

Therefore,

$$\begin{aligned}\text{Aut}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) &= 6\\ &= \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{}, \sqrt[3]{2})\end{aligned}$$

Rings

Consider the integers under the normal operations, $(\mathbb{Z}, +, \cdot)$; this will serve as the motivation for rings in the future.

Definition of a Ring

Let R be a nonempty set with operations $(+, \cdot)$, with the following properties:

(1) $(R, +)$ is an abelian group:

- Closed: $r_1 + r_2 \in R,\ \forall r_1, r_2 \in R$
- Identity: $\exists 0_R,\ r + 0_R = 0_R + r = r$
- Associativity: $r_1 + (r_2 + r_3) = (r_1 + r_2) + r_3$
- Inverse: $\forall r \in R,\ \exists -r \in R, r + (-r) = 0_R$
- Commutativity: $r_1 + r_2 = r_2 + r_1$

(2) Closure under Multiplication: $r_1 \cdot r_2 \in R,\ \forall r_1, r_2 \in R$

(3) Associativity under Multiplication: $r_1 \cdot (r_2 \cdot r_3) = (r_1 \cdot r_2) \cdot r_3$

(4) Distributivity: $r_1 \cdot (r_2 + r_3) = r_1 \cdot r_2 + r_2 \cdot r_3, (r_1 + r_2) \cdot r_3 = r_1 \cdot r_3 + r_2 \cdot r_3$

We say $(R, +, \cdot)$ is a ring if it satisfies all these properties.

If $\exists 1_R \in R$ such that $r \cdot 1_R = 1_R \cdot r = r$, then we say R is a ring with identity, and 1_R is the multiplicative identity. If multiplication is commutative, then R is known as a commutative ring.

Examples

(1) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are commutative rings with identity value of 1.

(2) $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is a commutative ring with identity $1_R = [1]_n$.

(3) $(\mathbb{R}[x], +, \cdot)$, where $\mathbb{R}[x] = \left\{ \sum_{i=0}^{n} a_i x^i \mid a_i \in \mathbb{R} \right\}$, is a commutative ring with identity.

(4) $(2\mathbb{Z}, +, \cdot)$ is a commutative ring *without* identity.

(5) $(\text{Mat}_n(\mathbb{R}), +, \cdot)$, where $\text{Mat}_n(\mathbb{R})$ refers to $n \times n$ matrices with real entries, is a *non*commutative ring with identity.

Division Rings and Fields

Let R be a ring with identity. We say R is a *division ring* if $\forall r \in R \setminus \{0_R\}$, $\exists r^{-1} \in R$ with $r \cdot r^{-1} = 1_R = r^{-1} \cdot r$. If R is also commutative, then R is a *field*.

Examples

(1) $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, and $(\mathbb{C},+,\cdot)$ are all fields.

(2) Let p be prime, and set $F=\mathbb{Z}/p\mathbb{Z}$. Then, F is a field; we denote this $\mathbb{F}_p$.

(3) Define

$$\mathbb{H}=\{a+bi+cj+dk \mid a,b,c,d\in\mathbb{R}, i^2=j^2=k^2=-1, ij=k=-ji, jk=i=-kj, ki=j=-ik\}.$$

Then, $\mathbb{H}$ is a division ring, known as the Hamiltonian quaternions. Note that $\mathbb{C}\subset\mathbb{H}$.

Properties of Rings

Proposition 4.1: Let R be a ring.

(1) $0_R a = a0_r = 0\ \forall a\in R$
(2) $(-a)b=a(-b)=-(ab)\ \forall a,b\in R$
(3) $(-a)(-b)=ab\ \forall a,b\in R$
(4) If $\exists 1_R\in R$, then 1_R is unique, and $-a=(-1_R)a$.

Proof of (1): Let $a\in R$. Then,

$$\begin{aligned} 0_R a &= (0_R+0_R)a && \text{Additive Inverse}\\ 0_R a &= 0_R a + 0_R a && \text{Distributivity}\\ 0_R a + (-0_R a) &= 0_R a + 0_R a(-0_R a) &&\\ 0_R &= 0_R a. && \text{Additive Inverse}\end{aligned}$$

Proof of (2): Let $a,b\in R$. Note that $-(ab)$ is the unique inverse such that $ab+(-(ab))=0_R$ via group theory. We have

$$\begin{aligned} ab+(-a)b &= (a+(-a))b && \text{Distributivity}\\ &= (0_R)b && \text{Additive Inverse}\\ &= 0_R. && \text{By Property (1)}\end{aligned}$$

Thus, $(-a)b=-(ab)$.

Zero Divisor and Units in Rings

Let $a\in R$, $a\neq 0_R$. If $\exists b\in R$ with $b\neq 0_R$ such that $ab=0_R=ba$, then we say a is a zero divisor.

If $1_R\in R$, we say $u\in R$ is a unit if $\exists v\in R$ (can be equal to u) with $uv=1_R=vu$. The collection of units in R is denoted $R^\times$.

Exercise: Show that $R^\times$ is a group under multiplication.

Examples

(1) Let $R=\mathbb{Z}/6\mathbb{Z}$. Note that $[2]_6[3]_6=[6]_6=[0]_6$, so both $[2]_6$ and $[3]_6$ are both zero divisors. Additionally, $[4]_6[3]_6=[6]_6=[0]_6$. Meanwhile, since $(\mathbb{Z}/6\mathbb{Z})^\times=\{[1]_6,[5]_6\}$, those are the two units of $\mathbb{Z}/6\mathbb{Z}$.

(2) $\mathbb{Z}$ has no zero divisors. $\mathbb{Z}^\times=\{\pm 1\}$.

(3) $\mathbb{Q}$ has no zero divisors. $\mathbb{Q}^\times=\mathbb{Q}\setminus\{0\}$.

(4) $\mathbb{Z}[i]=\{a+bi\mid a,b\in\mathbb{Z}, i^2=-1\}$ has no zero divisors (as $\mathbb{C}$ is a field). $\mathbb{Z}[i]^\times=\{\pm 1,\pm i\}$.

Subrings

Let $(R, +, \times)$. If $S \subseteq R$ is a nonempty subset, and $(S, +, \cdot)$ is a ring, then S is a subring of R. To see S is a subring, it is enough to show:

- $S \neq \emptyset$.
- S is closed under subtraction.
- S is closed under multiplication of elements in S.

Examples

(1)

$$\underbrace{\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}}_{\text{subrings}}$$

(2) $\mathbb{R} \subseteq \mathbb{R}[x]$ is a subring.

(3) $S = \{[0]_4, [2]_4\} \subseteq \mathbb{Z}/4\mathbb{Z}$ is a subring.

Integral Domains

Let R be a commutative ring with identity. We say R is an integral domain if R has no zero divisors.

Examples

(1) $\mathbb{Z}$, the integers, is an integral domain, that is not a field.

(2) All fields are integral domains.

(3) $\mathbb{Z}/6\mathbb{Z}$ is *not* an integral domain, as it has zero divisors.

(4) $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain if n is composite.

Integral domains are nice due to allowance of cancellations. For example, if $2m = 2n$ in $\mathbb{Z}$, then we find $2(m - n) = 0$, and since $\mathbb{Z}$ has no zero divisors, it must be the case that $m = n$.

However, in a ring that is not an integral domain, such as $\mathbb{Z}/6\mathbb{Z}$, we cannot use the same technique to find the solution to a similar equation. For example, $3 \cdot 2 = 0 = 3 \cdot 4$, but $2 \neq 4$.

Proposition: Equations in Integral Domains

Let R be an integral domain. If $a, b, c \in R$ with $a \neq 0_R$, and $ab = ac$, then $b = c$.

Proof:

$$\begin{aligned} ab &= ac \\ a(b - c) &= 0_R \end{aligned}$$

Since $a \neq 0$,

$$\begin{aligned} b - c &= 0_R \\ b &= c. \end{aligned}$$

Theorem: Finite Integral Domains and Fields

If R is an integral domain, and $\text{card}(R) < \infty$,then R is a field.

Proof: Let $a \in R$, $a \neq 0_R$. Note $ab \neq 0_R$ for all $b \in R$, $b \neq 0_R$.

Define $\varphi_a : R \setminus \{0_R\} \to R \setminus \{0_R\}$, $b \mapsto ab$. If $\varphi_a(b) = \varphi_a(c)$, then $ab = ac$, and by our previous result, $b = c$ — therefore, φ_a is injective.

Since $R \setminus \{0_R\}$ is finite, and φ_a is injective, then φ_a is surjective. In particular, this means $\exists b \in R \setminus \{0_R\}$ with $\varphi_a(b) = 1_R$; therefore, $ab = 1_R$. Since R is commutative, $ba = 1_R$, so $b = a^{-1}$.