Galois Theory

Alec Zabel-Mena

<u>Text</u>

Gaois Theory (4^{th} edition)

Ian Stewart

September 18, 2020

Chapter 1

Classical Algebra.

1.1 Complex Numbers

Definition. A **Complex Number** is a pair (x, y) of real numbers together with binary operations $+$, $\cdot$ such that for $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$ and $(x_1, y_1)(x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_2)$, together with the relation $i^2 = (-1, 0)$. We denote the set of all complex numbers as $\mathbb{C}$.

Defining $(x, 0)$ as the real number x, we see that $\mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{R}^2$, moreover, defining $i = (0, 1)$, we see that $i^2 = (-1, 0) \in \mathbb{R}$. We can then define the pair $(x, y) \in \mathbb{C}$ as having the form $x + iy$, where $i^2 = -1$.

1.2 Subrings and Subfields of $\mathbb{C}$.

We restrict our notion of "subrings" and "subfields" to those concerning $\mathbb{R}$ and $\mathbb{C}$.

Definition. A **subring** of $\mathbb{C}$ is a nonempty set $R \subseteq \mathbb{C}$ such that $1 \in R$, and if $x, y \in R$ then $x + y, -x \in R$ and $xy \in R$.

Definition. A **subfield** of $\mathbb{C}$ is a subring $K \subseteq \mathbb{C}$ such that if $x \in K$ then $x^{-1} \in K$.

Since, we are talking about subrings and subfields in the sense of $\mathbb{R}$ and $\mathbb{C}$, then we denote x^{-1} to be $\frac{1}{x}$.

Example 1.1. (1) The set $\mathbb{Z}[i] \subseteq \mathbb{C}$ of all pairs of integers (a, b) of the form $a + ib$ is a subring of $\mathbb{C}$ but not a subfield. We call this set the **Gaussian integers**.

(2) The set $\mathbb{Q}[i] \subseteq \mathbb{C}$ of all pairs of rational numbers (p, q) of the form $a + ib$ forms not only a subring of $\mathbb{C}$, but also a subfield.

(3) The set $P[\pi]$ of all polynomials in π with rational coefficients is a subring of $\mathbb{C}$, but not a subfield.

(4) The set $\mathbb{Q}(\pi)$ of all rational expressions in π, $\frac{p(\pi)}{q(\pi)}$ (with $q(\pi) \neq 0$) with rational coeffients is a subfield of $\mathbb{C}$.

(5) The set $2\mathbb{Z}$ of all even integers is not a subring of $\mathbb{C}$.

(6) The set $\mathbb{Q}[\sqrt[3]{2}]$ of all pairs of rationla numbers (a, b) of the form $a + b\sqrt[3]{2}$ does not form a subring of $\mathbb{C}$ since it is not closed under $\cdot$. It is closed however under $+$.

Definition. Let K and L be subfields of $\mathbb{C}$. An **isomorphism** between K and L is a $1-1$ mapping $\phi : K \to L$ from K onto L such that $\phi(x + y) = \phi(x) + \phi(y)$ and $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in K$.

Proposition 1.2.1. *If $\phi : K \to L$ is an isomorphism, then:*

(1) $\phi(0) = 0$.

(2) $\phi(1) = 1$.

(3) $\phi(-x) = -\phi(x)$.

(4) $\phi(x^{-1}) = \phi(x)^{-1}$

Proof. (1) We have $0x = 0$ for all $x \in K$, so $\phi(0x) = \phi(0)\phi(x) = \phi(0)$. Let $\phi^{-1}(0) = x$, so $\phi(0)\phi^{-1}(0) = \phi\phi^{-1}(0) = 0$.

(2) This is esentially the same proof as (1), but with 1 instead of 0.

(3) We have that $x + (-x) = 0$, so $\phi(x + (-x)) = \phi(x) + \phi(-x) = \phi(0) = 0$, hence we get that $\phi(-x) = -\phi(x)$.

(4) This proof is analogous to that of (3).

∎

If $\phi : K \to L$ is $1 - 1$, but not necesarrily onto, then we call it a **monomorphism**. If $L = K$, then we call ϕ an **automorphism**.

Definition. A **primitive n-th root of unity** is an n-th root of 1 that is not an m-th root of 1 for any proper divisor m of n.

Example 1.2. We have that i is a 4th root of unity, as $i^4 = (i^2)^2 = (-1)^2 = 1$. The number $\zeta_n = e^{2i\pi/n}$ is also an nth root of unity.

Proposition 1.2.2. *Let $_n = e^{2i\pi/n}$, then ζ_n^k is a primitive nth root of unity if and only if* $\gcd(k, n) = 1$.

Proof. We prove the contrapositive of this proposition. Suppose that ζ_n^k is not a primitive nth root of unity, then $(\zeta_n^k)^m = 1$ for some n such that $n = mr$. Then $\zeta_n^{km} = 1 = \zeta_n^n$, hence $n = mr|kr$, therefore $r|k$, and since $r|n$, then $\gcd(k, n) \geq r > 1$ (by definition of the greatest common divisor).

Now suppose that $\gcd(k, n) = r > 1$. Then $n = mr$ for some $m \in \mathbb{Z}$, and $n = mr|km$ for some k. Thus we get that $(\zeta_n^k)^m = \zeta_n^{km} = 1$, therefore, ζ_n^k is not a primitive nth root of unity. ∎

Example 1.3. (1) textbfcomplex conjugation defined as the mapping $(x, y) \to (x, -y)$ (that is, $x + iy \to x - iy$) is an automorphism from $\mathbb{C}$ onto $\mathbb{C}$.

(2) Let $\mathbb{Q}[\sqrt{2}]$ be the set of all pairs of (p, q) rational numbers of the form $p + q\sqrt{2}$. Then $\mathbb{Q}[\sqrt{2}]$ is a subfield of $\mathbb{C}$. The map $p + q\sqrt{2} \to p - q\sqrt{2}$ is an automorphism from $\mathbb{Q}[\sqrt{2}]$ onto itself.

(3) Lel $\alpha = \sqrt[3]{2}$ and let $\omega = \frac{1}{2} + i\frac{\sqrt{3}}{2}$ be a primitive cube root of unity in $\mathbb{C}$. Then the set of all $\mathbb{Q}[\alpha]$ triples of rational numbers (p, q, r) of the form $p + q\alpha + r\alpha^2$ is a subfield of $\mathbb{C}$. The map $p + q\alpha + r\alpha^2 \to p + q\omega\alpha + r\omega\alpha^2$ is an monomorphism onto its image, but not an automorphism.

1.3 Solving Equations.