Algebraic Numbers I: Single Extensions

February 25, 2022 12:15 PM

A complex number α is an algebraic number if $\exists\ p(z) \in \mathbb{Q}[z]$ s.t. $p \neq 0$ and $p(\alpha) = 0$.

E.g. $\alpha = \sqrt{2}$ $\quad p(z) = 1 \cdot z^2 - 2$ $\quad 2z^2 - 4$ $\quad 1 \cdot z^3 - 2z$

Let $m(z) \in \mathbb{Q}[z]$ be non-zero, monic, of least degree s.t. $m(\alpha) = 0$.

Lemma. $m(z)$ is unique and irreducible over $\mathbb{Q}$.

We call $m(z)$ the minimal polynomial for α.

Given $\alpha = 1 + \sqrt{2}$ how do we compute $m(z)$?

Suppose $m(z) = 1 \cdot z + a \in \mathbb{Q}[z]$.

$m(\alpha) = 0 \Rightarrow 1 + \sqrt{2} + a = 0 \Rightarrow a = -1 - \sqrt{2} \notin \mathbb{Q}$.

Suppose $m(z) = 1 \cdot z^2 + az + b$ where $a, b \in \mathbb{Q}$.

$m(\alpha) = 0 \Rightarrow (1+\sqrt{2})^2 + a(1+\sqrt{2}) + b = 0$

$\Rightarrow 1 + 2\sqrt{2} + 2 + a + \sqrt{2}a + b = 0$

$\Rightarrow \sqrt{2}(2+a) + 3 + a + b = 0$

$a = -2 \Rightarrow b = -1$.

$\Rightarrow m(z) = z^2 - 2z - 1$.

Ex. Find the min. poly. for $\alpha = \sqrt{2} + \sqrt{3} + 1$.

$m(z) = 1 \cdot z^4 + az^3 + bz^2 + cz + d \in \mathbb{Q}[z]$.

Def. Algebraic number field.

Let α, β be algebraic numbers.

$\mathbb{Q}(\alpha)$ is the smallest field containing $\mathbb{Q}$ and α.

$\mathbb{Q}(\alpha, \beta)$ is " " " " " " α and β.

Eg. $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{2}) \subsetneq \mathbb{Q}(\sqrt{2}, \sqrt{3})$

Quotient rings. Let $m \in \mathbb{Q}[z]$ be non-zero with degree $d = \deg(m)$.

↙ Quotient ring.

Quotient rings. Let $m \in \mathbb{Q}[z]$ be non-zero with degree $d = \deg(m)$.

Quotient ring.

Recall that $\mathbb{Q}[z]/m = \{ [\sum_{i=0}^{d-1} a_i z^i] : a_i \in \mathbb{Q} \}$.

$[a] \pm [b] = [a \pm b]$

$[a] \cdot [b] = [a \cdot b \bmod m(z)]$

Theorem: $\mathbb{Q}[z]/m(z)$ is a field $\Leftrightarrow$ $m(z)$ is irreducible over $\mathbb{Q}$.

$[a]^{-1}$ — deg $a < d$; irreducible of degree d

Solve $s \cdot a + t m = \gcd(a, m) = 1$ in $\mathbb{Q}[z]$

$\Rightarrow [s \cdot a + t \cdot m] = [1]$

$\Rightarrow [s] \cdot [a] + [t] \cdot [m] = [1] \Rightarrow [s] \cdot [a] = [1]$ ($[m] = [0]$)

$[s] = [a]^{-1}$

Recall $[a] = \{ f : f \equiv a \bmod m \text{ i.e. } m \mid f - a \}$

E.g. $[0] = \{ m, 0, \dots \}$

Computing with algebraic numbers

Let α be an alg. num. with min. poly. $m(z)$.

Theorem $\mathbb{Q}(\alpha) \cong \mathbb{Q}[z]/m(z)$ with $\varphi(\alpha) = [z]$.

E.g. $\alpha = \sqrt{2}$, $m = z^2 - 2$

$\sqrt{2} \cdot (\sqrt{2}+1) \longrightarrow 2 + \sqrt{2}$

$\varphi \downarrow$ $\uparrow \varphi^{-1}$

$[z] \cdot [z+1] = [z \cdot (z+1)]$

$= [z^2 + z \bmod z^2 - 2] = [2 + z]$

The Cyclotomic number fields.

Let $\omega \in \mathbb{C}$ be a root of $x^n - 1$ s.t. $\omega^k \neq 1$ for $0 < k < n$.

[ω is a primitive n'th root of unity].

Let $\omega \in \mathbb{C}$ be a root of $x^n - 1$ s.t. $\omega \neq 1$ for $n > 1$.
[ω is a primitive n'th root of unity].
Let $M_\omega(z)$ be the min. poly. for ω.

n	x^n-1	ω	$M_\omega(x)$	$\deg M_\omega(x)$
1	$x-1$	1	$x-1$.	1
2	$x^2-1 = (x-1)(x+1)$	-1.	$x+1$	1
3	$x^3-1 = (x-1)(x^2+x+1)$	$-\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$	x^2+x+1	2
4	$x^4-1 = (x^2-1)(x^2+1)$	$\pm i$	x^2+1	2
5	$x^5-1 = (x-1)(x^4+x^3+x^2+x+1)$	___	$x^4+x^3+x^2+x+1$	4
6	$x^6-1 = (x^3-1)(x^3+1)$ $= (x^3-1)(x+1)(x^2-x+1)$	$+\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$	x^2-x+1	2.

The min poly $M_\omega(x)$ is called the n'th cyclotomic polynomial $\Phi_n(x)$. Notice $\deg \Phi_n(x) = \phi(n)$.
$\phi(n) = \#\{ a : 1 \le a \le n \text{ and } \gcd(a,n) = 1 \}$.

Ex. Let $\omega^5 = 1$ $\quad M_\omega(z) = z^4+z^3+z^2+z^1+1$. $\quad \mathbb{Q}(\omega)$.
$\downarrow$
$\mathbb{Q}[z]/M_\omega(z)$.

Solve $\{ \omega x + \omega y = 1,\ \omega^3 x + \omega^4 y = -1 \}$.

$\times \omega^4$ $\quad \omega^5 x + \omega^5 y = \omega^4 \quad \omega^5 x + \omega^6 y = -\omega^2$

(1) $1 \cdot x + 1 \cdot y = \omega^4$ (2) $1 \cdot x + \omega \cdot y = -\omega^2$

(1)−(2) $\quad 1 \cdot y - \omega y = \omega^4 + \omega^2$

$(1-\omega)y = \omega^4 + \omega^2$

$(1-\omega)^{-1} \stackrel{?}{=}$ $\quad$ Solve $s(1-z) + t \cdot (1 + z + z^2 + z^3 + z^4) = 1$.