Algebraic Numbers

November 11, 2023 10:25 PM

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

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

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

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

Proof. Exercise. $\quad m_1(z), m_2(z) \quad m_1(z) = 1 \cdot m_2(z) + r(z)$.

We call $m(z)$ the <u>minimal polynomial</u> for α.

Ex. $\alpha = 1 + \sqrt{2}$. How do we compute $m(z)$.

Elimination method.

?irreducible.

$$z = 1 + \sqrt{2} \Rightarrow (z-1) = \sqrt{2} \Rightarrow (z-1)^2 = 2$$
$$\Rightarrow z^2 - 2z + 1 - 2 = 0 \Rightarrow \boxed{z^2 - 2z - 1} = 0.$$

Let $z = 1 + s$ where $s^2 = 2$.

?irreducible.

Consider $\langle \underbrace{z - 1 - s,\ s^2 - 2 \rangle \cap \mathbb{Q}[z] = \langle z^2 - 2z + 1}_{\in B.} \rangle$

Linear algebra. $m(\alpha) = 0$ has least degree.

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

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

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

$$0 = m(\alpha) = m(1 + \sqrt{2}) = 1 + 2\sqrt{2} + 2 + a + a\sqrt{2} + b$$
$$= \underline{\sqrt{2}}\underbrace{(2 + a)}_{= 0} + \underline{1} \cdot \underbrace{(3 + a + b)}_{= 0}.$$

$$\Rightarrow \quad 2 + a = 0 \Rightarrow a = -2$$
$$3 + a + b = 0 \Rightarrow b = -1.$$

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

Ex. $\alpha = 1 + \sqrt{2} + \sqrt{3} + \underline{\sqrt{6}}$.

Def. Let α, β be algebraic numbers.

Def. Let α, β be algebraic numbers.

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

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

$\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\alpha,\beta)$ are called algebraic number fields.

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

<u>Computing with algebraic numbers.</u>

Let α be an algebraic number with min poly $m(z)$ of degree d.

Recall $R = \mathbb{Q}[z]/\underline{m(z)} = \{ [\sum_{i=0}^{d-1} a_i z^i : a_i \in \mathbb{Q}] \}$. is a quotient ring.

For $[a],[b] \in R$ then

$$[a] +_R [b] = [a +_{\mathbb{Q}[z]} b]$$

$$[a] \cdot_R [b] = [a \cdot b \bmod_{\mathbb{Q}[z]} m]$$

<u>Since m is irreducible then R is a field.</u>

Theorem 1. $R \cong \mathbb{Q}^d$ as a vector space.

The standard basis is $\{1, z, z^2, \dots, z^{d-1}\}$.

Theorem 2. $\mathbb{Q}(\alpha) \cong R$ with isomorphism $\phi(\alpha) = z$.

Ex. $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[z]/(z^2-2)$.

$$\begin{tikzcd}
\sqrt{2}(1+\sqrt{2}) \arrow[r, "="] \arrow[d, "\phi"] & \sqrt{2}+2. \\
{[z]\cdot[1+z] = [z + \overset{2}{\overset{\|}{z^2}} \bmod z^2-2] = [z+2]} \arrow[ur, "\phi^{-1}"'] &
\end{tikzcd}$$

To invert $[a] \in R$ solve $\underline{s}a + \underline{t}m = \gcd(a,m)$ in $\mathbb{Q}[z]$ using the EEA. $\deg(a) < m$, m is irreducible. $\Rightarrow \gcd(a,m) = 1$

$$\Rightarrow \underset{\text{in } \mathbb{Q}[z]}{sa + tm = 1} \Rightarrow \underset{\text{in } R}{[sa + \cancel{tm}]} = [1] = [sa] = \underset{\deg s < m.}{[s]} \cdot \underset{\deg < m}{[a]}.$$

$$\Rightarrow [a]^{-1} = [s].$$

E.g. $[a] = [1+z]$, $m = z^2 - z$.

$\mathbb{Q}[z]$

```
m := z^2-z;
gcdex(z+1, m, z, 's', 't');
s;
```

The cyclotomic (number) fields $\mathbb{Q}(\omega)$.

Let $\omega \in \mathbb{C}$ be a root of $x^n = 1$ s.t. $\omega^k \neq 1$ for $1 \le k < n$.
So ω is a primitive n'th root of unity.
Let $m_\omega(z)$ be the min poly for ω.

n	$x^n - 1$	ω	$m_\omega(z)$	$d = \deg m_\omega$
1	$x-1$	1	$z-1$	1
→ 2	$x^2-1 = (\cancel{x-1})(x+1)$	-1	$z+1$	1
3	$x^3-1 = (\cancel{x-1})(x^2+x+1)$	$-\frac{1}{2}+\frac{\sqrt{3}}{2}i$	z^2+z+1	2
4	$x^4-1 = (\cancel{x^2-1})(x^2+1)$	$\pm i$	z^2+1	2
5	$x^5-1 = (x-1)(x^4+x^3+x^2+x+1)$	?	$z^4+z^3+z^2+z+1$	4
6	$x^6-1 = (x^3-1)(x^3+1) = (x^3-1)(x+1)(x^2-x+1)$	$\frac{1}{2}\pm\frac{\sqrt{3}}{2}i$	z^2-z+1	2
7				6
8				4

$\deg(\omega_n) = \phi_n$ = Euler's totient function.

$m_\omega(z)$ is called the n'th cyclotomic poly.

The number field $\mathbb{Q}(\omega_n)$ is called a cyclotomic field.

Ex. Let $\omega^5 = 1$. $m_\omega(z) = z^4+z^3+z^2+z+1$.

Solve
$$\{\boxed{\omega}x + \omega y = 1,\ \omega^3 x + \omega^4 y = -1\}.$$
$\times\omega^4$ $\qquad$ $\times\omega^2$
$$\{1\cdot x + 1\cdot y = \omega^4 \ (1),\ 1\cdot x + \omega\cdot y = -\omega^2 \ (2)\}.$$

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

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

Solve $s(1-z) + tm = 1$ for $s, t \in \mathbb{Q}[z]$.