Algebraic Number Fields: Multiple Extensions

March 4, 2022 11:25 AM

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

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

Let $m(z)$ be the min. poly. for α and let $d = \deg(m)$.

Let $K = \mathbb{Q}[z]/m(z) = \{ [\sum_{i=0}^{d-1} a_i z^i] : a_i \in \mathbb{Q} \}$.

Theorem 1 $\underline{\mathbb{Q}(\alpha)} \cong \underline{K}$ with $\varphi(\alpha) = [z]$.

Theorem 2. $\underline{K} \cong \mathbb{Q}^d$ as a vector space.

Proof. Let $a, b \in K$, $s \in \mathbb{Q}$.

Take $\varphi([\sum_{i=0}^{d-1} a_i z^i]) = [a_0, a_1, \ldots, a_{d-1}] \in \mathbb{Q}^d$.

is bijective.

(i) $\varphi(\underline{a} + b) = \varphi([\Sigma a_i z^i] + [\Sigma b_i z^i]) = \varphi([\Sigma (a_i + b_i) z^i]) = [a_0 + b_0, \ldots, a_{d-1} + b_{d-1}]$

$\varphi(a) + \varphi(b) = \varphi([\Sigma a_i z^i]) \pm \varphi([\Sigma b_i z^i]) = [a_0, \ldots, a_{d-1}] + [b_0, \ldots, b_{d-1}] =$

(ii) $\varphi(sa) = s\,\varphi(a)$.

Def. The degree of a number field K is

$$[K : \mathbb{Q}] = \dim(K) = d = \deg m(z).$$

Multiple Extensions

Let α and β be algebraic numbers. The number field $K = \underline{\mathbb{Q}(\alpha, \beta)}$ is the smallest field containing $\mathbb{Q}$ and α and β.

How do we compute in K?

How do we represent elements of K?

What is a basis for K over $\mathbb{Q}$?

α, β	Basis	$[K:\mathbb{Q}]$	$m_\alpha(x)$	$m_\beta(y)$
$\sqrt{2}, \sqrt{3}$	$\{1, \sqrt{2}, \sqrt{3}, \sqrt{2}\cdot\sqrt{3}\}$	4	$x^2 - 2$	$y^2 - 3$
$\sqrt{2}, \sqrt[4]{2}$	$\{1, \sqrt[4]{2}, (\sqrt[4]{2})^2 = \sqrt{2}, (\sqrt[4]{2})^3 = \sqrt{2}\cdot\sqrt[4]{2}\}$	4	$x^2 - 2$	$y^4 - 2$

$\mathbb{Q}(\sqrt{2}) \subsetneq \mathbb{Q}(\sqrt[4]{2})$ $\mathbb{Q}(\sqrt{2}, \sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2})$.

$\mathbb{Q}(\sqrt{2}) \subsetneq \mathbb{Q}(\sqrt[4]{2}) \qquad \mathbb{Q}(\sqrt{2}, \sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}).$

$(y^2 - \sqrt{2})(y^2 + \sqrt{2})$

② Recursive Method.

Let $K = \mathbb{Q}[x]/M_\alpha(x)$, $L = K[y]/m_\beta(y)$ ← field.

$\mathbb{Q}(\alpha)$ ↑ a field. $\quad \mathbb{Q}(\alpha, \beta)$

L is a field $\iff$ $m_\beta(y)$ is irreducible over L.

③ Grobner bases. $\quad 1 \cdot x^{d_\alpha} + \cdots \quad 1 \cdot y^{d_\beta} + \cdots$

Let $I = \langle M_\alpha(x), M_\beta(y) \rangle \subset \mathbb{Q}[x,y]$.

$G = [M_\alpha(x), m_\beta(y)]$ is a GB for I wrt any mon. ord.

Let $R = \mathbb{Q}[x,y]/I = \{ [\sum_{i=0}^{d_\alpha - 1} \sum_{j=0}^{d_\beta - 1} a_{ij} x^i y^j] : a_{ij} \in \mathbb{Q} \}$.

R is a field $\iff$ I is maximal over $\mathbb{Q}$. ??

$\iff$ $m_\beta(y)$ is irreducible over $\mathbb{Q}(\alpha) = K$.

③ Primitive elements. $\quad \mathbb{Q}(\alpha, \beta)$

Let $\gamma = c_1 \alpha + c_2 \beta$ for $c_1, c_2 \in \mathbb{Q}$.

If $\mathbb{Q}(\gamma) \cong \mathbb{Q}(\alpha, \beta)$ then γ is called a prim. elem.

Let $m(z)$ be the min poly for γ and $d = \deg m$.

$\mathbb{Q}(\gamma) \cong \mathbb{Q}[z]/m(z) = \{ [\sum_{i=0}^{d-1} a_i z^i] : a_i \in \mathbb{Q} \}$

↑ one variable.

How do we compute $m_\gamma(z)$ given $M_\alpha(x)$ and $m_\beta(y)$?

what is $\varphi(\alpha) =$ and $\varphi(\beta) =$?

We know $\varphi^{-1}(\gamma) = c_1 \alpha + c_2 \beta$.

Theorem. Let G be the monic reduced G.B. for

$\langle M_\alpha(x), m_\beta(y), z - (c_1 x + c_2 y) \rangle$.

$\gamma = c_1 \alpha + c_2 \beta$

$$\langle m_\alpha(x),\ m_\beta(y),\ z-(c_1x+c_2y) \rangle.$$
$$\gamma = c_1\alpha + c_2\beta$$

w.r.t. $>_{lex}$ with $x>y>z$ (or $y>x>z$).

Then $G = \left\{ m_\gamma(z),\ 1\cdot x + \sum_{i=0}^{d-1} a_i z^i,\ 1\cdot y + \sum_{i=0}^{d-1} b_i z^i \right\}$

$d = \deg m_\gamma(z)$

$$\varphi(\underset{\alpha}{x}) = -\sum_{i=0}^{d-1} a_i z^i \qquad \varphi(\underset{\beta}{y}) = -\sum_{i=0}^{d-1} b_i z^i.$$

$G = 3x + \sqrt{2}y + \sqrt{3}z + 3\sqrt{2} + 1.$

Application.

Let $A, B \in \mathbb{Q}(\alpha,\beta)[x_0, x_1, \dots, x_n]$ and $G = GCD(A,B)$.

$$\begin{array}{ccc} \mathbb{Q}(\alpha,\beta) & [x_0, & \underbrace{x_1,\dots,x_n}] \\ \varphi_\beta \downarrow \ \downarrow \varphi_\gamma & \downarrow & \downarrow K_r \\ \mathbb{Z}_p(\gamma) & [x, & y] \end{array}$$

$d = \deg m_\gamma(z)$

$$\mathbb{Z}_p(\gamma) \cong \mathbb{Z}_p[z]/(m_\gamma(z) \bmod p) = \left\{ \left[\sum_{i=0}^{d-1} a_i z^i\right] : a_i \in \mathbb{Z}_p \right\}$$