Primitive Elements

November 14, 2023 11:47 AM

Def. Let $K = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ be our algebraic number field.
An algebraic number γ is a <u>primitive element</u> if $\mathbb{Q}(\gamma) \equiv K$.

Does a prim. elem. exist for every K? Yes.

Theorem $\exists c_1, \dots, c_n \in \mathbb{Q}$ s.t. $\gamma = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n$ is a prim elem.
Almost all non-zero choices for c_i's work.

Idea: Compute the isomorphism $\varphi: K \to \mathbb{Q}(\gamma)$ and instead of computing in K compute in $\mathbb{Q}(\gamma)$.
$\mathbb{Q}(\gamma) = \mathbb{Q}[z]/m(z)$ where m is the min poly for γ over $\mathbb{Q}$.

Theorem. Let B be a basis for K over $\mathbb{Q}$.
Let $d = \dim(K:\mathbb{Q})$.
Let $c_1, \dots, c_n \in \mathbb{Z}$, $\gamma = c_1\alpha_1 + \cdots + c_n\alpha_n$
Let $m(z)$ be the min. poly. for γ over $\mathbb{Q}$.
The following statements are equivalent.

(i) γ is a prim. elem. for K.
(ii) $\deg(m) = d$.
→ (iii) $\det(A) \neq 0$ where $A = \begin{bmatrix} | & | & | & & | \\ [1]_B & [\gamma]_B & [\gamma^2]_B & \cdots & [\gamma^{d-1}]_B \\ | & | & | & & | \end{bmatrix}$

To compute in $\mathbb{Q}(\gamma) \equiv \mathbb{Q}[z]/m(z)$ we need $m(z)$.
Letting $m(z) = z^d + a_{d-1}z^{d-1} + \cdots + a_1 z + a_0$,
$0 = m(\gamma) = a_{d-1}\gamma^{d-1} + \cdots + a_1\gamma + a_0 = -\gamma^d$

We have $A \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{d-1} \end{bmatrix} = \begin{bmatrix} | \\ [-\gamma^d]_B \\ | \end{bmatrix}$. Solving this linear system gives us $m(z)$.

E.g. $\alpha_1 = \sqrt{2}$, $\alpha_2 = \sqrt{3}$. Consider $\gamma = 1\cdot\sqrt{2} + 1\cdot\sqrt{3} = 1\cdot z_1 + 1\cdot z_2$. $c_1 = 1$ $c_2 = 1$
$m_1(z_1) = z_1^2 - 2$, $m_2(z_2) = z_2^2 - 3$. $R = \mathbb{Q}[z_1, z_2]/\langle m_1, m_2\rangle$.
A basis for R is $B = \{1, z_1, z_2, z_1 \cdot z_2\}$. $d = 2\cdot 2 = 4$.

$\begin{bmatrix}1\\ \gamma\\ \gamma^2\end{bmatrix}_B = \begin{bmatrix}0\\1\\1\\0\end{bmatrix}$ $\gamma^2 = (z_1+z_2)(z_1+z_2) = z_1^2 + z_1z_2 + z_2z_1 + z_2^2$

$= 5 + 2z_1z_2$

$\begin{bmatrix}\gamma^2\end{bmatrix}_B = \begin{bmatrix}5\\0\\0\\2\end{bmatrix}$ $\gamma^3 = (z_1+z_2)(5+2z_1z_2) = 5z_1+5z_2+2z_1^2z_2+2z_1z_2^2$

$= 11z_1+9z_2$

$\begin{bmatrix}\gamma^3\end{bmatrix}_B = \begin{bmatrix}0\\11\\9\\0\end{bmatrix}$ $\gamma^4 = (z_1+z_2)(11z_1+9z_2) = 49 + 20z_1z_2$. $\begin{bmatrix}\gamma^4\end{bmatrix}_B = \begin{bmatrix}49\\0\\0\\20\end{bmatrix}$

$A = \begin{bmatrix}1&0&5&0\\0&1&0&11\\0&1&0&9\\0&0&2&0\end{bmatrix} \xrightarrow{R_3 \leftarrow R_3 - R_2} \begin{bmatrix}1&0&5&0\\0&1&0&11\\0&0&0&-2\\0&0&2&0\end{bmatrix} \xrightarrow{R_3 \leftrightarrow R_4} \begin{bmatrix}1&0&5&0\\0&1&0&11\\0&0&2&0\\0&0&0&-2\end{bmatrix}$

$\det(A) = 2\cdot(-2)\cdot(-1) = 4 \neq 0.$

Since $\det(A) = 4$ $\gamma = \sqrt{2}+\sqrt{3} = z_1+z_2$ is a primitive element.

$[A|b] = \begin{bmatrix}1&0&5&0&-49\\0&1&0&11&0\\0&1&0&9&0\\0&0&2&0&-20\end{bmatrix}$ Solving $A\cdot a = [-\gamma^4]_B \Rightarrow a = \begin{bmatrix}1\\0\\-10\\0\end{bmatrix}\begin{matrix}a_0\\a_1\\a_2\\a_3\end{matrix}$

$\Rightarrow M(z) = z^4 - 10z^2 + 1.$

Thus $K = \mathbb{Q}(\sqrt{2},\sqrt{3}) \cong \mathbb{Q}[z]/(z^4-10z^2+1) = R$ where a basis $B' = \{1, z, z^2, z^3\}$.

What is the isomorphism $\phi : K \to R$?

$z = \gamma = z_1+z_2$. so $\phi^{-1}(z) = z_1+z_2$.

$\phi^{-1}([a+bz+cz^2+dz^3]) = A\begin{bmatrix}a\\b\\c\\d\end{bmatrix} = A[f]_{B'}$

$= [f]$.

where $A^{-1} = \begin{bmatrix}1&0&0&-5/2\\0&-9/2&11/2&0\\0&0&0&1/2\\0&1/2&-1/2&0\end{bmatrix}$. $\begin{bmatrix}0\\1\\0\\0\end{bmatrix} = \begin{bmatrix}0\\-9/2\\0\\1/2\end{bmatrix}$

$\phi([a+bz_1+cz_2+dz_1z_2]) = A^{-1}\begin{bmatrix}a\\b\\c\\d\end{bmatrix} = A^{-1}[g]_B.$

$= [g]$

E.g. What is $\phi(\sqrt{2}) = \phi(z_1)$. $A^{-1}\begin{bmatrix}0\\1\\0\\0\end{bmatrix} = \begin{bmatrix}0\\-9/2\\0\\1/2\end{bmatrix} \xrightarrow{B'} 0 - \frac{1}{2}z + 0z^2 + \frac{1}{2}z^3$.