Multiple Algebraic Extensions

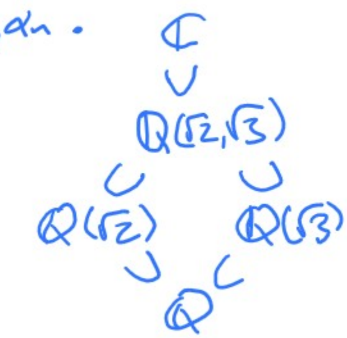
November 14, 2023 11:46 AM

Assignment #6 due Monday Nov 27th @ 11pm.

Computing in $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$.

Def. Let $\alpha_1, \dots, \alpha_n$ be algebraic numbers.
$\mathbb{Q}(\alpha_1, \dots, \alpha_n)$ is the smallest field contining $\mathbb{Q}, \alpha_1, \dots, \alpha_n$.
So $\mathbb{Q}(\alpha_1, \dots, \alpha_n) \subset \mathbb{C}$.

E.g. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.
Notice $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$ are subfields of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.



How can we compute in $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$?
Use $\mathbb{Q}(\alpha_1, \dots, \alpha_n) \cong \underline{\mathbb{Q}(\alpha_1)}(\alpha_2)(\alpha_3)\cdots(\alpha_n)$.

$L_0 := \mathbb{Q}$
$L_1 := \mathbb{Q}(\alpha_1) \cong \mathbb{Q}[z_1]/m_1(z_1)$ where m_1 is the min. poly for α_1 over $\mathbb{Q}$.
$L_2 := L_1[z_2]/m_2(z_2)$ where m_2 " " " " " α_2 over L_1.
$\vdots$
$L_n := L_{n-1}[z_n]/m_n(z_n)$ where m_n " " " " " α_n over L_{n-1}.

Let $d_k = \deg(m_k, z_k) \geq 1$. L_k is a quotient ring.
$\Rightarrow L_k \cong L_{k-1}^{d_k} \leftarrow \dim(L_k)$ as a vector space with basis
$B_k = \{1, z_k, z_k^2, \dots, z_k^{d_k - 1}\}$.
Since m_k is irreducible over L_{k-1}, L_k is a field and
$L_k \cong \mathbb{Q}(\alpha_1, \dots, \alpha_k)$ for $1 \leq k \leq n$.

E.g. $\underset{\smile}{\alpha_1 = \sqrt{2}}$, $\alpha_2 = \sqrt{3}$.
$z_1 = \sqrt{2} \Rightarrow z_1^2 = 2 \Rightarrow \boxed{z_1^2 - 2} = 0 \Rightarrow m_1 = z_1^2 - 2$.
$\Rightarrow L_1 = \mathbb{Q}[z_1]/(z_1^2 - 2)$, $B = \{1, z_1\}$, $d_1 = 2$.
Notice $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. so $\deg(m_2, z_2) > 1$.

Try. $m_2(z_2) = 1\cdot z_2^2 + (a_1 z_1 + a_0) z_2 + (b_1 z_1 + b_0) \in L_1[z_2]$.

$0 = m_2(\sqrt{3}) = 3 + (a_1 z_1 + a_0) z_2 + (b_1 z_1 + b_0)$

$\Rightarrow \quad 0 = a_1 \overset{\sqrt{2}}{z_1} \overset{\sqrt{3}}{z_2} + a_0 \overset{\sqrt{3}}{z_2} + b_1 \overset{\sqrt{2}}{z_1} + (3 + b_0)$

$\Rightarrow \quad a_1 = 0,\ a_0 = 0,\ b_1 = 0,\ b_0 = -3.$

$\Rightarrow \quad m_2(z_2) = z_2^2 - 3. \quad B_2 = \{1, z_2\}.$

$L_2 = \{ [a_1 + a_2 z_2] : a_1, a_2 \in L_1 \}$

We could represent $[(3+2z_1)\cdot 1 + (7+5z_1)\cdot z_2] \in L_2$ as $[[3,2],[7,5]]$. I do this in recden.

E.g. $\alpha_1 = \sqrt{2}$, $\alpha_2 = 1 + \sqrt{2} + \sqrt{3}$.

$m_1(z_1) = z_1^2 - 2$

$m_2(z_2) = z_2^2 - (2z_1 + 2) z_2 + 2z_1 \in L_1[z_2]$.

We also have $L_n \cong \mathbb{Q}[z_1, \dots, z_n] / \overbrace{\langle m_1, m_2, \dots, m_n \rangle}^{I} = R$.

In $>_{lex}$ with $z_1 < z_2 < \cdots < z_n$ $LM(m_i(z_i)) = z_i^{d_i}$.

Since $\gcd(LM(m_i), LM(m_j)) = 1 \Rightarrow G = \{m_1, \dots, m_n\}$ is a GB for I.

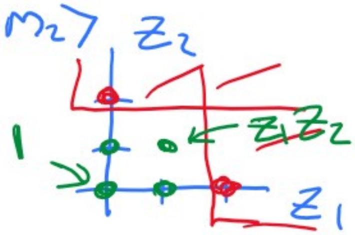
$R \cong \mathbb{Q}^d$ where $d = \prod_{k=1}^{n} d_k$. d is called the degree of L_n over $\mathbb{Q}$ or $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$ over $\mathbb{Q}$. So $R \cong \mathbb{Q}^d$.

A basis for R is $\overline{\langle LT(I) \rangle}$.

E.g. $m_1 = z_1^2 - 2$, $m_2 = z_2^2 - 3$, $I = \langle m_1, m_2 \rangle$

$\langle LT(I) \rangle = \langle z_1^2, z_2^2 \rangle$

$B = \{1, z_1, z_2, z_1 z_2\}$



We could represent elements of R as multivariate polynomials in $\mathbb{Q}[z_1, \dots, z_n]$. Then $[a]\cdot[b] = [ab \bmod G]$. This is quite slow.