Example 2.16

Suppose we know $\alpha = \sqrt{5} + \sqrt[4]{5} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$, but are not given a polynomial with $p(\alpha) = 0$.

How to find the minimal polynomial?

Proposition 2.15 $\rightsquigarrow$ find minimal $n \in \mathbb{N}$ s.t. $1, \alpha, \ldots, \alpha^n$ are $\mathbb{Q}$-linearly dependent.

$$\alpha = 5^{1/2} + 5^{1/4}$$

$$\alpha^2 = 5 + 2 \cdot 5^{3/4} + 5^{1/2}$$

$$\alpha^3 = 5^{3/2} + 3 \cdot 5^{5/4} + 3 \cdot 5^1 + 5^{3/4}$$

$$= 15 + 15 \cdot 5^{1/4} + 5 \cdot 5^{1/2} + 5^{3/4}$$

$$\alpha^4 = 30 + 20 \cdot 5^{1/4} + 30 \cdot 5^{1/2} + 20 \cdot 5^{3/4}$$

All of the above can be written as $\mathbb{Q}$-linear combinations of $1, 5^{1/4}, 5^{1/2}, 5^{3/4}$. In vector form

$$\left.\begin{array}{lll} 1 & \rightsquigarrow & (1, 0, 0, 0) \\ \alpha & \rightsquigarrow & (0, 1, 1, 0) \\ \alpha^2 & \rightsquigarrow & (5, 0, 1, 2) \\ \alpha^3 & \rightsquigarrow & (15, 15, 5, 1) \\ \alpha^4 & \rightsquigarrow & (30, 20, 30, 20) \end{array}\right\} \mathbb{Q}\text{-linearly dependent}$$

linear system:
$$\begin{cases} a + 5c + 15d = 30 \\ b + 15d = 20 \\ b + c + 5d = 30 \\ c + d = 20 \end{cases}$$

solution

$$\alpha^4 \overset{?}{=} a + b\alpha + c\alpha^2 + d\alpha^3$$

$$\rightsquigarrow \alpha^4 - 10\alpha^2 - 20\alpha + 20 = 0$$

Lemma 2.17

A field extension $K \hookrightarrow L$ is finite if and only if $L = K(\alpha_1, \dots, \alpha_n)$ with $\alpha_1, \dots, \alpha_n$ algebraic over K.

Proof

"$\Leftarrow$" Consider $K(\alpha_1, \dots, \alpha_n) = ((K(\alpha_1))(\alpha_2)) \dots (\alpha_n)$ as a chain $K \hookrightarrow L_1 \hookrightarrow L_2 \hookrightarrow \dots \hookrightarrow L_n = L$ of simple extensions, where $L_i = L_{i-1}(\alpha_i)$.

By assumption α_i algebraic over K, so α_i algebraic over $L_{i-1} \supset K$.

By Prop 2.13 each $[L_i : L_{i-1}] < \infty$ so by multiplicativity of degree (Corollary 1.13)

$$[L:K] = [L_n : L_{n-1}] \dots [L_1 : K] < \infty$$

"$\Rightarrow$" Suppose $[L:K] = n < \infty$. Let $\alpha_1, \dots, \alpha_n$ be a K-basis of L. Then $L = K(\alpha_1, \dots, \alpha_n)$. If any α_i were transcendental, then from $K \hookrightarrow K(\alpha_i) \hookrightarrow L$ we get

$$[L:K] \geq [K(\alpha_i):K] = \infty$$

Thm 1.12 Corollary 2.5

Let $K \subset \mathbb{C}$ subfield, $p \in K[t]$. Over $\mathbb{C}$ p factors as

$$p = (t-\alpha_1)^{n_1}(t-\alpha_2)^{n_2} \cdots (t-\alpha_l)^{n_l},$$

where $\alpha_1, \dots, \alpha_l \in \mathbb{C}$ are the distinct roots of p and $n_i \geq 1$.

Definition 2.18

- The <u>multiplicity</u> of the root α_i of p is the integer n_i.
- If $n_i > 1$, we call $\alpha_i \in \mathbb{C}$ a <u>multiple root</u> of p

Lemma 2.19

Let K be a subfield of $\mathbb{C}$.

If $p \in K[t]$ is irreducible, it has no multiple roots.

Proof

Suppose $\alpha \in \mathbb{C}$ is a multiple root of p. Then

$$p = (t-\alpha)^2 q, \qquad q \in \mathbb{C}[t]$$

(Note: this is not a factorization in $K[t]$!)

This implies that the derivative

$$p' = 2(t-\alpha)q + (t-\alpha)^2 q'$$

also has the root $p'(\alpha) = 0$.

Exercise: a common root $\alpha \in \mathbb{C}$ implies that there exist a common factor $f \in K[t]$, $\deg f \geq 1$.

But p is irreducible, so ~~no~~ it has no nontrivial factors. $\square$

Example 2.20

$p = t^6 - 3t^2 - 2 \in \mathbb{Q}[t]$ Factors over $\mathbb{C}$ as

$$p = (t-i)^2 \underbrace{(t+i)^2 (t-\sqrt{2})(t+\sqrt{2})}_{=: q}$$

$$q = t^4 + 2it^3 - 3t^2 - 4it + 2$$

Then $q' = 4t^3 + 6it^2 - 6t - 4i$

and $p' = 2(t-i)q + (t-i)^2 q'$

$= 6t^5 - 6t$

By the Euclidean algorithm,

$$p = \frac{1}{6} t \cdot p' - 2t^2 - 2$$

$$p' = (-3t^3 + 3t)(-2t^2 - 2)$$

$\Rightarrow \gcd(p, p') = -2(t^2 + 1)$

Indeed p is reducible in $K[t]$:

$$p = (t^2+1)^2 (t^2 - 2)$$

Theorem 2.21 (Primitive element theorem)

Let $K \subset L \subset \mathbb{C}$ be subfields such that $[L:K] < \infty$.

Then $\exists\, \theta \in L$ such that $K(\theta) = L$.

Proof

Lemma 2.17 $\Rightarrow$ $L = K(\alpha_1, \dots, \alpha_n)$ with $\alpha_1, \dots, \alpha_n \in L$ algebraic over K.

Consider first the case $L = K(\alpha, \beta)$ $(n=2)$.

Let $\theta = \alpha + \lambda\beta$, $\lambda \in K$

We will show $K(\theta) = K(\alpha, \beta)$ for most elements $\lambda \in L$.

Let $m \in K(\theta)[t]$ be the minimal polynomial of β over $K(\theta)$.

Suffices to show $\deg m = 1$, since then $\beta \in K(\theta)$ (by Ex 1.3)

and if $\beta \in K(\theta)$, then also $\alpha = \theta - \lambda\beta \in K(\theta)$.

Let $f, g \in K[t]$ be the minimal polynomials of α, β respectively.

Define $h \in K(\theta)[t]$ by $h(t) = f(\theta - \lambda t)$.

Then $g(\beta) = 0$ (by definition) and

$$h(\beta) = f(\theta - \lambda\beta) = f(\alpha) = 0$$

That is $g, h \in K(\theta)[t]$ have a common root β.

Lemma 2.7 $\Rightarrow$ $m \mid g$ and $m \mid h$ $\Rightarrow$ $m \mid \gcd(g, h)$

Claim: $\deg \gcd(g, h) = 1$ for most $\lambda \in K$.

Proof of claim: suppose $\deg \gcd(g,h) \geq 2$.

g irreducible over $K \overset{\text{Lemma 21g}}{\Longrightarrow}$ β not a multiple zero

$\Rightarrow \exists\, \beta' \in \mathbb{C}$, $\beta' \neq \beta$, $g(\beta') = h(\beta') = 0$.

By the definition of h, we obtain

$$h(\beta') = f(\theta - \lambda\beta') = 0$$

so $\alpha' := \theta - \lambda\beta'$ is a root of f.

Then $\alpha + \lambda\beta = \theta = \alpha' + \lambda\beta'$

$$\Rightarrow \lambda = \frac{\alpha' - \alpha}{\beta - \beta'}, \quad \beta - \beta' \neq 0$$

Therefore if λ is not of the form

$$\lambda = \frac{(\text{root of } f) - \alpha}{\beta - (\text{root of } g)}$$

then $\deg \gcd(g,h) = 1$.

f, g have finitely many roots $\Rightarrow$ most λ not of that form

This resolves the $n=2$ case $L = K(\alpha, \beta)$.

For general $L = K(\alpha_1, \ldots, \alpha_n)$, we consider

$$K \hookrightarrow K(\alpha_1, \alpha_2) \hookrightarrow K(\alpha_1,\alpha_2)(\alpha_3, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_n)$$

By the previous argument $K(\alpha_1, \alpha_2) = K(\theta)$ for some θ, so

$$K(\alpha_1, \ldots, \alpha_n) = K(\theta)(\alpha_3, \ldots, \alpha_n) = K(\theta, \alpha_3, \ldots, \alpha_n)$$

and the claim follows by induction $\square$

3 ALGEBRAIC & CONSTRUCTIBLE NUMBERS

3A ALGEBRAIC NUMBERS

Proposition 3.1

Let $K \hookrightarrow L$ and $L = K(\alpha_1, \ldots, \alpha_n)$, $\alpha_i \in L$.
Then $\alpha_1, \ldots, \alpha_n$ algebraic over K
if and only if $K \hookrightarrow L$ algebraic extension.

Proof

"$\Leftarrow$" Immediate.

"$\Rightarrow$" Lemma 2.17 $\Rightarrow$ $[L:K] < \infty$.

If $\exists \alpha \in L$ transcendental over K,
then $[L:K] \geq [K(\alpha):K] = \infty$ (see proof of Lemma 2.17) $\square$

Corollary 3.2

Let $K \hookrightarrow L$ be a field extension. Let

$$A = \{\alpha \in L : \alpha \text{ algebraic over } K\}$$

Then A is a subfield of L.

Proof

$0, 1 \in A$ (as roots of $t \in K[t]$ and $t-1 \in K[t]$)

We need to show that $\alpha, \beta \in A \Rightarrow \alpha+\beta, \alpha \cdot \beta, -\alpha, \alpha^{-1} \in A$.

For fixed $\alpha, \beta \in A$. Consider $K \hookrightarrow K(\alpha, \beta) \subset L$

$\alpha+\beta, \alpha\cdot\beta, -\alpha, \alpha^{-1} \in K(\alpha,\beta) \xRightarrow{\text{Prop}}$ all algebraic over K. $\square$

Definition 3.3

The field of algebraic numbers is the subfield

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \alpha \text{ algebraic over } \mathbb{Q}\}$$

The notation $\overline{\mathbb{Q}}$ is because $\overline{\mathbb{Q}}$ is the <u>algebraic closure</u> of $\mathbb{Q}$: the smallest algebraically closed field containing $\mathbb{Q}$.

Definition 3.4

A field K is algebraically closed if every nonconstant $p \in K[t]$ has a root in K.

A general construction for the algebraic closure of an abstract field K can be found in Stewart Ch. 17.9.

Prop 3.1 implies that in $K \hookrightarrow L$

$\alpha, \beta \in L$ & $f, g \in K[t]$ such that $f(\alpha) = 0 = g(\beta)$

$\Rightarrow \exists p, q, r, s \in K[t]$ $p(\alpha+\beta) = q(\alpha\beta) = r(-\alpha) = s(\alpha^{-1}) = 0$

but does not say what p, q, r, s are.

One explicit construction is based on the following:

Theorem 3.5

Let $K \hookrightarrow L$ and $\alpha \in L$.

α is algebraic over K if and only if

$\exists$ a square matrix $A \in K^{n \times n}$ with an eigenvalue α

(That is, view A as a linear map $L^n \to L^n$.
Then $\exists v \in L^n$ such that $Av = \alpha v$)

Definition 3.6

Let $p = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 \in K[t]$ monic.

The companion matrix of p is

$$A = \begin{pmatrix} 0 & & & & & -a_0 \\ 1 & 0 & & & & -a_1 \\ & 1 & 0 & & & -a_2 \\ & & 1 & \ddots & & \vdots \\ & & & \ddots & 0 & -a_{n-2} \\ & & & & 1 & -a_{n-1} \end{pmatrix} \in K^{n \times n}$$

Proof of Theorem 3.5

"$\Leftarrow$" An eigenvalue is a root of the characteristic polynomial

$$p = \det(tI - A) \in K[t]$$

Hence eigenvalues of a matrix with coefficients in K are algebraic over K.

"$\Rightarrow$" If $\alpha \in L$ is algebraic over K, $\exists p \in K[t]$, $p(\alpha) = 0$.

Claim: p is the characteristic polynomial of its companion matrix A

Proof: compute $\det(tI - A)$ using a cofactor expansion along the last column

$$tI - A = \left(\begin{array}{cccccc|c}
t & & & & & & a_0 \\
-1 & t & & & & & a_1 \\
\hline
 & -1 & t & & & & a_2 \\
\hline
 & & & & & & \vdots \\
 & & -1 & & & & \\
 & & & & & t & a_{n-2} \\
 & & & & & -1 & t + a_{n-1}
\end{array}\right)$$

$$\det(tI - A) = (-1)^{n-1}\left(a_0 q_0(t) - a_1 q_1(t) + \dots + (-1)^{n-1}(t + a_{n-1}) q_{n-1}(t)\right)$$

$$q_j(t) = \det \left(\begin{array}{cccc|cccc}
t & & & & & & & \\
-1 & t & & & & & & \\
 & -1 & \ddots & & & & & \\
 & & & t & & & & \\
\hline
 & & & & -1 & t & & \\
 & & & & & -1 & t & \\
 & & & & & & \ddots & \\
 & & & & & & & -1
\end{array}\right)\begin{array}{l} \text{j rows} \\ \\ \\ \\ \text{n-1-j rows} \\ \\ \\ \\ \end{array} = t^j \cdot (-1)^{n-1-j}$$

$\Rightarrow$ all signs cancel out, $\det(tI - A) = p$ $\square$.