Q What about transcendental elements?

Let $F(x)$ denote the field of rational functions over F. It is, the field of fractions of $F[x]$, and its elements are all $f(x)/g(x)$, where $f(x), g(x) \in F[x]$. In this case x is transcendental over F.

And we have

Thm: Suppose $L:K$ an extension, $\alpha \in L$ transcendental over K.
Then the evaluation map

$$ev_\alpha : K[x] \to K[\alpha] \subset L$$
$$p(x) \mapsto p(\alpha)$$

can be extended to an isomorphism

$$\Phi_\alpha : K(x) \longrightarrow K(\alpha).$$

Proof: Recall $K(x)$ is obtained by considering an equivalence relation on $(K[x] \times (K[x] \setminus \{0\})$

$$(f, g) \sim (\tilde{f}, \tilde{g}) \iff f\tilde{g} = \tilde{f}g \text{ in } K[x]$$

And we write f/g for $[(f,g)]$, the class of (f,g).
Since $\alpha \in L$ is transcendental over L,
$g(\alpha) \neq 0$ for any $g \in K[x] \setminus \{0\}$ and

We can define a map $\phi_\alpha : K[x] \times (K[x] \setminus 0) \to K(\alpha)$

via $\phi_\alpha((f,g)) = f(\alpha) g(\alpha)^{-1}$

and if $(f,g) \sim (\tilde{f},\tilde{g})$ then $f(\alpha)\tilde{g}(\alpha) = \tilde{f}(\alpha) g(\alpha)$

hence $f(\alpha) g(\alpha)^{-1} = \tilde{f}(\alpha) \tilde{g}(\alpha)^{-1}$

and $\phi_\alpha(f,g) = \phi(\tilde{f},\tilde{g})$

Thus ϕ_α is constant on equivalence classes ie it is well defined,

and we can define
$$\Phi_\alpha : K(x) \to K(\alpha)$$
$$f/g \mapsto f(\alpha) g(\alpha)^{-1}$$

It is straightforward to verify Φ_α is a ring hom

Since $\Phi_\alpha(x) = \alpha = ev_\alpha(x)$, $\Phi_\alpha(k) = k = ev_\alpha(k)$

$K(\alpha) \subseteq \Phi_\alpha(K(x))$

On the other hand if $f/g \in K(x)$, then

$\Phi_\alpha(f/g) = f(\alpha) g(\alpha)^{-1} \in K(\alpha)$. Hence

$\Phi_\alpha(K(x)) \subset K(\alpha)$ and $\Phi_\alpha(K(x)) = K(\alpha)$

If the restriction that α, β are algebraic is removed, the statement is not true.

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{2} = 2 \quad \text{alg.}$$

Here $\sqrt{2}^{\sqrt{2}}$ is trans. by Gelfond-Schreider

• e^{π} = Gelfond Constant is transcendental.

$$e^{\pi} = \left(e^{i\pi}\right)^{-i} \qquad \begin{array}{l} \alpha = e^{i\pi} = -1 \text{ alg } \neq 0, 1 \\ \beta = -i \text{ alg, not in } \mathbb{Q}. \end{array}$$

Hence by Gelfond-Schreider e^{π} is transcendental.

To see this consider the polynomial

$p(x) = x^2 - (\pi + e)x + \pi e = (x - \pi)(x - e)$

If both $\pi + e$, πe were algebraic, then $p(x)$ would be a poly with algebraic coefs.

Since $\mathbb{Q}(a+b)$, $\mathbb{Q}(ab)$ alg over $\mathbb{Q}$ imply the roots of $x^2 - (a+b)x + ab$ are also algebraic this will imply that the roots of the polynomial $p(x)$ must be algebraic which is a contradiction to transcendence of π, and e.

- Lindemann showed that e^{α} for any algebraic α is transcendental. Since $e^{i\pi} = -1$ is algebraic $i\pi$, hence π must be transcendental.

- Gelfond–Schneider Thm. If α, β alg. numbers $\alpha \neq 0, 1$, $\beta \notin \mathbb{Q}$, then $\alpha^{\beta} = \exp(\beta \log \alpha)$ is transcendental.

But $\mathbb{R}$ is uncountable

Hence there are uncountably many real numbers which are transcendental / $\mathbb{Q}$.

Rmk

In general given a real number, to show that it is not algebraic is hard.

- π is transcendental / $\mathbb{Q}$ but not over the larger field $\mathbb{Q}(\pi^2)$. It satisfies $x^2 - \pi^2 = 0$
  So being transcendental is also always wrt a base field.

  (Where as note if $L : K : F$
  if $\alpha \in L$ is alg over F then it is alg over any field $K \supseteq F$)

- α, β alg $\Rightarrow$ $\alpha + \beta$ alg but

  α, β trans $\not\Rightarrow$ $\alpha + \beta$ trans.

  $\pi - \pi = 0$ is alg.

- It is not known if $\pi + e$ is transcendental (or πe, or π^e)
- It is known at least one of $\pi + e$, πe must be transcendental

Note $\ker \overline{\Phi}_\alpha = \{0\}$ since $\nexists$ no non-zero polys s.t $f(\alpha) = 0$.

Hence $K(x) \cong K(\alpha)$ for a transcendental element α.

$\boxtimes$

Question Do transcendental numbers / $\mathbb{Q}$ exist in complex numbers?

The fact that they do exist was showed first by Liouville in 1844.

Hermite proved in 1873 that e is transcend. / $\mathbb{Q}$

Lindemann " " 1882 that π is transcendtl / $\mathbb{Q}$

One can show that transcendtl real #s exist by the following argument (Cantor 1874)

let $\overline{\mathbb{Q}}$ = field of alg #s / $\mathbb{Q}$.
$\{\alpha \in \mathbb{C} \mid \alpha$ is the root of a poly $p(x) \in \mathbb{Q}[x]\}$

Then the set $\overline{\mathbb{Q}} \cap \mathbb{R} \subset \mathbb{R}$ is countable

$\overline{\mathbb{Q}} \cap \mathbb{R} = \bigcup_n \{$algebraic elts of $\mathbb{R}$ of degree $n\}$

Before we move to splitting fields let's summarize what we've seen so far.

- If $f(x) \in F[x]$ is an irreducible poly of degree n then $\exists$ an extension K of F which contains a zero of f.

$$K = F[x]/(f(x)) = F(\alpha) = \{ a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} \mid a_i \in F \}.$$

- If $f(x) \in F[x]$ an irred poly and L is an extension of F containing a root α of f, then L contains $F(\alpha) \cong F[x]/(f(x))$

- Let $\varphi : F \to \tilde{F}$ an isom of field $p \in F[x]$ an irred poly, $\tilde{p}(x) = \varphi(p)(x) \in \tilde{F}[x]$.

  If α is a root of p in some ext. of F and β is a root of $\tilde{p}$ in some ext of $\tilde{F}$ then $\exists$ unique isom

  $\sigma : F(\alpha) \to \tilde{F}(\beta)$ extending φ.

  s.t. $\sigma(\alpha) = \beta$

  $\sigma|_F = \varphi$.

  ie. $F(\alpha) : F$ and $\tilde{F}(\beta) : \tilde{F}$ are isomorphic extensions of fields.

In general we have the following definition

Defn An isomorphism between 2 field extensions $L : K$, $\tilde{L} : \tilde{K}$ is a pair of field isomorphisms

$$\varphi : K \longrightarrow \tilde{K} \quad \text{and} \quad \sigma : L \longrightarrow \tilde{L}$$

such that if $\bar{i} : K \hookrightarrow L$, $j : \tilde{K} \hookrightarrow L$
$\bar{i}$ (resp j) embeddings of K (resp $\tilde{K}$) into L (reps $\tilde{L}$)
then for all $k \in K$ the following diagram commutes.

$$\begin{tikzcd} K \arrow[r, "\bar{i}"] \arrow[d, "\varphi"'] \arrow[dr, phantom, "\circlearrowright"] & L \arrow[d, "\sigma"] \\ \tilde{K} \arrow[r, "j"'] & \tilde{L} \end{tikzcd}$$

$$j(\varphi(k)) = \sigma(\bar{i}(k))$$

The field structure is preserved as well as the embedding of the small field in the large one.
If we identify K with $\bar{i}(K)$ and
$\tilde{K}$ with $j(\tilde{K})$
then $\bar{i}, j$ are inclusions and the commutativity relation becomes

$$\sigma|_K = \varphi .$$

- If $\alpha \in K$ is alg over F, then $\exists !$ monic irred poly $m(x) \in F(x)$, (called the min. poly of α over F) which has α as a root

  If $f \in F[x]$, and $f(\alpha) = 0$ then $m(x) | f(x)$ in $F[x]$

- $\alpha \in K$ is alg over F then
  1. $F[\alpha] = F(\alpha) = F[x]/m(x)$
  2. $[F(\alpha) : F] = \deg m =: n$
  3. $1, \alpha, \alpha^2 \ldots \alpha^{n-1}$ is a basis of $F(\alpha)$ as an F-vector space

- $\alpha \in K$ alg over $F \iff [F(\alpha) : F] < \infty$

- $[K : F] < \infty \implies K$ is alg over F

Warning: $\not\Leftarrow$

- $[K : F] < \infty \iff K = F(\alpha_1 \ldots \alpha_n)$ with α_i alg over F.

- $L : K$, $K : F$ alg extensions $\iff L : F$ alg.

§2.3 Splitting fields

Let $f(x) \in F[x]$ be a polynomial. We've seen that $\exists$ a field K which contains an isom. copy of F such that $f(x)$ has a root $\alpha \in K$.
Equivalently $f(x) = (x-\alpha)g(x)$, $g(x) \in K[x$

The next question is whether $\exists$ a field L in which $f(x)$ can be factored completely into linear factors.

Defn An extention L of F is called a splitting field for $f(x) \in F[x]$ if f factors completely in $L[x]$ and f does not split over any intermediate field $F \subset K \subsetneq L$

The next thm guarantees the existence of such a splitting field.

Thm 2.18 Let F be a field and $f \in F[x]$ a polynomial of degree n. Then $\exists$ an extention K of F which is a splitting field of f over F, with $[K:F] \leq n!$

Proof We use induction on $n = \deg f$.

If $n=1$ then take $K=F$ and we're done.
Suppose $n>1$: If the irreducible factors of $f(x)$ over F are all degree 1, then again we can take $K=F$.
Otherwise at least one of the irred factors of $f(x)$, say $g(x)$ has degree ≥ 2 ie

$$f(x) = g(x)h(x), \quad \deg g \leq \deg f = n.$$

By Kronecker's thm, $\exists$ an extention $E_1 \supseteq F(\alpha_1)$ of F containing a root α of $g(x)$, hence of f. The extention $F(\alpha_1):F$ has degree at most n (Since $f(\alpha_1) = g(\alpha_1)h(\alpha_1) = 0$, $\min_{\alpha,F}(x) \mid f(x)$).

We can write $f(x) = (x-\alpha_1)f_1(x)$ in $F(\alpha_1)[x]$, where $\deg f_1 = n-1$

By induction $\exists$ an extention E of $F(\alpha_1)$ containing all roots of $f_1(x)$ and $[E:F(\alpha_1)] \leq (n-1)!$
Since $F(\alpha_1) \subset E$ contains α_1, and E contains all roots of f_1, E contains all roots of $f(x) = (x-\alpha)f_1(x)$.

$$[E:F] = [E:F(\alpha_1)][F(\alpha_1):F]$$

$$\leq (n-1)!\, n = n!$$

Take $K = \bigcap_{\beta} E_\beta$ where E_β runs over

all subfields of E containing F which also contains all roots of $f(x)$.
Then K is a splitting field for $f(x)$ and its degree $\leq n!$

Eg $x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2})$
A splitting field of $x^4 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{2}i) = \mathbb{Q}(\sqrt[4]{2}, i)$

In the second description note one of the field generators is not a root of x^4-2.

The splitting field of x^4-2 over $\mathbb{R}$ is $\mathbb{R}(\sqrt[4]{2}, i\sqrt[4]{2}) = \mathbb{R}(i) = \mathbb{C}$

Rmk

(1) As irreducibility, the choice of base field is important in determining the splitting field.
Over $\mathbb{Q}$, the splitting field of x^4-2 has degree 8 whereas over $\mathbb{R}$, it has degree 2.

(2) The splitting field of a poly is in general a bigger extension than the extension obtained by adjoining a single root.

If f is irreducible then adjoining a single root of f to the base field gives, independently of the choice of the root,

an extension $F(\alpha)$ unique up to isom over K
ie. $F(\alpha) \cong F(\beta) = F[x]/(f(x))$ where
f is irred and α, β are any 2 roots.

If f is not irreducible this is not the case
eg $f(x) = (x^2-2)(x^2-3)$

adjoining a single root, $\sqrt{2}$ or $\sqrt{3}$ leads to non-isomorphic extensions.

$$\mathbb{Q}(\sqrt{2}) \not\cong \mathbb{Q}(\sqrt{3})$$

Hence it might seem that we might construct different splitting fields for f by varying the choice of the irreducible factors in the proof of thm 2.18.
But this is not the case and the next thm shows that up to isom splitting fields are unique.

Thm 2.19 let $\varphi : F \to \tilde{F}$ be an isom, $f(x) \in F[x]$
$\tilde{f}(x) = (\varphi f)(x)$. Let $K, \tilde{K}$ be splitting fields of f and $\tilde{f}$ over $F, \tilde{F}$ resp.
Then the isomorp. φ extends to an isom $\sigma : K \to \tilde{K}$ ie $\sigma|_F = \varphi$,

$$[K:F] = [\tilde{K}:\tilde{F}]$$

and the number of such extensions is at most $[K:F]$

(ie in particular $K:F$, $\tilde{K}:\tilde{F}$ are isom. extensions)

<u>Rmk</u> Before we prove 2.19, note that it immediately gives the uniqueness (up to isom) of splitting fields by taking $F = \tilde{F}$ and φ = identity map, we obtain

<u>Thm 2.20</u> Let $f \in F[x]$ be a non-constant polynomial. If K and $\tilde{K}$ are 2 splitting fields of f over F then $[K:F] = [\tilde{K}:F]$ and there is an isom

$$\sigma : K \longrightarrow \tilde{K} \text{ fixing all of } F \text{ pointw}$$

ie $\sigma|_F = \text{id}$.

Moreover the number of such isom $\sigma : K \longrightarrow \tilde{K}$ is at most $[K:F]$.

<u>Proof of Thm 2.19</u> Induction on $[K:F]$

If $[K:F] = 1$ then $K = F$ and $\tilde{K} = \tilde{F}$ and the only extension σ of φ in this case is φ so the # of extensions of φ to K is $1 = [K:F]$.

Suppose $[K:F] > 1$. Since K is generated over F by the roots of f, $f(x)$ has at least one root $\alpha \in K$ which is not in F.
Fix this α for the rest of the proof

Let $m(x)$ be the min poly of α over F
then $m | f$. If there is an isom
$\sigma : K \to \tilde{K}$ extending φ, then
$\sigma(\alpha)$ is a root of $(\varphi m)(x)$

Hence the values of $\sigma(\alpha)$ (to be determined)
must come from roots of $(\varphi m)(x)$.

Next note that $\tilde{m} = \varphi(m)(x)$ has a root in $\tilde{K}$:
Since isom $\varphi : F \to \tilde{F}$ extends to a ring isom
$F[x] \to \tilde{F}[x]$. And
$m(x) | f(x)$ in $F[x] \implies (\varphi m) | \varphi f$ in $\tilde{F}[x]$.

Since m is irred so is $\varphi m = \tilde{m}$
Since φf splits completely in $\tilde{K}[x]$
by defn of $\tilde{K}$, its factor φm also
splits in $\tilde{K}$. Hence $\varphi(m)(x)$ has a root
in $\tilde{K}$. So pick a root $\tilde{\alpha} \in \tilde{K}$ of φm
Then $d = \deg m = \deg \varphi(m) > 1$
since $[F(\alpha) : F] > 1$ and $[F(\alpha) : F] = \deg m$

Note there are at most d choices for $\tilde{\alpha}$ in $\tilde{K}$.
and once the choice of $\tilde{\alpha}$ is made, we have
a unique ext φ' of φ
$\varphi' : F(\alpha) \to \tilde{F}(\tilde{\alpha})$
and $\tilde{\varphi}|_F = \varphi$.
(This is Thm 2.6).
and $[F(\alpha) : F] = [\tilde{F}(\tilde{\alpha}) : \tilde{F}]$

$$\begin{array}{ccc} F(\alpha) & \xrightarrow{\varphi'} & \tilde{F}(\tilde{\alpha}) \\ d \,| & & |\, d \\ F & \xrightarrow{\varphi} & \tilde{F} \end{array}$$

Now we can induct on degrees of splitting fields.
Take as new base field $F(\alpha)$ and $\tilde{F}(\tilde{\alpha})$ which are isomorphic via φ'.
Since K is a splitting field of f over F it is also a splitting field of f over the larger field $F(\alpha)$. Similarly $\tilde{K}$ is a splitting field φf over $\tilde{F}(\tilde{\alpha})$

Since $d > 1$, $[K : F(\alpha)] = \dfrac{[K:F]}{d} < [L:K]$

By induction $\varphi' : F(\alpha) \to \tilde{F}(\tilde{\alpha})$ has an extension to a field isom $\sigma : K \to \tilde{K}$
and

$$[K:F] = [K : F(\alpha)][F(\alpha):F]$$
$$= [\tilde{K} : \tilde{F}(\tilde{\alpha})][\tilde{F}(\tilde{\alpha}) : \tilde{F}] = [\tilde{K} : \tilde{F}]$$

and $\sigma|_{F(\alpha)} = \varphi'$ and $\exists$ at most $[K : F(\alpha)]$ such extensions σ of φ'.

Note $\sigma|_F = \varphi$ since, $\varphi'|_F = \varphi$.

Since φ' is determined by $\varphi(\alpha) \in \tilde{K}$, which is a a root of φm, we have at most d different hom $\varphi' : F(\alpha) \to \tilde{K}$. Hence
the number of isom $K \to \tilde{K}$ that lift φ is the number of hom. $\varphi' : F(\alpha) \to \tilde{K}$ lifting φ (there are at most d different φ', depending on choice of $\tilde{\alpha}$) times the number of extensions of each φ' to an isom $\sigma : K \to \tilde{K}$ hence

in total $\exists$ at most $d[K:F(\alpha)] = [K:F]$ extensions of φ to an isom $\sigma : K \to \tilde{K}$.

Note every isom $\sigma : K \to \tilde{K}$ extending φ is the extension of some intermediate isom φ' of $F(\alpha)$ with a subfield of $\tilde{K}$.
As before $\sigma(\alpha)$ must be a root of σm. Define $\tilde{\alpha} := \sigma(\alpha)$
Since $\sigma|_F = \varphi$, the restriction $\sigma|_{F(\alpha)}$ is a field hom which is φ on F and sends α to $\tilde{\alpha}$, so $\sigma|_{F(\alpha)}$ is an isom from $F(\alpha)$ to $\tilde{F}(\sigma(\alpha)) = \tilde{F}(\tilde{\alpha})$. Thus σ is a lift of the intermediate field isom
$$\varphi' := \sigma|_{F(\alpha)}$$

$\boxtimes$

$$\begin{tikzcd}
\sigma : K \arrow[r] \arrow[d, dash] & \tilde{K} \arrow[d, dash] \\
\varphi' : F(\alpha) \arrow[r] \arrow[d, dash, "d"'] & \tilde{F}(\tilde{\alpha}) \arrow[d, dash, "d"] \\
\varphi \quad F \arrow[r] & \tilde{F}
\end{tikzcd}$$

Examples

① $x^3 - 2 \in \mathbb{Q}[x]$ has splitting field

$\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, where $\zeta_3^3 = 1$,

Hence ζ_3 is a root of $x^3 - 1 = (x-1)(x^2+x+$

hence $\min_{\zeta_3, \mathbb{Q}}(x) = x^2 + x + 1$

$$\begin{tikzcd}[column sep=small]
& \mathbb{Q}(\sqrt[3]{2}, \zeta_3) \arrow[dl, no head] \arrow[dr, no head] & \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[dr, no head, "3"'] & & \mathbb{Q}(\zeta_3) \arrow[dl, no head, "2"] \\
& \mathbb{Q} &
\end{tikzcd}$$

Since $\gcd(2,3) = 1$

$[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}] = 6 = 3$

This is in fact the generic situation but there are many examples with much smaller splitting fields.

Eg. ② $f(x) = x^n - 1 \in \mathbb{Q}[x]$

the roots are ζ_n^k $k = 0, \ldots n-1$

$\zeta_n^k = e^{2\pi i k/n}$

Hence $\mathbb{Q}(\zeta_n)$ is a splitting field

If $n = p$ $\quad x^p - 1 = (x-1)\underbrace{(x^{p-1} + x^{p-2} + \cdots + 1)}$ $:= \Phi_p(x)$

$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \deg \Phi_p = p - 1 < p!$