MA542 Lecture

Timothy Kohl

Boston University

March 21, 2025

It's an interesting exercise to compute $irr(\alpha, F)$ for a given α.

For example, let $\alpha = \sqrt{2} + \sqrt{3}$, what is $irr(\alpha, \mathbb{Q})$?

If we start by squaring α we get

$$\begin{aligned} \alpha^2 &= 2 + 2\sqrt{2}\sqrt{3} + 3 \\ &= 5 + 2\sqrt{6} \end{aligned}$$

and so $\alpha^2 - 5 = 2\sqrt{6}$ so $(\alpha^2 - 5)^2 = 24$ so that $\alpha^4 - 10\alpha^2 + 25 = 24$ and so $\alpha^4 - 10\alpha^2 + 1 = 0$ so α is a root of $f(x) = x^4 - 10x^2 + 1$

As it turns out, this *is* $irr(\alpha, \mathbb{Q})$ but the difficulty is in proving that $x^4 - 10x^2 + 1$ is irreducible in $\mathbb{Q}[x]$, but we shall find a nice, slightly indirect, way of proving it is, by using the idea of the dimension of an algebraic extension like $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$.

So for α an algebraic element over F we have that

$$\{f(x) \in F[x] \mid f(\alpha) = 0\} = \langle irr(\alpha, F)\rangle$$

and therefore

$$F(\alpha) \cong F[x]/\langle irr(\alpha, F)\rangle$$

where, if $deg(irr(\alpha, F)) = n$ means that

$$F(\alpha) = \{c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 \mid c_i \in F\}$$

meaning that $dim_F(F(\alpha)) = n$, in that $F(\alpha)$ is an F-vector space with basis

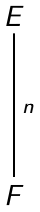
$$\{1, \alpha, \ldots, \alpha^{n-1}\}$$

Let's explore the dimension idea a bit more.

Definition

Let E be an extension field of F. We say that E has degree n over F, and write $[E : F] = n$ if E has dimension n when viewed as a vector space over F.
If $[E : F]$ is finite then we call E a finite extension of F, otherwise E is an infinite extension.

and sometimes we indicate the degree in a diagram like this:



For example

- $[\mathbb{Q}(i) : \mathbb{Q}] = 2$
- $[\mathbb{C} : \mathbb{R}] = 2$
- $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$
- $[\mathbb{Q}(\pi) : \mathbb{Q}]$ is infinite

and in general, if α is algebraic over F and $deg(irr(\alpha, F)) = n$ then $[F(\alpha) : F] = n$.

Also, comparing this to the last example in the list, $[\mathbb{Q}(\pi) : \mathbb{Q}]$, above points to an interesting and important fact about algebraic extensions.

We showed that if $\alpha = \sqrt{3} + \sqrt{2}$ then $f(\alpha) = 0$ for $f(x) = x^4 - 10x^2 + 1$.

And since $irr(\alpha, \mathbb{Q})$ generates the ideal of all polynomials with α as a root, we must have $irr(\alpha, \mathbb{Q}) | x^4 - 10x^2 + 1$.

So the question is whether $irr(\alpha, \mathbb{Q}) = x^4 - 10x^2 + 1$ or is a proper divisor.

We use that fact that $deg(irr(\alpha, \mathbb{Q})) = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ since it is the degree $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ which we shall determine.

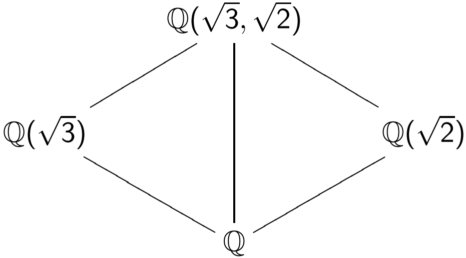
We have $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ where both are distinct extension fields of $\mathbb{Q}$.

We should note first that $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{3}) = \mathbb{Q}$. Why?

Well if $\sqrt{2} \in \mathbb{Q}(\sqrt{3})$ for example, then $\sqrt{2} = a + b\sqrt{3}$ for $a, b \in \mathbb{Q}$.
If $b = 0$ then this implies $\sqrt{2} = a$ which is impossible since $a \in \mathbb{Q}$.
And if $a = 0$ then $\sqrt{2} = b\sqrt{3}$ which means $b = \frac{\sqrt{2}}{\sqrt{3}}$ which is also impossible since $b \in \mathbb{Q}$.

So $2 = (a^2 + 3b^2) + (2ab\sqrt{3})$ so that $\sqrt{3} = \frac{2-(a^2+3b^2)}{2ab}$ which is impossible since $\sqrt{3} \notin \mathbb{Q}$, whereas the right hand side *is* in $\mathbb{Q}$ of course.
In general no element $c + d\sqrt{2} \in \mathbb{Q}(\sqrt{3})$ either.

This implies then that $\mathbb{Q}(\sqrt{3},\sqrt{2})$ is an extension field of *both* $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{2})$, which we can diagram:



where $[\mathbb{Q}(\sqrt{3},\sqrt{2}):\mathbb{Q}(\sqrt{3})]=2$ and $[\mathbb{Q}(\sqrt{3},\sqrt{2}):\mathbb{Q}(\sqrt{2})]=2$ so $[\mathbb{Q}(\sqrt{3},\sqrt{2}):\mathbb{Q}]=4$ which can be verfied independently since $\{1,\sqrt{2},\sqrt{3},\sqrt{2}\sqrt{3}=\sqrt{6}\}$ is a basis for $\mathbb{Q}(\sqrt{3},\sqrt{2})$ over $\mathbb{Q}$.

i.e. $\mathbb{Q}(\sqrt{3},\sqrt{2}) = \mathbb{Q}(\sqrt{3})(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}(\sqrt{3})\}$ so that

$$a + b\sqrt{2} = (c + d\sqrt{3}) + (e + f\sqrt{3})\sqrt{2} = c + d\sqrt{3} + e\sqrt{2} + f\sqrt{6}$$

i.e. a linear combination of $\{1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3} = \sqrt{6}\}$.

What we shall show (to finish the argument) is that $\mathbb{Q}(\sqrt{3}+\sqrt{2}) = \mathbb{Q}(\sqrt{3},\sqrt{2})$ which means that $irr(\sqrt{3}+\sqrt{2}, \mathbb{Q})$ must be degree 4 and therefore equal to $f(x) = x^4 - 10x^2 + 1$.

To show $\mathbb{Q}(\sqrt{3}+\sqrt{2}) = \mathbb{Q}(\sqrt{3},\sqrt{2})$ is actually relatively easy.

Consider

$$\frac{1}{\sqrt{3}+\sqrt{2}} = \frac{1}{\sqrt{3}+\sqrt{2}}\frac{\sqrt{3}-\sqrt{2}}{\sqrt{3}-\sqrt{2}} = \sqrt{3}-\sqrt{2}$$

which is slightly unexpected, but odd relations like this are quite common when one deals with radical expressions.

The point is $\mathbb{Q}(\sqrt{3}+\sqrt{2})$ contains $\sqrt{3}-\sqrt{2}$ which means it contains

$$\sqrt{3}+\sqrt{2}+(\sqrt{3}-\sqrt{2}) = 2\sqrt{3} \text{ and } \sqrt{3}+\sqrt{2}-(\sqrt{3}-\sqrt{2}) = 2\sqrt{2}$$

and therefore $\sqrt{2}$ and $\sqrt{3}$ independently.

Thus $\mathbb{Q}(\sqrt{3},\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{3}+\sqrt{2})$, and since $\mathbb{Q}(\sqrt{3}+\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{3},\sqrt{2})$ they must be equal.

Thus $[\mathbb{Q}(\sqrt{3}+\sqrt{2}):\mathbb{Q}] = 4 = deg(x^4 - 10x^2 + 1)$ and so $x^4 - 10x + 1$ must equal $irr(\sqrt{3}+\sqrt{2},\mathbb{Q})$ since

$$deg(irr(\sqrt{3}+\sqrt{2},\mathbb{Q})) = [\mathbb{Q}(\sqrt{3}+\sqrt{2}):\mathbb{Q}] = 4$$

and $irr(\sqrt{3}+\sqrt{2},\mathbb{Q}) | x^4 - 10x^2 + 1$.

Theorem

If E is a finite extension of F then E is an algebraic extension of F.

PROOF: First we recall that E being algebraic over F means that *all* elements of E are roots of polynomials in $F[x]$.
So since E is finite over F then $[E:F]=n$ for some fixed integer $n\geq 1$.
If $\beta\in E$ is a non-zero element, then consider the set
$S=\{1=\beta^0,\beta,\beta^2,\beta^{n-1},\beta^n\}$ which contains $n+1$ elements.
By basic linear algebra, the largest linearly independent set in a vector space of dimension n has n elements, so therefore an $n+1$ element set like S must be linearly *dependent* and so there is a linear dependence relation

$$c_n\beta^n+\cdots+c_1\beta+c_0=0 \quad c_i\in F$$

ergo for $f(x)=c_nx^n+\cdots+c_1x+c_0\in F[x]$ we have $f(\beta)=0$ and so β is algebraic over F. □.

The converse of this is false.

For example $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots)$, namely the field obtained by adjoining $\sqrt{p}$ for all primes p, is algebraic over $\mathbb{Q}$ but is definitely not a finite extension of $F = \mathbb{Q}$.

Recall that for finite groups, LaGrange's theorem was an **immensely** ubiquitous and useful result that one uses frequently in proving different facts about groups.

Indeed, one of the first results one showed was that all groups of order p are cyclic, and thus unique.

In particular, we had the fact that for $K \leq H \leq G$ one has $[G:K] = [G:H][H:K]$ for a (finite) group G with subgroups H and K.

In particular, if for example $[G:K] = p$ for p prime that either $[G:H] = 1$ and $[H:K] = p$ or vice/versa.

In this same spirit we have the following fact about the degree $[E:F]$ of a field extension E/F.

Theorem

Let K be a finite extension of E and E a finite extension of F then K is a finite extension of F, and in fact, $[K:E][E:F]=[K:F]$.

PROOF: The proof of this is, more or less, a linear algebra argument.

So we have that $F\subseteq E\subseteq K$, where say $[K:E]=n$ and $[E:F]=m$, so suppose $X=\{x_1,\dots,x_n\}$ is a basis for K over E and $Y=\{y_1,\dots,y_m\}$ is a basis for E over F.

We wish to show that $YX=\{y_jx_i \mid j=1,\dots,m; i=1,\dots,n;\}$ is a basis for K over F.

The main challenge is to keep track of the 'bookkeeping'.

Let $v \in K$ with $v = c_1x_1 + c_2x_2 + \cdots + c_nx_n$, expressed as an E-linear combination of the basis elements in X, that is, each $c_i \in E$.

And since each $c_i \in E$ then $c_i = d_{i1}y_1 + d_{i2}y_2 + \cdots + d_{im}y_m$ for coefficients $d_{ij} \in F$, which yields

$$\begin{aligned} v =& (d_{11}y_1 + d_{12}y_2 + \cdots + d_{1m}y_m)x_1 + \\ & (d_{21}y_1 + d_{22}y_2 + \cdots + d_{2m}y_m)x_2 + \\ & \vdots \\ & (d_{n1}y_1 + d_{n2}y_2 + \cdots + d_{nm}y_m)x_n \end{aligned}$$

PROOF (continued)
But this means

$$
\begin{aligned}
v = & d_{11}\mathbf{y_1}\mathbf{x_1} + d_{12}\mathbf{y_2}\mathbf{x_1} + \cdots + d_{1m}\mathbf{y_m}\mathbf{x_1} + \\
& d_{21}\mathbf{y_1}\mathbf{x_2} + d_{22}\mathbf{y_2}\mathbf{x_2} + \cdots + d_{2m}\mathbf{y_m}\mathbf{x_2} + \\
& \vdots \\
& d_{n1}\mathbf{y_1}\mathbf{x_n} + d_{n2}\mathbf{y_2}\mathbf{x_n} + \cdots + d_{nm}\mathbf{y_m}\mathbf{x_n}
\end{aligned}
$$

which implies that YX spans K as a vector space over F.

And by letting $v = 0$, one can, using the linear independence of X over E and the linear independence of E over F deduce that YX is linearly independent over F, and so YX is a basis of K over F.

Moreover, we deduce that $[K : F] = |YX| = |Y| \cdot |X| = [K : E][E : F]$, and that K therefore is obviously a finite extension of F. $\square$

One *extremely* simple consequence of this fact is the following.

Proposition

There is no field properly contained between $\mathbb{R}$ and $\mathbb{C}$.

Proof.

If $\mathbb{R} \subseteq E \subseteq \mathbb{C}$ then $[\mathbb{C} : E][E : \mathbb{R}] = [\mathbb{C} : \mathbb{R}]$.

But since $[\mathbb{C} : \mathbb{R}] = 2$ then either $[\mathbb{C} : E] = 1$ or $[E : \mathbb{R}] = 1$ and if $[K : F] = 1$ for K an extension field of F, it must be that $K = F$.

Thus either $E = \mathbb{C}$ or $E = \mathbb{R}$. □

And, more generally, if $[E:F]=p$ for p a prime then there is no intermediate field K between F and E as then $[E:K][K:F]=p$ so that either $[E:K]=1$ or $[K:F]=1$.

The degree formula is also used to determine the possible degrees of intermediate fields in general.