MA542 Lecture

Timothy Kohl

Boston University

March 24, 2025

Let's consider another splitting field.

Let $f(x) = x^4 - 2 \in \mathbb{Q}[x]$, and observe that the roots are $\pm\sqrt[4]{2}$,$\pm i\sqrt[4]{2}$ and so any splitting field must contain $\sqrt[4]{2}$ and i, so if E is a (the) splitting field for $f(x)$ over $\mathbb{Q}$ then E is contained in $\mathbb{Q}(i, \sqrt[4]{2})$, where a $\mathbb{Q}$ basis is

$$\{1, \sqrt[4]{2}, \sqrt[4]{2}^2, \sqrt[4]{2}^3, i, i\sqrt[4]{2}, i\sqrt[4]{2}^2, i\sqrt[4]{2}^3\}$$

so $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}] = 8$ and thus $[\mathbb{Q}(i, \sqrt[4]{2}) : E][E : \mathbb{Q}] = 8$.

Now, since $\mathbb{Q}(i, \sqrt[4]{2}) \supseteq E \supseteq \mathbb{Q}$ then $[E : \mathbb{Q}] = 1, 2, 4,$or 8.

But since $\sqrt[4]{2} \in E$ then $[E : \mathbb{Q}] \geq [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ and since $i \notin \mathbb{Q}(\sqrt[4]{2})$ then E properly contains $\mathbb{Q}(\sqrt[4]{2})$ so in fact $[E : \mathbb{Q}] = 8$ which implies that $E = \mathbb{Q}(i, \sqrt[4]{2})$.

Here is a another example; let's prove $\mathbb{Q}(2^{1/2}, 2^{1/3}) = \mathbb{Q}(2^{1/6})$.

First note that $(2^{1/6})^3 = 2^{1/2}$ and $(2^{1/6})^2 = 2^{1/3}$, so $\mathbb{Q}(2^{1/6})$ contains both $\mathbb{Q}(2^{1/2})$ and $\mathbb{Q}(2^{1/3})$ and $[\mathbb{Q}(2^{1/6}) : \mathbb{Q}] = 6$ since $\{1, 2^{1/6}, 2^{2/6}, \dots, 2^{5/6}\}$ is a basis, and so

$$[\mathbb{Q}(2^{1/6}) : \mathbb{Q}(2^{1/2}, 2^{1/3})][\mathbb{Q}(2^{1/2}, 2^{1/3}) : \mathbb{Q}] = [\mathbb{Q}(2^{1/6}) : \mathbb{Q}] = 6$$

But now we can subdivide this further since obviously $\mathbb{Q}(2^{1/2}, 2^{1/3})$ contains $\mathbb{Q}(2^{1/2})$ so

$$[\mathbb{Q}(2^{1/6}) : \mathbb{Q}(2^{1/2}, 2^{1/3})][\mathbb{Q}(2^{1/2}, 2^{1/3}) : \mathbb{Q}(2^{1/2})][\mathbb{Q}(2^{1/2}) : \mathbb{Q}] = [\mathbb{Q}(2^{1/6}) : \mathbb{Q}]$$

where $[\mathbb{Q}(2^{1/2} : \mathbb{Q}] = 2$ of course, so

$$[\mathbb{Q}(2^{1/6}) : \mathbb{Q}(2^{1/2}, 2^{1/3})][\mathbb{Q}(2^{1/2}, 2^{1/3}) : \mathbb{Q}(2^{1/2})] = 3$$

so $[\mathbb{Q}(2^{1/2}, 2^{1/3}) : \mathbb{Q}(2^{1/2})]$ is 1 or 3, so why can't it be 1?

i.e. Is it possible that $2^{1/3} \in \mathbb{Q}(2^{1/2})$?

No, and we shall show more generally that $\mathbb{Q}(2^{1/2}) \cap \mathbb{Q}(2^{1/3}) = \mathbb{Q}$.

First, since $[\mathbb{Q}(2^{1/2}) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(2^{1/3}) : \mathbb{Q}] = 3$ then

$$[\mathbb{Q}(2^{1/2}) : \mathbb{Q}(2^{1/2}) \cap \mathbb{Q}(2^{1/3})][\mathbb{Q}(2^{1/2}) \cap \mathbb{Q}(2^{1/3}) : \mathbb{Q}] = [\mathbb{Q}(2^{1/2}) : \mathbb{Q}] = 2$$
$$[\mathbb{Q}(2^{1/3}) : \mathbb{Q}(2^{1/2}) \cap \mathbb{Q}(2^{1/3})][\mathbb{Q}(2^{1/2}) \cap \mathbb{Q}(2^{1/3}) : \mathbb{Q}] = [\mathbb{Q}(2^{1/3}) : \mathbb{Q}] = 3$$

so $[\mathbb{Q}(2^{1/2}) \cap \mathbb{Q}(2^{1/3}) : \mathbb{Q}]$ is a divisor of 2 and 3, so it's 1.

As such, $[\mathbb{Q}(2^{1/2}, 2^{1/3}) : \mathbb{Q}(2^{1/2})] = 3$ and so $[\mathbb{Q}(2^{1/6}) : \mathbb{Q}(2^{1/2}, 2^{1/3})] = 1$ and so $\mathbb{Q}(2^{1/6}) = \mathbb{Q}(2^{1/2}, 2^{1/3})$.

Primitive Element Theorem

We've seen, for example, that $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ and so one wonders if this is always the case.

That is, for α,β algebraic over F, does there exist an element γ such that $F(\alpha,\beta) = F(\gamma)$, where now $F(\gamma)$ is what we call a simple extension (generated by a single alebraic element) so that a basis consists of powers of γ, namely $\{1,\gamma,\dots,\gamma^{n-1}\}$ where $[F(\alpha,\beta):F] = [F(\gamma):F] = n$.

If so, we call γ a *primitive element*.

We note that, in the $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ case we obtained the primitive element $\sqrt{2}+\sqrt{3}$ by simply adding together the $\sqrt{2}$ and $\sqrt{3}$.

Does this work in general? almost...

Theorem

If $char(F) = 0$ or F is a finite field, and α, β are algebraic over F then there exists a primitive element γ so that $F(\alpha, \beta) = F(\gamma)$.

PROOF: (Sketch) If F is a finite field, then for α, β algebraic over F, one has that $E = F(\alpha, \beta)$ is finite as well, and one can show that, in fact, $E^* = E - \{0\}$ is a cyclic group under multiplication.

This means that there is a $\gamma \in E^*$ such that all non-zero elements of E are powers of γ, which means $F(\gamma) \supseteq E$, but since obviously $F(\gamma) \subseteq E$ we get that $E = F(\gamma)$.

PROOF (continued)
The proof for when $char(F) = 0$ can be found in the classic book by van der Waerden.

The key fact (which we proved earlier) is that if $char(F) = 0$ then any irreducible polynomial in $F[x]$ has no repeated roots.

As a result $\gamma = \alpha + \lambda\beta$ is a primitive element for $F(\alpha, \beta)$ (i.e. $F(\alpha, \beta) = F(\gamma)$) for all but finitely many $\lambda \in F$. $\square$

And indeed, frequently $\lambda = 1$ works, i.e. $F(\alpha, \beta) = F(\alpha + \beta)$ generally.

Note also, that this generalizes to field extensions of the form $F(\alpha_1, \alpha_2, \ldots, \alpha_m)$ (for $\alpha_1, \ldots, \alpha_m$ algebraic over F) in that these also have primitive elements γ such that $F(\alpha_1, \alpha_2, \ldots, \alpha_m) = F(\gamma)$.

Let's take a look at another example, namely the field $\mathbb{Q}(\sqrt[3]{2},\zeta_3)$ for $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$ which is the splitting field for $x^3 - 2 \in \mathbb{Q}[x]$.

First, we make a small adjustment, namely we observe that since $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$ then $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ and so $\mathbb{Q}(\sqrt[3]{2},\zeta_3) = \mathbb{Q}(\sqrt[3]{2},\sqrt{-3})$.

We claim that $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) = \mathbb{Q}(\sqrt[3]{2} + \sqrt{-3})$.

First, note that $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2, \sqrt{-3}, \sqrt{-3}\sqrt[3]{2}, \sqrt{-3}\sqrt[3]{2}^2\}$ is a basis for $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ over $\mathbb{Q}$.

We will, for notational convenience, denote this set $\{v_1, v_2, v_3, v_4, v_5, v_6\}$.

One can show, by foiling things out that for $\gamma = \sqrt[3]{2} + \sqrt{-3}$ one has:

$$
\begin{aligned}
\gamma^0 &= v_1 \\
\gamma^1 &= v_2 + v_4 \\
\gamma^2 &= -3v_1 + v_3 + 2v_5 \\
\gamma^3 &= 2v_1 - 9v_2 - 3v_4 + 3v_6 \\
\gamma^4 &= 9v_1 + 2v_2 - 18v_3 + 8v_4 - 12v_5 \\
\gamma^5 &= -60v_1 + 45v_2 + 2v_3 + 9v_4 + 10v_5 - 30v_6
\end{aligned}
$$

and we can show that these linear combinations of the $\{v_i\}$ are a linearly independent set since the matrix

$$
\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 \\
-3 & 0 & 1 & 0 & 2 & 0 \\
2 & -9 & 0 & 3 & 0 & 3 \\
9 & 2 & -18 & 8 & -12 & 0 \\
-60 & 45 & 2 & 9 & 10 & -30
\end{bmatrix}
$$

row reduces to the identity.

So this shows that $\{1, \gamma^1, \ldots, \gamma^5\}$ is also a basis of $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ and so $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) = \mathbb{Q}(\sqrt[3]{2} + \sqrt{-3})$.

What we can also prove (albeit with some amount of computation!) is that $\sqrt[3]{2} + \sqrt{-3}$ is a root of

$$p(x) = x^6 + 9x^4 - 4x^3 + 27x^2 + 36X + 31$$

but the question is whether $p(x) = irr(\sqrt[3]{2} + \sqrt{-3}, \mathbb{Q})$.

So we can ask, for $\gamma = \sqrt[3]{2} + \sqrt{-3}$, is γ the root of a quadratic $x^2 + ax + b$? If it were then we would have

$$(-3v_1 + v_3 + 2v_5) + a(v_2 + v_4) + bv_1 = 0$$

namely $(-3 + b)v_1 + av_2 + v_3 + av_4 + 2v_5 = 0$ which is impossible since $v_1, \ldots, v_5$ belong to the basis so they are linearly independent.

Similarly, γ is not the root of a cubic $x^3 + ax^2 + bx + c$, nor of any quadratic, or quintic.
We derived what the powers of $\{\gamma^0, \ldots, \gamma^5\}$ look like as linear combinations of $\{v_1, \ldots, v_6\}$.

We can show that $\gamma^6 = -23v_1 - 90v_2 + 135v_3 - 120v_4 + 54v_5 + 12v_6$ which we write as a linear combination of $\{\gamma^0, \ldots, \gamma^5\}$ in that

$$\begin{aligned}
\gamma^0 &= v_1 \\
\gamma^1 &= v_2 + v_4 \\
\gamma^2 &= -3v_1 + v_3 + 2v_5 \\
\gamma^3 &= 2v_1 - 9v_2 - 3v_4 + 3v_6 \\
\gamma^4 &= 9v_1 + 2v_2 - 18v_3 + 8v_4 - 12v_5 \\
\gamma^5 &= -60v_1 + 45v_2 + 2v_3 + 9v_4 + 10v_5 - 30v_6
\end{aligned}$$

and we find that $\gamma^6 = -9\gamma^4 + 4\gamma^3 - 27\gamma^2 - 36\gamma - 31\gamma^0$ i.e. $p(\gamma) = 0$.
So $irr(\gamma, \mathbb{Q}) = p(x) = x^6 + 9x^4 - 4x^3 + 27x^2 + 36X + 31$.

Thus

$$\mathbb{Q}(\sqrt[3]{2}, \zeta_3) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) = \mathbb{Q}(\sqrt[3]{2} + \sqrt{-3}) \cong \mathbb{Q}[x]/\langle p(x) \rangle$$

where $p(x) = x^6 + 9x^4 - 4x^3 + 27x^2 + 36X + 31 = irr(\sqrt[3]{2} + \sqrt{-3}, \mathbb{Q})$.

Algebraic Extensions of Algebraic Extensions

Theorem

If K is algebraic over E and E is algebraic over F then K is algebraic over F.

PROOF: Let $\alpha \in K$ then $p(\alpha) = 0$ for $p(x) = b_n x^n + \cdots + b_0 \in E[x]$ an irreducible polynomial.

So, we have that the $b_i \in E$ where E is algebraic over F, so consider the following set of extensions of F.

PROOF (continued)

$$\begin{aligned} F_0 &= F(b_0) \\ F_1 &= F_0(b_1) = F(b_0, b_1) \\ &\vdots \\ F_{n-1} &= F_{n-2}(b_{n-1}) \\ F_n &= F_{n-1}(b_n) = F(b_0, b_1, \ldots, b_n) \end{aligned}$$

and since each $b_i \in E$ (which is algebraic over F) we have that $[F_0 : F]$, $[F_1 : F_0]$,...,$[F_n : F_{n-1}]$ are all finite.

Moreover $b_0 \in F_0$, $b_0, b_1 \in F_1$,...,$b_n, b_{n-1}, \ldots, b_0 \in F_n$.

PROOF (continued)
So $p(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$ must be in $F_n[x]$ and α being a root of $p(x)$ means that α is algebraic over F_n so $[F_n(\alpha) : F_n]$ is finite.

But now,
$[F_n(\alpha) : F] = [F_n(\alpha) : F_n][F_n : F_{n-1}][F_{n-1} : F_{n-2}] \cdots [F_1 : F_0][F_0 : F]$
which is a finite product of finite values and is therefore finite.

i.e. α belongs to a field $F_n(\alpha)$ which is of finite degree over F (and therefore an algebraic extension of F) so α must be algebraic over F. $\square$