Lecture 17: Algebraic Field Extensions

Algebraic extensions are our primary focus.

Let K be an extension of the field F.

Def^n/ The element $\alpha \in K$ is said to be <u>algebraic</u> over F if α is a root of some nonzero $f(x) \in F[x]$. If α is not algebraic over F then α is said to be <u>transcendental</u> over F. The extension K/F is said to be <u>algebraic</u> if <u>every</u> element of K is algebraic over F.

Notice that if α is algebraic over F and L is an extension of F then α is algebraic over L as well.

Proposition (9): Let α be algebraic over F. Then $\exists!$ monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ which has α as a root. A polynomial $f(x) \in F[x]$ has α as a root iff $m_{\alpha,F}(x)$ divides $f(x)$ in $F[x]$

Proof: we may cover in-class, it's on p. 520 of D&F. //
(I go through it next page, it's not hard)

Corollary (10): If L/F is an extension of fields and α is algebraic over both F and L then $m_{\alpha,L}(x)$ divides $m_{\alpha,F}(x)$ in $L[x]$

$\boxed{E1}$ $\mathbb{C}/\mathbb{R}$ has i algebraic over $\mathbb{R}$ and $\mathbb{C}$, $\left(\begin{array}{l} m_{i,\mathbb{C}}(x) = x - i \\ m_{i,\mathbb{R}}(x) = x^2+1 \end{array}\right)$

Proposition (9)

Let α be algebraic over F. Then $\exists!$ monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ which has α as a root. A polynomial $f(x) \in F[x]$ has α as root iff $m_{\alpha,F}(x)$ divides $f(x)$ in $F[x]$

Proof: Suppose α is algebraic over F, then suppose $g(x)$ is poly. of minimal degree with $g(\alpha) = 0$. Without loss of generality we can make $g(x)$ monic by multiplying by appropriate unit. If $g(x)$ is reducible then $g(x) = a(x)\,b(x)$ where $a(x), b(x) \in F[x]$ and $a(x), b(x)$ have lesser degree than $g(x)$. Then

$$g(\alpha) = a(\alpha)\,b(\alpha) = 0$$

hence either $a(\alpha) = 0$ or $b(\alpha) = 0$ contradicting construction of g. Thus $g(x)$ is irreducible. NEXT, suppose $f(x) \in F[x]$ with $f(\alpha) = 0$ then divide $f(x)$ by $g(x)$ to find $q(x), r(x) \in F[x]$ for which $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$ and

$$f(x) = g(x)\,q(x) + r(x)$$

then $f(\alpha) = g(\alpha)\,q(\alpha) + r(\alpha) \Rightarrow r(\alpha) = 0 \Rightarrow r(x) = 0$ by minimality of $g(x)$. Thus $f(x) = g(x)\,q(x)$. Consequently $g(x)$ divides $f(x)$. Conversely, if $g(x) \mid f(x)$ then $f(x) = g(x)\,q(x)$ for some $q(x) \in F[x]$ and $\therefore$ $f(\alpha) = g(\alpha)\,q(\alpha) = 0$.

Proposition 11

Let α be algebraic over F and let $F(\alpha)$ be the field generated by α over F. Then

$$F(\alpha) \cong \frac{F[x]}{(m_\alpha(x))}$$

Hence $[F(\alpha):F] = \deg(m_\alpha(x)) = \deg(\alpha)$

Lest we forget to define, assume α algebraic over F

Def^n/ The polynomial $m_{\alpha,F}(x)$ (or $m_\alpha(x)$ where context allows) which is monic and irreducible $\ni$ such that $m_{\alpha,F}(\alpha) = 0$ is called the <u>minimal polynomial</u> for α over F. Also, $\deg(\alpha) = \deg(m_{\alpha,F}(x))$.

$\boxed{E2}$ $\alpha = \sqrt{2}$ has $m_{\sqrt{2},\mathbb{Q}}(x) = x^2 - 2$, $\deg(\sqrt{2}) = 2$ over $\mathbb{Q}$.

$\boxed{E3}$ $\alpha = \sqrt{67}$ has $m_{\sqrt{67}}(x) = x^2 - 67 \in \mathbb{Q}[x]$ thus $\deg(\sqrt{67}) = 2$ over $\mathbb{Q}$.

$\boxed{E4}$ $\alpha = \sqrt[n]{2}$ has $m_{\alpha,\mathbb{R}}(x) = x - \sqrt[n]{2}$

$\therefore \deg(\sqrt[n]{2}) = 1$ over $\mathbb{R}$

whereas $m_{\alpha,\mathbb{Q}}(x) = x^n - 2 \therefore \deg(\sqrt[n]{2}) = n$ over $\mathbb{Q}$.

Remark: irreducibility of above polynomials thanks to <u>Eisenstein</u>.

Proposition 12:

The element α is algebraic over F iff the simple extension $F(\alpha)/F$ is finite. More precisely, if α is an element of an extension of degree n over F then α satisfies a poly. of degree at <u>most</u> n over F and if α satisfies a poly. of degree n over F then the deg of $F(\alpha)$ over F is at most n.

<u>Proof</u>: If α algebraic over F then $[F(\alpha):F] = \deg(m_{\alpha,F}(x))$. Hence $[F(\alpha);F] < \infty$. Conversely, suppose α is an element with $F(\alpha)/F$ with $[F(\alpha):F] = n$ then $1, \alpha, \alpha^2, \ldots, \alpha^n$ is linearly dependent. Consequently, $\exists\, b_0, \ldots, b_n \in F$ with at least one nonzero b_j such that $b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_n\alpha^n = 0$. Hence $b(x) = b_0 + b_1 x + \cdots + b_n x^n \in F[x]$ is nonzero with $b(\alpha) = 0$ $\therefore$ α is algebraic over F.

<u>Remark</u>: key idea, if $[K:F] = n$ and $\alpha \in K$ then $F(\alpha) \subseteq K$ and thus $1, \alpha, \alpha^2, \ldots \in K \Rightarrow \underbrace{1, \alpha, \ldots, \alpha^n}_{n+1 \text{ vectors in } K}$ <u>not</u> LI

Corollary 13:

If the extension K/F is finite then it is algebraic

<u>Proof</u>: Suppose $\alpha \in K$ where K/F is finite. Then $F(\alpha)$ is a subfield of $K \Rightarrow F(\alpha)$ is <u>subspace</u> of K consequently, $[F(\alpha):F] \leq [K:F] = n$ $\therefore$ $F(\alpha)/F$ is finite and thus α is algebraic. //

$\boxed{E5}$ Suppose F is field with $\mathrm{char}(F) \neq 2$.
Let K be an extension of F of degree 2, $[K:F]=2$.
Suppose $\alpha \in K$ and $\alpha \notin F$. Since $F(\alpha) \subset K$ we know, by Prop. 12, α has $\deg(\alpha) \leq 2$ and $\deg(\alpha) \neq 1$ since $\alpha \notin F$ and $m_{\alpha,F}(x) = x+b \Rightarrow \alpha \in F \rightarrow\leftarrow$
$\therefore$ $m_{\alpha,F}(x) = x^2+bx+c$ for some $b, c \in F$
Then as $F \subseteq F(\alpha) \subseteq K$ and $\dim_F(F(\alpha)) = 2$ we find $F(\alpha) = K$.

<u>Complete The Square!</u>

$$x^2+bx+c = \left(x+\frac{b}{2}\right)^2 - \frac{b^2}{4} + c$$
$$= (x + b/2)^2 - \frac{b^2-4c}{4}$$
$$= \left(x + \frac{b}{2} + \frac{1}{2}\sqrt{b^2-4c}\right)\left(x + \frac{b}{2} - \frac{1}{2}\sqrt{b^2-4c}\right)$$

Identify $\alpha = \frac{-b \pm \sqrt{b^2-4c}}{2}$ and for $\alpha \notin F$ we need that $b^2-4c \neq \delta^2$ for any $\delta \in F$.
We can argue $F(\alpha) = F(\sqrt{b^2-4c})$ since if $\sqrt{b^2-4c}$ is in a field then $\frac{-b}{2} \pm \frac{\sqrt{b^2-4c}}{2} = \alpha$ is in the field as $b, 2 \in F$.

<u>Quadratic Extensions</u>: any extension K of F of degree 2 is of the form $F(\sqrt{D})$ where $D \in F$ and $D \neq \delta^2$ for some $\delta \in F$

Th$^{\underline{m}}$ (14) Let $F \subseteq K \subseteq L$ be fields. Then
$$[L:F] = [L:K][K:F]$$
where this has natural meaning when L/K and K/F is finite and also when either L/K or K/F is infinite then L/F is infinite.

Proof: Suppose $[L:K] = m$ and $[K:F] = n$.
Then $\exists$ basis $\underbrace{\alpha_1, \alpha_2, \ldots, \alpha_m}_{\beta}$ over K for $L = \text{span}_K(\beta)$
Likewise $\exists$ basis $\gamma = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ over F for $K = \text{span}_F(\gamma)$.
Let $x \in L$ then $\exists\, c_1, c_2, \ldots, c_m \in K$ s.t. $x = \sum_{i=1}^{m} c_i \alpha_i$.
Then $c_i \in K = \text{span}_F(\gamma)$ hence $\exists\, b_{ij} \in F$ s.t. $c_i = \sum_{j=1}^{n} b_{ij}\sigma_j$
thus $x = \sum_{i=1}^{m}\sum_{j=1}^{n} b_{ij}\sigma_j\alpha_i \in \text{span}_F(\Upsilon)$ where

$\Upsilon = \{\alpha_i\sigma_j \mid 1 \leq i \leq m,\ 1 \leq j \leq n\}$. It remains to prove Υ is LI from which we can see $|\Upsilon| = mn$ and $|\beta| = m$ and $|\gamma| = n$ so $[L:K][K:F] = mn = [L:F]$.
Suppose $\sum_{i=1}^{m}\sum_{j=1}^{n} b_{ij}\sigma_j\alpha_i = 0$ for $b_{ij} \in F$,

$$\Rightarrow \sum_{j=1}^{n} b_{ij}\sigma_j = 0 \quad \text{by LI of } \beta.$$

$$\Rightarrow b_{ij} = 0 \quad \text{by LI of } \gamma$$

$$\Rightarrow \Upsilon \text{ is LI.}$$

The infinite case follows from natural arguments as given on top of pg. 524 of D&F. //

Corollary (15)

Suppose L/F is finite extension and let K be any subfield of L containing F $(F \subseteq K \subseteq L)$. Then $[K:F]$ divides $[L:F]$

These results are very simple and natural, but I think their application requires some new thinking.

$\boxed{E6}$ Consider α the real root of $x^3 - 3x - 1$ which falls between 0 and 2. We can argue $\sqrt{2} \notin \mathbb{Q}(\alpha)$ as $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ whereas $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ and $\sqrt{2} \in \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\alpha)$

$\Rightarrow [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$ divides $[\mathbb{Q}(\alpha) : \mathbb{Q}]$

$\Rightarrow 2$ divides 3. (nope.)

$\therefore \sqrt{2} \notin \mathbb{Q}(\alpha)$.

$\boxed{E7}$ $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$

$(\sqrt[6]{2})^3 = 2^{3/6} = \sqrt{2} \Rightarrow \sqrt{2} \in \mathbb{Q}(\sqrt[6]{2})$

$\Rightarrow \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[6]{2})$

$\mathbb{Q}(\sqrt[6]{2})$

| $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt{2})] = 3$ ← minimal poly. of $\sqrt[6]{2}$ over $\mathbb{Q}(\sqrt{2})$ is degree 3.

$\mathbb{Q}(\sqrt{2})$

| $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$

$\mathbb{Q}$

$m_{\sqrt[6]{2},\, \mathbb{Q}(\sqrt{2})}(x) = x^3 - \sqrt{2}$.

Def^n/ An extension K/F is <u>finitely generated</u> if $\exists$ elements $\alpha_1, \alpha_2, \ldots, \alpha_k$ in K such that $K = F(\alpha_1, \alpha_2, \ldots, \alpha_k)$

We defined $F(\alpha_1, \alpha_2, .., \alpha_k)$ to be smallest field containing both F and the elements $\alpha_1, \alpha_2, .., \alpha_k$. You can find proof of the Lemma below on p. 525

<u>Lemma 16</u>: $F(\alpha, \beta) = (F(\alpha))(\beta)$ that is, the field generated over F by α & β is the same as the field generated by β over the field $F(\alpha)$ gen. by α.

<u>Proof</u>: the field $F(\alpha,\beta)$ contains F and α $\therefore$ contains $F(\alpha)$ moreover $F(\alpha,\beta)$ also contains $\beta \Rightarrow (F(\alpha))(\beta) \subseteq F(\alpha,\beta)$. Likewise, $(F(\alpha))(\beta)$ contains $F, \alpha, \beta \Rightarrow F(\alpha,\beta) \subseteq (F(\alpha))(\beta)$ by supposed minimality of $F(\alpha,\beta)$. //

We can iterate the process of Lemma 16,

$$\begin{aligned} F(\alpha_1, \alpha_2, \alpha_3) &= (F(\alpha_1, \alpha_2))(\alpha_3) \\ &= ((F(\alpha_1))(\alpha_2))(\alpha_3) \text{ etc.} \end{aligned}$$

$\boxed{E8}$ $\mathbb{Q}(\sqrt[6]{2}, \sqrt{2}) = \mathbb{Q}(\sqrt[6]{2})$ since $\sqrt{2} = (\sqrt[6]{2})^3$
$\alpha = \sqrt{2}$ has degree 1 over $\mathbb{Q}(\sqrt[6]{2})$.

E9 Let's study $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

We wish to show $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

- Since $\deg(\sqrt{3}) = 2$ over $\mathbb{Q}$

  $\Rightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3}) / \mathbb{Q}(\sqrt{2})$ is degree at most 2 extension

- If $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$, so we need to show $x^2 - 3$ has no root in $\mathbb{Q}(\sqrt{2})$.

  That is, we need $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Suppose $a, b \in \mathbb{Q}$ and

$$\sqrt{3} = a + b\sqrt{2}$$
$$3 = (a + b\sqrt{2})^2 = a^2 + 2ab\sqrt{2} + 2b^2$$

  If $ab \neq 0$ then $\sqrt{2} = \frac{3 - a^2 - 2b^2}{2ab} \in \mathbb{Q}$ (impossible)

  If $b = 0$ then $\sqrt{3} = a \in \mathbb{Q}$ (impossible)

  If $a = 0$ then $\sqrt{3} = b\sqrt{2} \Rightarrow \sqrt{6} = 2b \in \mathbb{Q}$ (impossible)

- Thus $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ and

$$\underbrace{[\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}]}_{4} = \underbrace{[\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}(\sqrt{2})]}_{2} \underbrace{[\mathbb{Q}(\sqrt{2}), \mathbb{Q}]}_{2}$$

Th^{m} (17) The extension K/F is finite iff K is generated by finite # of algebraic elements over F. More precisely, a field generated by finite # of algebraic elements of degrees $n_1, n_2, \ldots, n_k$ is algebraic of degree $\leq n_1 n_2 \cdots n_k$

Corollary (18) Suppose α and β are algebraic over F. Then $\alpha \pm \beta$, $\alpha\beta$, α/β (for $\beta \neq 0$) and α^{-1} for $\alpha \neq 0$ are all algebraic.

Corollary (19) Let L/F be arbitrary extension. Then the collection K of elements of L that are algebraic over F form a subfield of K of L.

E10 ALGEBRAIC NUMBERS

If we consider $\mathbb{C}/\mathbb{Q}$ then $\overline{\mathbb{Q}}$ denotes the subfield of all algebraic elements of $\mathbb{C}$ over $\mathbb{Q}$. This is an infinite subfield (in terms of rational dimension).

Notice $\sqrt[n]{2} \in \overline{\mathbb{Q}}$ for $n = 2, 3, 4, \dots$ thus

$\{1, \sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \dots\}$ is LI over $\mathbb{Q}$ subset of $\overline{\mathbb{Q}}$.

$\therefore\ [\overline{\mathbb{Q}} : \mathbb{Q}] \geq n$ for all $n \in \mathbb{N}$, $n > 1$.

Def^{n}/ $\overline{\mathbb{Q}}$ is the set of complex numbers which are algebraic over $\mathbb{Q}$.

Remark: we can argue $\overline{\mathbb{Q}}$ is countable thus $\mathbb{C}$ (which is uncountable) has $\overline{\mathbb{Q}}$ as proper subfield. Likewise $\overline{\mathbb{Q}} \cap \mathbb{R} \subseteq \mathbb{R}$ gives a countable subfield of real algebraic #'s, again a proper subfield of the uncountable $\mathbb{R}$.

Th^{m} (20)

If K is algebraic over F and L is algebraic over K then L is algebraic over F

Def^{n}/ Let K_1 and K_2 be subfields of K. Then the composite field of K_1 & K_2, denoted K_1K_2, is the smallest subfield of K containing K_1 & K_2. We define $K_1K_2 \cdots K_n$ in like fashion.

E11 $\mathbb{Q}(\sqrt{2})\,\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$ since both fields contain $\sqrt{2}$ and $\sqrt[3]{2}$ since $(\sqrt[6]{2})^3 = \sqrt{2}$, $(\sqrt[6]{2})^2 = \sqrt[3]{2}$ and $\frac{\sqrt{2}}{\sqrt[3]{2}} = \sqrt[6]{2}$

PROPOSITION (21)

Let K_1 and K_2 be two finite extensions of a field F contained in K. Then

$$[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$$

with equality iff an F-basis for one of the fields remains LI over the other field. If $\alpha_1, .., \alpha_m$ and $\beta_1, \dots, \beta_n$ we bases for K_1 & K_2 respective, then the elements $\alpha_i\beta_j$ for $i = 1, .., m$, $j = 1, .., n$ span K_1K_2

Proof: Note $K_1K_2 = F(\alpha_1, .., \alpha_m), \beta_1, .., \beta_n) = K_1(\beta_1, .., \beta_n)$

we see $\beta_1, .., \beta_n$ span K_1K_2 over K_1 $\therefore$ $[K_1K_2 : K_1] \leq m = [K_2 : F]$

where $=$ is attained if $\{\beta_1, \dots, \beta_n\}$ is LI over K_1.

Observe $[K_1K_2 : F] = [K_1K_2 : K_1][K_1 : F]$

$$\leq [K_2 : F][K_1 : F]. //$$

GRAPHICALLY

$$\begin{tikzcd} & K_1K_2 & \\ K_1 \arrow[ur, dash, "\leq m"] & & K_2 \arrow[ul, dash, "\leq n"'] \\ & F \arrow[ul, dash, "n"] \arrow[ur, dash, "m"'] & \end{tikzcd}$$

Corollary (22)

Suppose $[K_1 : F] = n$ and $[K_2 : F] = m$ as in above proposition, and suppose $\gcd(m, n) = 1$ then,

$$[K_1K_2 : F] = [K_1 : F][K_2 : F] = nm$$

Proof: can you prove this?

$\boxed{E12}$ the composite of the fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt[3]{2})$ have $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$

hence $\gcd(2, 3) = 1 \Rightarrow [\underbrace{\mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt[3]{2})} : \mathbb{Q}] = 6$

E11, we saw this was $\mathbb{Q}(\sqrt[6]{2})$.