§13.2 ALGEBRAIC EXTENSIONS

Let $F$ be a field and $K/F$ be a field extension.

Def. An element $\alpha \in K$ is algebraic over $F$ if $\alpha$ is a root of a polynomial in $F[x]$.

If $\alpha$ is not algebraic, $\alpha$ is TRANSCENDENTAL over $F$.

If all $\alpha \in K$ are algebraic over $F$, then $K/F$ is an ALGEBRAIC EXTENSION.

Proof. Let $\alpha \in K$ be algebraic over $F$. Then there exists a unique, monic, irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ for which $\alpha$ is a root.

Also, if $\alpha$ is a root of some $f(x) \in F[x]$, then $m_{\alpha,F}(x) \mid f(x)$.

If $g(x) = g_n x^n + \ldots + g_0$ for $g_0, \ldots, g_n \in F$ have $\alpha$ as a root, of minimal degree $n > 0$. Replacing $g(x)$ with $\left(\frac{1}{g_n}\right)g(x)$ can assume $g(x)$ monic.
Suppose \( g(x) = a(x)b(x) \) in \( F[x] \).

then \( a(a) b(a) = g(a) = 0 \) in \( F \)

\[ \Rightarrow \exists \mu \text{ such that } a(a) = 0 \text{ or } b(a) = 0 \]

By choice of \( g(x) \), one of \( a(x) \) or \( b(x) \) must be scalar, the other degree \( m \), i.e. one of \( a(x) \) or \( b(x) \)

is a unit in \( F[x] \) and so \( g(x) \) irreducible.

Now suppose \( \alpha \) is a root of \( f(x) \in F[x] \),

\( f(\alpha) \neq 0 \) using the division algorithm, write

\[ f(x) = q(x)g(x) + r(x) \]

for \( q(x), r(x) \in F[x] \) and with either \( r(x) = 0 \) or \( \deg r(x) < \deg g(x) \).

Note:

\[ r(\alpha) = f(\alpha) - q(\alpha)g(\alpha) = 0 \]

Due to minimal degree (or all assumptions on \( g(x) \)).

see that \( r(\alpha) = 0 \), and thus \( g(x) \mid f(x) \) in \( F[x] \).

Remaining: \( g(x) \) is unique.

Suppose \( p(x) \) is monic irreducible polynomial in \( F[x] \)

with root \( \alpha \).

Then by the above, \( g(x) \mid p(x) \), since \( p(x) \) irreducible,

\( g(x), p(x) \) associates, both monic \( \Rightarrow g(x) = p(x) \).
Def. Let $\alpha \in K$, a \textit{algebraic over} $F$. Using the \textit{proceeding}, refer to the unique \textit{monic irreducible polynomial in} $F[x]$ \textit{vanishing at} $\alpha$ as the \textit{minimal polynomial} of $\alpha$ over $F$, written $m_{\alpha,F}(x)$.

Corollary: Let $F \subseteq L \subseteq K$ be field extensions and suppose $\alpha \in K$ is algebraic over both $F$ and $L$. Then $m_{\alpha,L}(x) \mid m_{\alpha,F}(x)$ in $L[x]$.

Proof (using proceeding). \hfill \Box

Recall from last time: suppose $\alpha \in K$ is algebraic over $F$, $m(x)$ is its minimal polynomial over $F$ for $\alpha$, $\deg m(x) = n$.

Then $F(\alpha) \cong F[x]/\langle m(x) \rangle$ \hfill [proved last time]

$[F(\alpha) : F] = n = \deg m(x)$

Prop. Let $\alpha \in K$. Then $\alpha$ is algebraic over $F$ if and only if $[F(\alpha) : F] < \infty$.

Proof $\Rightarrow$ from immediately above.
Consider \( \{ 1, \alpha, \alpha^2, \ldots \} \).

Assuming \([F(\alpha) : F] = n < \infty\), this set is

\( F \)-linearly dependent. So there exists

\[ 1, \alpha, \alpha^2, \ldots, \alpha^n \]

such that \( \alpha^n + a_1 \alpha + \ldots + a_n \alpha = 0 \)

i.e. it is linearly dependent.

In other words, \( \alpha \) is a root of \( a_n \alpha^n + a_{n-1} \alpha^{n-1} + \ldots + a_1 \alpha + a_0 \in F[X] \).

i.e. a algebraic over \( F \). \( \Box \)

**Theorem**

Let \( F \leq K \leq L \) be field extensions. Then

\[ [L : F] = [L : K][K : F] \]

(Infinitely degree extensions allowed).

Assume first \([L : K] = m \leq \infty\), \([K : F] = n < \infty\)

let \( \alpha_1, \ldots, \alpha_m \) be a \( K \)-basis for \( L \), \( \beta_1, \ldots, \beta_n \)

be an \( F \)-basis for \( K \). Then every element of \( L \)

can be written as

\[ (b_1 \beta_1 + b_2 \beta_2 + \ldots + b_n \beta_n) \alpha_1 + \ldots + (b_{m1} \beta_1 + \ldots + b_{mn} \beta_n) \]

i.e. The \( \alpha_i \beta_j \) products \( F \)-span \( L \).

To show independence.
To show independence, suppose otherwise.

Then there exist \( b_{ij} \in F \) for \( 1 \leq i \leq m \) \( 1 \leq j \leq n \) not all zero with

\[
\sum_{i,j} b_{ij} \alpha_i \beta_j = 0
\]

Rewrite

\[
(b_{11} \beta_1 + b_{12} \beta_2 + \ldots + b_{1n} \beta_n) \alpha_1
\]

\[
\alpha_1
\]

\[
+ \ldots + (b_{m1} \beta_1 + b_{m2} \beta_2 + \ldots + b_{mn} \beta_n) \alpha_m = 0
\]

\[a_m\]

[N.B. different \( b_{ij} \) than in spanning proof]

so \( \{\alpha_1, \ldots, \alpha_m\} \) \( K \)-linear dependent, contradicting since \( b_{ij} \) not all zero, \( \alpha_1, \ldots, \alpha_m \) cannot be all zero, since \( \beta_1, \ldots, \beta_n \) are independent (F indep)

Hence \( \alpha_1 \beta_1 \) \( F \)-linear independent, so

\[
\]

Cases where one of \([L:F],[L:K]\) is or \([K:F]\)

are infinite left as an exercise \( \Box \)
Example

Consider \( x^3 - 3 \in \mathbb{Q}[x] \)

irreducible by Eisenstein's criterion (and Gauß lemma)

Let \( \alpha \in \mathbb{R} \) be a root of \( x^3 - 3 \)

Now that \([\mathbb{Q}(\alpha) : \mathbb{Q}] = 3\) from before

Now suppose \( \sqrt{2} \in \mathbb{Q}(\alpha) \), then \( \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\alpha) \)

But then

\[
3 = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})] [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]
\]

\[
= \sqrt{2} \quad \text{contradiction.}
\]

Def

A field of the form \( F(\alpha_1, \ldots, \alpha_n) \) is

Finitely Generated over \( F \) (as a field)

Lemma

Let \( \alpha_1, \ldots, \alpha_n \in K \) a field extension of \( F \)

Then

\[
F(\alpha_1, \ldots, \alpha_n)
\]

is a field if and only if

\[
\big((F(\alpha_1))(\alpha_2)\big)(\alpha_3) \ldots (\alpha_n)
\]

Pf

First assume \( n = 2 \), \( \alpha = \alpha_1 \), \( \beta = \alpha_2 \)

Since \( (F(\alpha))(\beta) \) is a field containing \( F, \alpha, \beta \),

we have \( F(\alpha, \beta) \subseteq (F(\alpha))(\beta) \)

On the other hand, since \( F(\alpha, \beta) \) is a field containing \( F \)

and \( \alpha \), we have \( F(\alpha) \subseteq F(\alpha, \beta) \).

Next, since \( F(\alpha) \) is field containing \( F \), \( \beta \), \( (F(\alpha))(\beta) \subseteq F(\alpha, \beta) \)

hence equal. \( \blacksquare \)
Theorem

\[ [K : F] < \infty \iff K \text{ is finitely generated over } F \]

\( (\Rightarrow) \)

Let \( \alpha_1, \ldots, \alpha_n \) be an \( F \)-basis for \( K \). Then \( K = F(\alpha_1, \ldots, \alpha_n) \) in particular.

Also, each \( F(\alpha_i) \subseteq K \) for all \( 1 \leq i \leq n \).

\( \therefore \alpha_1, \ldots, \alpha_n \) are algebraic over \( F \) (exercise).

\( \therefore \) \( K \) generated by finitely many elements algebraic over \( F \).

\( (\Leftarrow) \)

Suppose \( K = F(\alpha_1, \ldots, \alpha_n) \) where \( \alpha_1, \ldots, \alpha_n \in K \)

are all algebraic over \( F \).

For \( 1 \leq i \leq n \) set \( F_i = F(\alpha_1, \ldots, \alpha_i) \)

set \( F_0 = F \) (note \( F_n = K \)) so we have extensions

\[ F = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_{n-1} \subseteq F_n = K \]

find \( F_i = F_{i-1}(\alpha_i) \) for \( 1 \leq i \leq n \).

By above, since each \( \alpha_i \) is algebraic over \( F_{i-1} \) for \( 1 \leq i \leq n \), we have

\[ [F_i : F_{i-1}] = [F_i(\alpha_i) : F_{i-1}] < \infty \]

But \( [K : F] = [F_n : F_{n-1}][F_{n-1} : F_{n-2}] \cdots [F_1 : F_0] < \infty \)

HW 2 Next Thursday.