$\text{Algebra}$  8 February 2011

13.2.15 - you skipped it, # fail

F field
α ∈ extension field $\overline{F}$

$F(\alpha) = F[\alpha] \iff \alpha$ algebraic over $F$

Note: Suppose $\alpha$ not algebraic over $F$

then $1, \alpha, \alpha^2, \ldots$ are $F$-linearly independent

$F[\alpha] \cong F[\alpha]$ contains kernel nontrivial map $F[\alpha] \to F[\alpha]$

no kernel in obvious map

and $F[\alpha]$ not a field.

In showing $x^3 - 2$ not irreducible over $\mathbb{Q}[i]$

$x^3 - 2$ reducible over $\mathbb{Q}[i] \implies x^3 - 2$ has a root in $\mathbb{Q}[i]$

\[ t = \frac{p(x)}{q(x)} \text{ some rational function} \]

$k(x)$

$1 \cup k(t)$

$x$ as member of $k(x)$

$(k(t))[x] \quad p(x)$

$(k[\mathbb{C})][x] \quad p(x) - tQ(x)$
§ 13.4 continued

F a field

An algebraic closure for F will be an algebraically closed field that is algebraic over F.

Last time we proved existence of algebraic closure, want uniqueness.

**Lemma** Let L be an algebraically closed field, let k be a simple extension of F, and suppose there is an embedding (i.e., an injective field homomorphism) \( \sigma : F \rightarrow L \). Then \( \sigma \) extends to an embedding \( \hat{\sigma} : K \rightarrow L \) (i.e., there is an embedding \( \hat{\sigma} : K \rightarrow L \) s.t. \( \hat{\sigma}|_F = \sigma \)).

**Proof** \( K = F(a) \) and let \( p(x) = m_a(x) \in F[X] \)

Extending \( \sigma \) to an injective ring homomorphism

\[ \sigma : F[X] \rightarrow \sigma(F)[X], \]

\( \sigma(p(x)) \) is irreducible in \( \sigma(F)[X] \)

Since L is algebraically closed, can choose a root \( \beta \in L \) of \( \sigma(p(x)) \). We have

\[ K = F(a) \cong F[X]/(p(x)) \xrightarrow{\alpha(p(x))} \sigma(F)[X]/\sigma(p(x)) \cong (\sigma(F)[X]/\sigma(p(x))) \cong \sigma(F)[X]/\sigma(p(x)) \cong L. \]

If \( K \) is a simple extension of \( F \), and \( F \) has an embedding into an algebraically closed field \( L \), can the embedding extend to an embedding of \( K \) into \( L \).
We have an embedding \( \phi : K \to L \), with

\[
\phi|_F = 0
\]

Taking \( \phi = \psi \) lemma follows. \( \square \)

**Theorem** Let \( L \) be an algebraically closed field

Let \( K \) be an algebraic extension of \( F \)

and let \( \phi : F \to L \) be a field embedding. Then

1. There exists an embedding \( K \to L \) restricting to \( \phi \) on \( F \)

2. If \( K \) algebraically closed and \( L \) is algebraic over \( \phi(F) \) then the embedding \( K \to L \) is an isomorphism.

**Proof** Let \( S \) be the set of all pairs \( (K, \tau) \)

where \( K \) is a subfield of \( L \) containing \( F \) and

\( \tau : K \to L \) is an extension of \( \phi : F \to L \)

Since \( (F, \phi) \in S \), so \( S \neq \emptyset \). For \( (K, \tau) \)

and \( (K', \tau') \in S \), say that \( (K, \tau) \leq (K', \tau') \) if

\( K \subseteq K' \) and if \( \tau|_K = \tau' \)

So \( S \) is partially ordered set.

Moreover if \( (K_1, \tau_1) \leq (K_2, \tau_2) \leq \ldots \) is a

chain in \( S \), then \( (K_\infty, \tau_\infty) \in S \) for

\[
K_\infty = \bigcup K_i \quad \tau_\infty : K_\infty \to L \quad \lambda_i \in K_i \quad \tau_i = \tau_i (\lambda_i)
\]

If \( L \) algebraically closed, \( F \) embeds into \( L \), and \( K \) algebraic extension of \( F \),

then the embedding extends to an embedding of \( K \) into \( L \), and if \( K \) algebraically closed, then \( K \cong L \).

Start by taking \( S \) set of pairs \((K, \tau) \). \( K \leq K', \phi_F, \tau : K \to L \) extending \( F \to L \)

Take a partial order \( (K, \tau) \leq (K', \tau') \) if \( K \subseteq K' \) and \( \tau|_K = \tau' \).
Zorn's Lemma implies to \( S \), and exists a maximal member of \( S \), say \((k_{\text{max}}, \tau_{\text{max}})\) of \( S \).

Now, \( k_{\text{max}} = K \).

Suppose contrary \( k_{\text{max}} \neq K \).

Take \( \alpha \in K \setminus k_{\text{max}} \).

Since \( K \) algebraic over \( F \), \( \alpha \) algebraic over \( k_{\text{max}} \).

\( \tau_{\text{max}} \) extends to embedding \( k_{\text{max}}(\alpha) \to L \).

Lemma prior, \( \tau_{\text{max}} \)(\( k_{\text{max}}, \tau_{\text{max}} \)) not maximal \( \Rightarrow \) \( k_{\text{max}} = K \).

\( \Rightarrow \) \( \tau_{\text{max}} \) extends to embedding \( K \to L \) and \( \tau \) follows \( \square \).

For (2) suppose as assumed \( K \) algebraically closed and \( L \) algebraic over \( \sigma(F) \). By (1), extend \( \sigma \) to a field embedding \( K \to L \).

\( \Rightarrow \) \( L \) is algebraic extension of algebraically closed (why) field \( \sigma(K) \). By earlier, \( \sigma(K) \) must have no proper extension, so \( \sigma(K) = L \), and \( \tau \) follows \( \square \).

By Zorn's Lemma, get a maximal \((k_{\text{max}}, \tau_{\text{max}})\). \( k_{\text{max}} = K \) since otherwise \( \alpha \in K \setminus k_{\text{max}} \) \( k_{\text{max}}(\alpha) \) extension of \( k_{\text{max}} \) and \( \tau_{\text{max}} \) extends, contradicting maximality.

If \( K \) algebraically closed, embedding of \( K \) into \( L \) implies \( L \) extends \( K \), but \( K \) algebraically closed so \( K = L \).
Algebraic closures of $F$ are isomorphic.

**Corollary**: Let $K, L$ be algebraic closures of $F$. Then there is an isomorphism $\psi : K \to L$ such that $\psi|_F$ is the identity on $F$.

\[
\begin{array}{c|cc}
K & \psi & L \\
F & \frac{\text{id}}{1} & F \\
\end{array}
\]

Remark: Can now refer to the algebraic closure of $F$.

**Proposition**: Let $f(x) \in F[x]$ be nonscalar. Let $K, K'$ be splitting fields for $f(x)$ over $F$. Then there is an isomorphism $K \to K'$ that restricts to the identity on $F$.

**Proof**: Let $L$ be the algebraic closure of $F$. Note that $L$ algebraic over $F$, since $K'$ algebraic over $F$. Then $L$ is also the algebraic closure of $F$ (with $K' \subseteq L$).

Now, by Lemma, there is an embedding

\[
\begin{array}{c|cc}
K & \rightarrow & L \\
F & \rightarrow & F \\
\end{array}
\]

Now $K = F(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are in $L$, $K$ and $f(x) = \lambda(x - \alpha_1) \cdots (x - \alpha_n) \in F[x]$ for some $\lambda \in F$. 

Splitting fields isomorphic
\[ f(x) = a_n(x - \sigma(a_1)) \cdots (x - \sigma(a_n)) \text{ in } L[x] \]
\[ \sigma(a_1), \ldots, \sigma(a_n) \text{ is a complete list of the roots in } L \text{ of } f(x). \]

But \( K' \leq L \) is a splitting field for \( f(x) \) over \( F \)
so \( K' = F(\sigma(a_1), \ldots, \sigma(a_n)) \)
\[ \therefore K' = \sigma(K) \text{ (think about this).} \]

Proposition follows \( \square \)

Fact we'll use without proof:

**FUNDAMENTAL THEOREM OF ALGEBRA**

\( \mathbb{C} \) is algebraically closed.

\[ \text{§ 13.5 SEPARABLE and INSEPAREABLE EXTENSIONS} \]

Throughout, \( F \) is a field. To start...

Let \( f(x) \in F[x] \) not scalar and write

\[ f(x) = \lambda (x - \alpha_1)^{n_1} (x - \alpha_2)^{n_2} \cdots (x - \alpha_k)^{n_k} \]

for \( \lambda \in F \), and for \( \alpha_1, \ldots, \alpha_k \) in some splitting for \( f(x) \) over \( F \), with \( \alpha_1, \ldots, \alpha_k \) distinct

and with \( n_1, \ldots, n_k \) positive integers.
For $1 \leq i \leq k$ we say that $\alpha_i$ is a **SIMPLE ROOT** when $n_i = 1$, and a **MULTIPLE ROOT** otherwise. If $n_1 = n_2 = \ldots = n_k = 1$, we say $f(x)$ is **SEPARABLE**.

Say $f(x)$ is **INSEPARABLE** otherwise.

Note. Separability or inseparability does not depend on the choice of splitting field. (why?)

**Ex.** Let $F = \mathbb{F}_p(t)$

$t$ indeterminate, $\mathbb{F}_p$ the field with $p$ elements, $p$ prime

Consider $x^p - t \in F[x]$.

Let $\alpha$ be a root of $x^p - t$ in some field extension of $F$.

Since the characteristic of $F$ is $p$ (check),

$x^p - t = (x - \alpha)^p$ (check).

Set $R = \mathbb{F}_p[t]$. Then $R$ is an integral domain and $F$ is the field of fractions of $R$.

Also, the ideal of $R$ generated by $t$, i.e. $(t)$ is a prime ideal (indeed, maximal) $R/(t) = \mathbb{F}_p$.

So by the general form of Eisenstein's Criterion, and

so $x^p - t$ is irreducible in $R[x]$. By general version of Gauss' Lemma, $x^p - t$ irreducible in $F[x]$.

A root of $f(x)$ is simple if only one factor of $(x - \alpha)$ in $f(x)$ multiple otherwise.

$f(x)$ is separable if all roots are simple.
We conclude $x^p - t$ irreducible in $F[x]$, and has exactly one root in any splitting field over $F$.