Review

- Field $F$
- $p(x) \in F[x]$ irreducible

Lemma $F[x]/(p(x))$ is a field. $\square$

Set $K = F[x]/(p(x))$

Consider $p(\lambda) \in F[y] \subseteq K[y]$

$p(\lambda) = 0 \in \overline{K}$ where $\overline{\lambda} = \lambda \mod (p(x))$

$p(x) = p(\lambda)$

\[ F \xrightarrow{i} F[x] \xrightarrow{\lambda} F[x]/(p(x)) \]

above inclusion $F$ into $K$ extends to a homomorphism $F[y] \rightarrow K[y]$ injective

\[ f(y) \rightarrow f(x) \]

\[ f(x) \xrightarrow{\overline{x}} F[x]/(p(x)) \xrightarrow{\overline{f(x)}} \overline{f(x)} \]
§ 13.4 (continued)

Throughout, $F$ a field.

Recall $g(x) \in F[x]$ splits completely over $K$, with $K/F$ if

$$g(x) = (x - \alpha_1) \cdots (x - \alpha_n)$$

in $K[x]$ for $\lambda, \alpha_1, \ldots, \alpha_n \in K$. $g(\alpha)$ not scalar.

The splitting field for $g(x)$ over $F$ is minimal field in which $g(x)$ splits. The splitting field for $g(x)$ over $F$ always exists (provided $g(x)$ not scalar).

Example

Consider $x^3 - 2 \in \mathbb{Q}[x]$ irreducible by Eisenstein’s criterion. The complex roots are

$$\sqrt[3]{2}, \frac{1}{\sqrt[3]{2}} \left( -1 + i \sqrt{3} \right), \frac{1}{\sqrt[3]{2}} \left( -1 - i \sqrt{3} \right)$$

It follows that the field $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ is a splitting field over $\mathbb{Q}$ for $x^3 - 2$.

If $F(\lambda, \alpha_1, \ldots, \alpha_n) \subseteq K$, any extension of $F$ contained in $K$ in which $f(x)$ splits completely contains $F(\lambda, \alpha_1, \ldots, \alpha_n)$ because $K[x]$ is a UFD, so $F(\lambda, \alpha_1, \ldots, \alpha_n)$ is a splitting field.

A polynomial splits in $K$ if splits into linear factors (and constant factors).

A splitting field is a minimal such field not a base field $F[x]$.

$F(\lambda, \alpha_1, \ldots, \alpha_n) \subseteq K$ because $K[x]$ a UFD, so that factorization applies.
Def Let $S$ be a collection of polynomials in $F[x]$. Then a SPLITTING FIELD of $S$ over $F$ is a field $K/F$ in which all polynomials in $S$ split, and is minimal over such fields.

A field extension of $F$ that is the splitting field of some $S \subseteq F[x]$ is called a NORMAL EXTENSION of $F$.

Remark In the preceding, if $S$ is finite, then a splitting field for $S$ is exactly the same as the splitting field for the product of its members $s_i$.

Prop Let $f(x) \in F[x]$ have degree $n$, for $n \geq 1$ and let $K$ be a splitting field for $f(x)$ over $F$. Then $[K:F] \leq n!$.

If $\alpha \in K$ is a root of $f(x)$, then

$[F(\alpha) : F] \leq n$.

In $(F(\alpha_1))[x]$, $f(x) = (x - \alpha_1) f_1(x)$

for some $f_1(x) \in (F(\alpha_1))[x]$ with $\deg f_1 \leq n - 1$.

Now $\alpha_2$ a root of $f_1(x)$, so

$[F(\alpha_1, \alpha_2) : F(\alpha_1)] \leq n - 1$.

So continue to see $[F(\alpha_1, \ldots, \alpha_n) : F(\alpha_1)] = n!$.

A splitting of a set of polynomials is the extension field (minimal) in which all the polynomials split.

A field extension that is a splitting for some set $S$ is a normal extension.

If a splitting field for $f(x) \in F[x]$ then $[K:F] \leq n!$. 

A splitting of a set of polynomials is the extension field (minimal) in which all the polynomials split.

A field extension that is a splitting for some set $S$ is a normal extension.

If a splitting field for $f(x) \in F[x]$ then $[K:F] \leq n!$. 

A splitting of a set of polynomials is the extension field (minimal) in which all the polynomials split.

A field extension that is a splitting for some set $S$ is a normal extension.

If a splitting field for $f(x) \in F[x]$ then $[K:F] \leq n!$. 

A splitting of a set of polynomials is the extension field (minimal) in which all the polynomials split.

A field extension that is a splitting for some set $S$ is a normal extension.

If a splitting field for $f(x) \in F[x]$ then $[K:F] \leq n!$. 

Next study $x^n - 1$, but first

Prop  Let $G$ be a finite subgroup of $F^x$, the multiplicative group of units, $\neq F\{0\}$.
Then $G$ is cyclic.

Proof
Since $G$ is a finite abelian group, known from the fundamental theorem of finite abelian groups, that $G$ can be written as product of cyclic groups:

$$G \cong \left( \mathbb{Z}/r_1 \mathbb{Z} \right) \times \cdots \times \left( \mathbb{Z}/r_t \mathbb{Z} \right)$$

for primes $p_i$ and $r_i > 1$.

Next suppose $p = p_i = p_j$ for some $1 \leq i < j \leq t$.

Further suppose wlog $r_i \leq r_j = s$.

Then there are at least

$$p_r + p_s - 1$$

distinct elements with order dividing $p^s$.

But every element in $G$ with order dividing $p^s$ is a root of $x^{p_s} - 1 \in F[x]$, which has at most $p^s$ roots, contradiction, so no primes appear with multiplicity, so $G$ is cyclic because in the proof of the fundamental theorem of finite abelian groups, and

$$G \cong \mathbb{Z}/(p_{r_1} \cdots p_{r_t}) \mathbb{Z}$$

If $F^x = F\{0\}$, multiplicative group, and $G \subseteq F^x$, $G$ finite, then $G$ is cyclic.

$G$ abelian, finite, so $G \cong \prod_{i} \left( \mathbb{Z}/p_i \mathbb{Z} \right)$.

First we show $p_i$ distinct by number of elements whose order divide $p_i$.

Then product of coprime order cyclic groups is cyclic.
Now choose a positive integer $n$ and consider $x^n - 1 \in F[x]$, let $K$ be a field extension of $F$. The roots in $K$ of $x^n - 1$ are called \textit{n$^\text{th}$ roots of unity}.

At least one such exists, namely 1.

Let $\alpha, \beta \in K$ be $n$th roots of 1.

Then $(\alpha \beta)^n = \alpha^n (\beta^n)^{-1} = 1$. Thus, the $n$th roots of 1 in $K$ form a finite multiplicative subgroup of $K^\times$ and, by above, must be cyclic.

If $x^n - 1$ splits completely in $K$ and if $\alpha \in K$ is a root of $x^n - 1$ that generates the $n$th roots of unity in $K$, then we say $\alpha$ is a \textit{primitive} root of unity in $K$.

\textbf{Examples}

1. Consider $x^n - 1 \in \mathbb{Q}[x]$.

In $\mathbb{C}$, the roots are $\{\zeta_k \zeta_{k/n}^{(n-1)} | \zeta_{k/n} \text{ for } k = 0, 1, \ldots, n-1\}$.

Set $\zeta_n = e^{2\pi i/n}$. Then $\zeta_n$ is a primitive $n$th root of 1 in $\mathbb{C}$. Call $\mathbb{Q}(\zeta_n)$ the \textbf{cyclotomic field of $n$th roots of unity over $\mathbb{Q}$}.

The roots of $x^n - 1$ are the $n$th roots of unity.

Any $n$th root generating the whole multiplicative group of $n$th roots is a \textit{primitive} root.

$\mathbb{Q}(\zeta_5)$ will be a \textit{primitive} root of unity in the cyclotomic field of $5$th roots of unity.

\textit{cyclo tonic field of $n$th roots of unity}
Note $(\mathbb{Q}(\zeta_n))$ is a splitting field over $\mathbb{Q}$ in $\mathbb{C}$ for $x^n - 1$.

**Exercise**

\[ MV^n x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + 1) \]

\[ \therefore \\ deg \ 5_n \leq n - 1 \]

8. Suppose $F$ has characteristic $p \neq 0$.

**Exercise**

Then $x^p - 1 = (x - 1)^p$ (exercise)

\[ \therefore \ 1 \text{ is the only } p^{th} \text{ root of unity in any field extension of } F \]