Last Time

* If $F \subseteq L \subseteq K$ is a tower of field extensions,
  
  $$[K:F] = [K:L] \cdot [L:F].$$

* If $K/F$ is an extension & $\alpha \in K$ then
  
  $\alpha$ is alg. over $F$ $\iff [F(\alpha):F] < \infty$.

* If $\alpha_1, \ldots, \alpha_n \in K$ are algebraic over $F$ then $F(\alpha_1, \ldots, \alpha_n)/F$ is finite (hence algebraic).

§ 15.6 Adjoining Roots

Let $f(x) \in F[x]$ be an irreducible polynomial over a field $F$.

Then $\langle f \rangle \subseteq F[x]$ is a maximal ideal, so $F[x]/\langle f \rangle$ is a field. Moreover, we have a map $\iota : F \to F[x]/\langle f \rangle$.

Let $\iota(a) = \overline{a}$ be a homomorphism, $\iota(1) = \overline{1}$, & $F$ is a field, so $\iota$ is an injection. Moreover, inside $F[x]/\langle f \rangle$ we have $f(\overline{x}) = f(\overline{x}) = 0$, so $\overline{x}$ is a root of $f$.

Prop Let $f(x) \in F[x]$ be any polynomial. There exists an extension $F \subseteq K$ s.t. $f(x)$ splits into linear factors in $K[x]$.

Remark If $F = \mathbb{Q}$ (or $\mathbb{R}$ or $\mathbb{Q}(\sqrt{-3})$ or...) could take $\mathbb{Q}$ less clear if $F = \mathbb{F}_3$ or $F = \mathbb{C}(t)$. 
Pf. Let \( g(\alpha) \) be an irreducible factor of \( f(\alpha) \) in \( F[\alpha] \). Then \( g(\alpha) \) (and hence \( f(\alpha) \)) have a root \( \alpha \in F[\alpha]/\langle g \rangle \), which is an extension of \( F \). Over \( F[\alpha]/\langle g \rangle \), write 
\[
f(\alpha) = (\alpha - \alpha) \cdot f_1(\alpha),
\]
so that \( \deg f_1 = \deg f - 1 \). We are done by induction on degree.

\[\text{Def.}\] The derivative of a polynomial \( f(x) = a_nx^n + \ldots + ax + a_0 \in F[x] \) is 
\[
 f'(x) = na_n x^{n-1} + \ldots + a_1 \in F[x].
\]

Prop. Let \( f(x) \in F[x] \) be a polynomial with \( \deg f > 1 \) and let 
\[ f'(x) \text{ be its derivative.} \]

\[\begin{align*}
1 & \quad f \text{ has a multiple root over some extension } K \text{ of } F, \\
2 & \quad \gcd(f, f') \neq 1. \quad \text{[Prop.]} \]

Pf. \( 1 \Rightarrow 2 \) Let \( K \supseteq F \) be an extension such that 
\( f \) splits completely in \( K[x] \); write 
\[
f(\alpha) = (\alpha - \alpha)^2 \cdot g(\alpha)
\]
over \( K[\alpha] \). Then 
\[
f'(\alpha) = 2(\alpha - \alpha) \cdot g(\alpha) + (\alpha - \alpha)^2 \cdot g'(\alpha)
\]
so \( \alpha - \alpha \) is a common divisor of \( f, f' \) and 
\[
\gcd(f, f') \neq 1.
\]

\( 2 \Rightarrow 1 \) Let \( K \supseteq F \) be an extension such that 
\( f \) splits completely in \( K[x] \); write 
\[
f(\alpha) = c(x - \alpha_1) \cdots (x - \alpha_n)
\]
for \( \alpha_1, \ldots, \alpha_n \) distinct. Then 
\[ f' = c(x - \alpha_1) - (x - \alpha_n) + c(x - \alpha_1) - (x - \alpha_n)
\]
so that 
\[
\gcd(f, f') = 1 \left( \frac{1}{c} (x - \alpha_i) \right) f' \text{ for } 1 \leq i \leq n.
\]
§ 15.7 Finite fields

Let $F$ be a finite field. Then $\text{char } F \neq 0$ so that $\text{char } F = p > 0$ for some prime $p$ and $F_p \leq F$ with $[F : F_p] = r > 0$.

⇒ All finite fields have prime power order.

Ex \[x^2 + x + 1 \in F_2[x] \text{ is irreducible (no roots!), so}\]

\[
F_4 := \frac{F_2[x]}{(x^2 + x + 1)} \text{ is a field of order } 4.
\]

elts \[\{0, 1, \alpha, \alpha + 1\}.
\]

\[
\alpha^2 = -(\alpha + 1) = \alpha + 1, \text{ etc.}
\]

\[
\alpha^2 + \alpha + 1 = 0 \text{ char } 2
\]

Q \ How to construct $F_{2^r}$ (or $F_{p^r}$) in general?

Trick! Consider $f(x) = x^q - x \in F_p[x]$ where $q = p^r$.

Then $f'(x) = q x^{q-1} - 1 = -1 \Rightarrow \gcd(f, f') = 1$ & $f$ has no multiple roots.

Lem \ Let $f(x) = x^q - x \in F_p[x]$ with $q = p^r$ & let $f(x)$ split.

K = \{ $\alpha \in L : f(\alpha) = 0$ \}. Then $|K| = q$ and

K is a subfield of L (with $F_p \subseteq K$).
Cor Let \( f(x) \in F[x] \) be an irreducible polynomial.

1. If \( f'(x) \neq 0 \) then \( f(x) \) has no multiple roots in any extension \( K \) of \( F \).

2. If \( \text{char} F = 0 \) then \( f(x) \) has no multiple roots in any extension \( K \) of \( F \).

\[ Pf \]

(1) We have \( \deg f' < \deg f \). Since \( f \) is irreducible, if \( f' \neq 0 \) then \( f + f' \) so \( \gcd (f, f') = 1 \).

(2) If \( \text{char} F = 0 \) then \( f' \neq 0 \) whenever \( \deg f > 0 \). \( \square \)

Rem Consider the field \( F = \mathbb{F}_3(u) \) and let \( f(x) = x^3 - u \in F[x] \).

Then \( f \) is irreducible (u-Eisenstein!?) and

\[ f'(x) = p \cdot x^{p-1} - 0 = 0 \, \text{ in } K[x] \, \text{ is a root of } f(x) \, (\text{so } x^p = u) \, \text{ then} \]

\[ \sum_{i=0}^{3} \binom{3}{i} x^i u^{3-i} = \binom{3}{0} x^3 + \binom{3}{1} x^2 u + \binom{3}{2} x u^2 + \binom{3}{3} u^3 \]

\[ = x^3 u^3 + x^2 u^2 + xu + u^3 = -u + x^3 = x^3 - u \, \text{ in } K[x] \]