Warning: In characteristic, \( f'(x) = 0 \) does not mean \( f(x) = \text{const.} \).

For example, \( f(x) = x^{1/p} + 1 \):

\[
f'(x) = p x^{1/p - 1} = 0
\]

If \( f(x) = g(x^p) \) then:

\[
f'(x) = g'(x^p) \cdot px^{p-1} = 0
\]

Proof of 12.1.4: From 10.4.6 we know that \( f(x) \) no repeated root.
if it has no root in common with $f'(x)$

Since

\[ f(x) = (x-a)^2 g(x) \]

\[ f'(x) = 2(x-a)g(x) + (x-a)^2 g'(x) \]

\[ = (x-a)(2g(x) + (x-a)g'(x)) \]

\[ \alpha \text{ is a root of both } f \text{ and } f' \]

\[ \Rightarrow \text{ if } f'(x) = 0 \text{ then every root of } f(x) \text{ is also a root of } f'(x). \text{ Hence } f(x) \text{ has a repeated root if its root is not exact.} \]
If \( f'(x) \neq 0 \) and \( x \) is a root of both \( f \) and \( f' \), then \((x-a)\) divides both of them. But \( \deg f' < \deg f \), so \( f \neq f' \) and the irreducibility of \( f \) means \( \gcd(f, f') = 1 \). But they are both divisible by \( (x-a) \). This is a contradiction.

Hence \( f \) and \( f' \) do not have a common root and \( f \) is separable. QED
Proof of 12.1.6

1) In char 0, \( f'(x) \neq 0 \Rightarrow f(x) \) is not constant. But \( f(x) \) is not constant, so \( f'(x) \neq 0 \) and it is separable by 12.1.4.

2) \( \Rightarrow \) Assume \( f(x) = g(x^p) \) for some \( g(x) \in F[x] \). This means \( f'(x) = 0 \), so \( f(x) \) is not separable.

\( \Leftarrow \) If \( f(x) \neq g(x^p) \) then
\[ f(x) = a_m x^m + \cdots + a_n x^n + \cdots + a_0 \]
for some $i$ not div by $p$, $a_i \neq 0$.

$$f'(x) = \cdots \cdot a_i x^{i-1} + \cdots$$

$\not\equiv 0 \pmod{p}$

so $f(x)$ is separable by $12.1.4$

QED

Cor. 12.1.7 Every field of characteristic $0$ is perfect.

Cor. 12.1.8 Every finite field is perfect.

Proof: Let $\bar{F}$ be a finite field of
characteristic $p$ case $f(x)$
is an irreducible polynomial
and $f(x) = g(x^p)$. We will show
this means $f(x)$ can be factored
Let $g(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$
$f(x) = g(x^p) = a_n x^{np} + a_{n-1} x^{np-1} + \ldots + a_0$
Let $a_i^* = b_{i/n}$ (We know the Frobenius
map in $F$ is onto, so $\exists! b_i$ with
$b_{i/n} = a_i^*$)
f(x) = g(x^p) = b_n x^{np} + b_{n-1} x^{np-1} + \ldots + b_0
\[(b_n x^n - b_m x^m + \ldots + b_0)^k\]

so \(f(x)\) is not irreducible. QED

Hence the only non-perfect fields are infinite and have char \(p > 0\).

**Def 12.1.12**

1) Let \(E\) be a field. An 
\(\phi : E \rightarrow E\) is an **automorphism** of \(E\).

2) For \(F \subseteq E\) is a subfield,
an $F$-automorphism of $E$ is an automorphism that fixes $F$.

Thm 12.1.13. Let $E/F$.

1) The set $\text{Aut}(E)$ of automorphisms of $E$ is a group under composition.

2) The set $\text{Aut}_F(E)$ of $F$-automorphisms is a subgroup.

You can prove this.

Def 12.1.14. The kernels of $\alpha$ of $E/F$ in $\text{Aut}_F(E)$. 
Examples $d = \text{square}$

$E/T$ | $Q$ | $R$ | $\frac{\mathbb{F}_p}{\mathbb{F}_p} = \mathbb{Z}/p\mathbb{Z}$

$\text{Gal}(E/F)$ | $C_2$ | $C_2$ | $C_n$

$\text{Gal}(\mathbb{F}_p^n/\mathbb{F}_p)$ is generated by the

Frobenius map $\phi : x \mapsto x^p$

$\phi^n : x \mapsto x^{p^n}$

Example for later $F = \mathbb{Q}$

$E = \mathbb{Q}(\sqrt[3]{4}) = \mathbb{Q}(e^{2\pi i/n})$

$\text{Gal}(E/F) = ?$
Example \( F = \mathbb{Q} \), \( E = \mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) \)

\[
\text{Gal}(E/F) = C_2 \times C_2 \] is the Galois group of \( E/F \) as \( E \) is a splitting field of \( f(x) = x^3 - 2 
\)

<table>
<thead>
<tr>
<th>( \sqrt{2} )</th>
<th>( \sqrt[3]{3} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>(-\sqrt{2})</td>
<td>(-\sqrt[3]{3})</td>
</tr>
<tr>
<td>(-\sqrt[3]{3})</td>
<td>(-\sqrt{3})</td>
</tr>
</tbody>
</table>

\( f(x) = x^3 - 2 \) is irreducible in \( \mathbb{Q} \), and \( E \) is a splitting field of \( f(x) \). The Galois group \( \text{Gal}(E/F) \) permutes the three roots of \( f(x) \).
Prop 12.10.16 \( F \subseteq E \) \( \phi \in \text{Gal}(E/F) \)

Then \( \phi(f(\alpha)) = f(\phi(\alpha)) \)

for \( \alpha \in E \), \( f(x) \in F[x] \).

e.g. \( \phi(x^2-7) = \phi(x)^2 - 7 \).

Case \( \phi(\alpha) = 0 \) then \( f(\phi(\alpha)) = 0 \)

Hence the Galois permutes the roots of any polynomial \( f(x) \in F[x] \).
**Proposition 12.1.19** Let $E = F(x)$ and $\phi \in \text{Aut}(E/F)$.

Then $\phi$ is determined by $\phi(x)$.

Let $E = F(x_1, x_2, \ldots, x_n)$. Then $\phi$ is determined by $\{ \phi(x_i) \}$.

These follow from

**Lemma 12.1.18** Let $E$ be a finite extension of $F$ with $F$-basis $\{ v_1, v_2, \ldots, v_n \}$. Then $\phi$ is determined by $\{ \phi(v_i) \}$. 
Proof of Con: \( E \) has an \( F \)-basis consisting of monomials in the di.

Hence Lemma applies!

First day example:

\[
W = \frac{-1 + \sqrt[3]{-3}}{2}
\]

\[
E = \mathbb{Q}(\sqrt[3]{3}, \omega)
\]

\( E \) has an \( F \) basis:

\[
\{ 1, \sqrt[3]{3}, \sqrt[3]{4}, \omega, \omega^2, \omega^3 \sqrt[3]{4} \}
\]
We want to prove

**Theorem 12.1.24** Let \( f(x) \in F[x] \) be separable with splitting field \( E \).

Then \(|\text{Gal}(E/F)| = [E : F]|.

\text{e.g. } F = \mathbb{Q}, E = \mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\alpha)

where \( \alpha \) is a root of \( f(x) = x^3 - 2 \).

Thus \( E \) is not the splitting field of \( f(x) \). \( \text{Gal}(E/F) = \mathbb{Z}/3 \) but \([E : F] = 3\).
To prove 12.1.24 we need

Lemma 12.1.23 Let \( p(x) \in F[x] \) be an irreducible factor of \( f(x) \) with \( \alpha \) and \( \beta \). Then \( \exists \gamma \in \text{Gal}(E/F) \) with \( \gamma(\alpha) = \beta \).