Def: A polynomial $p(x)$ is __separable__ if it's irreducible factors all split as products of distinct linear factors (ie. it's irreducible factors only have simple roots)

Ex: x^2-1, both -1 and 1 are simple roots!

Ex: x^4-2x^2+1, -1 and 1 are both roots
$= (x-1)^2(x+1)^2$ w/ multiplicity 2
Not simple roots!

Hard thing to do: find a polynomial over a field F which is not separable.

Def: A field is __perfect__ if every polynomial over that field is separable.

Theorem: If F is a field and $\mathrm{char}(F)=0$ then F is perfect.

$\mathbb{Q}$, $\mathbb{C}$, $\mathbb{R}$, etc. all have characteristic 0.

Recall: if R is any ring
$\mathrm{char}(R) = \gcd\{n\in\mathbb{Z} \mid nr=0 \ \forall\, r\in R\}$

If $p\in\mathbb{Z}$ is prime, $\mathbb{Z}_p$ is a field.

$p\neq 0$ in $\mathbb{Z}$ but $pa=0 \ \forall\, a\in\mathbb{Z}_p$!
So $\mathrm{char}(\mathbb{Z}_p)=p$.

Theorem: If F is a finite field, then F is perfect!

Notation: $\mathbb{F}_p = \mathbb{Z}_p$

Crazy example: $F = \mathbb{F}_p(t)$ (t = formal variable)

$2t+3 \in F$, $\frac{8t^2+3t+4}{6t+2} \in F$, ...

If $p=2$: $\frac{t^2+1}{t+1}$, the coeff's are only $0, 1$, ...

Now consider the polynomial $f(x) \in F[x]$ given by

$$f(x) = x^p - t$$

Note $f(x)$ is irreducible in $F[x]$ (Eisenstein's Criterion)

Let E be a splitting field of $f(x)$.
and choose $a \in E$ to be a root of $f(x)$

$$0 = f(a) = a^p - t \quad \therefore \quad t = a^p$$

Hence: $f(x) = x^p - a^p = (x-a)^p$ Freshman's dream!

$$f(x) = \underbrace{(x-a)(x-a)(x-a)\dots(x-a)}_{p \text{ times!}}$$

a is a root of $f(x)$ w/ multiplicity $p > 1$
a is not simple!

f irred. but doesn't have simple roots

F is not perfect

f is not separable.

Def: Let $F \subseteq E$ be a field extension. We call E separable if for all $a \in E$ the minimal polynomial of a is separable.

Remark: If F perfect, all extensions are automatically separable!

Def: Let $F \subseteq E$ be a field extension. We call this extension normal if every polynomial $p(x) \in F[x]$ which has a root in E must split in $E[x]$.

Theorem: Let $F \subseteq E$ be an extension field. Then the following are equivalent:

(a) E is the splitting field of some $p(x) \in F[x]$
(b) $[E:F] < \infty$ and $F = E^{G(E/F)}$
(c) $F = E^G$ for some finite subgroup $G \leq Aut(E)$
(d) E is a normal, separable extension of F.

Ex: $F = \mathbb{Q}$, $E = \mathbb{Q}[\sqrt[3]{2}]$.
Q: is E a splitting field?
A: check whether it's normal.

$P(x) = x^3 - 2$ has the root $\sqrt[3]{2}$

The other two roots are: $x^3 - 2 = 0$
$x^3 = 2$

$x = \sqrt[3]{2} \cdot e^{2\pi i/3}$, $x = \sqrt[3]{2}\, e^{4\pi i/3}$

NOT IN E because not real

$p(x)$ doesn't split!

E is not normal ...

In fact $G(E/F) = ??$

$$E = \{a + b2^{1/3} + c\,2^{2/3} : a,b,c \in \mathbb{Q}\}$$

$$\varphi : E \xrightarrow{\text{aut}} E \qquad \varphi(a) = a \quad \forall\, a \in \mathbb{Q}.$$

$$\varphi(2^{1/3}) = \alpha \in E \qquad \Rightarrow 2 = \varphi(2) = \varphi(2^{1/3})^3 = \alpha^3$$

$$\varphi(2^{1/3}) = 2^{1/3} \qquad \Rightarrow \quad 2 = \alpha^3 \quad \Rightarrow \alpha = \sqrt[3]{2}$$

$$\varphi(2^{2/3}) = \varphi(2^{1/3})^2 = \left(2^{1/3}\right)^2 = 2^{2/3}$$

$$\varphi(a + b2^{1/3} + c2^{2/3}) = a + b2^{1/3} + c^{2/3}$$

$$\varphi = id \qquad \boxed{\therefore\; G(E/F) = \{id\}}$$

<u>Def</u>: A field extension which is finite, separable, and normal is called a <u>Galois extension</u>.

<u>Remark</u>: Some books only call $G(E/F)$ the Galois group <u>when</u> E/F is a Galois extension.

<u>Fundamental Theorem of Galois Theory</u>:

Theorem (FTGT): Let $F \subseteq E$ be a Galois extension and let $G = G(E/F)$.
Then there is a bijective correspondence

$$\left\{\begin{array}{c}\text{subgroups}\\ \text{of } G\end{array}\right\} \xleftrightarrow{1-1} \left\{\begin{array}{c}\text{intermediate}\\ \text{field extensions}\\ F \subseteq F' \subseteq E\end{array}\right\}$$

$$H \longmapsto E^H = \{a \in E \mid \sigma(a) = a \ \forall \sigma \in H\}$$

$$G(E/F') \longleftarrow F'$$

This correspondence satisfies the following properties:

(a) it sends normal subgroups to normal subfields and if $H \trianglelefteq G$ then $G(E^H/F) \cong G/H$

(b) it is inclusion-reversing: $H_1 \leq H_2 \Leftrightarrow E^{H_1} \supseteq E^{H_2}$

(c) $E^{\sigma H \sigma^{-1}} = \sigma(E^H) \quad \forall \sigma \in G, \quad H \leq G$

(d) $[H_2 : H_1] = [E^{H_1} : E^{H_2}]$.

<u>Big Example</u>: $F = \mathbb{Q}, \quad E = \mathbb{Q}[\sqrt[4]{2}, i]$

Note: E is a splitting field of $x^4 - 2$, so it is Galois!

Automorphisms of E?

$$\left.\begin{array}{l} r: \sqrt[4]{2} \mapsto i\sqrt[4]{2} \\ \quad\;\; i \mapsto i \end{array}\right\} \text{ completely determines } r$$

e.g. $r(\sqrt{2}\, i) = r((\sqrt[4]{2})^2 i)$
$= r(\sqrt[4]{2})^2 r(i)$
$= (i\sqrt[4]{2})^2 i = -i\sqrt{2}$

s = complex conjugation

$\sqrt[4]{2} \longmapsto \sqrt[4]{2}$

$i \longmapsto -i$

<u>Claim</u>: $G(E/\mathbb{Q})$ = generated by r, s

$= \{e, r, r^2, r^3, rs, r^2s, r^3s, s\}$

$\cong D_4$

subgroup lattice

$$\{e\}$$

$$\{e, s\}, \{r^2 s, e\}, \{r^2, e\}, \{rs, e\}, \{r^3 s, e\}$$

$$\{r^2, s, e, r^2 s\} \quad \{e, r, r^2, r^3\} \quad \{e, r^2, rs, r^3 s\}$$

$$D_4$$

subfield lattice

$$\mathbb{Q}[\sqrt[4]{2}, i]$$

$$\mathbb{Q}[\sqrt[4]{2}] \quad \mathbb{Q}[i\sqrt[4]{2}] \quad \mathbb{Q}[\sqrt{2}, i] \quad \mathbb{Q}[(1+i)\sqrt[4]{2}] \quad \mathbb{Q}[(1-i)\sqrt[4]{2}]$$

$$\mathbb{Q}[\sqrt{2}] \quad \mathbb{Q}[i] \quad \mathbb{Q}[i\sqrt{2}]$$

$$\mathbb{Q}$$