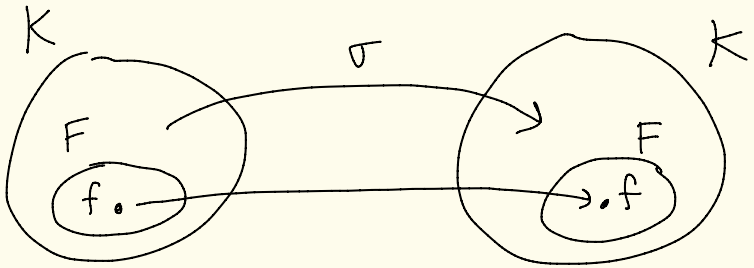
Math 5402

4/29/20

14.1 continued...

Recall: K is an extension of F.

$$\mathrm{Aut}(K/F) = \{ \sigma : K \to K \mid \sigma \text{ is a field isomorphism, } \sigma \text{ fixes } F \}$$



Prop: Let K be an extension of a field F. Then

$$\mathrm{Aut}(K) = \{ \sigma : K \to K \mid \sigma \text{ is a field isomorphism} \}$$

is a group under function composition.

And $\mathrm{Aut}(K/F)$ is a subgroup.

The identity element is $i : K \to K$ where $i(x) = x$ for all $x \in K$,

The inverse of $\sigma \in \mathrm{Aut}(K)$ is the function σ^{-1}.

Theorem: Let K/F be a field extension and let $\alpha \in K$ be algebraic over F. [That is, there exists some polynomial in $F[x]$ with α as a root.]

Let $\sigma \in Aut(K/F)$.

Then $\sigma(\alpha)$ is a root of $\min_{\alpha,F}(x)$.

proof: Suppose that α satisfies

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

where $a_0, a_1, \ldots, a_{n-1} \in F$. Since $\sigma \in Aut(K/F)$, σ fixes F.

Thus,

$$0 = \sigma(0) = \sigma\left(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0\right)$$

(σ is a field homomorphism)

$$= \sigma(\alpha)^n + \sigma(a_{n-1})\sigma(\alpha)^{n-1} + \cdots + \sigma(a_1)\sigma(\alpha) + \sigma(a_0)$$

($\sigma(x+y) = \sigma(x) + \sigma(y)$, $\sigma(xy) = \sigma(x)\sigma(y)$)

$$= \sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + \cdots + a_1\sigma(\alpha) + a_0$$

(σ fixes F)

So, if α is a root of $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ then so is $\sigma(\alpha)$. ▨

Ex: Consider $K = \mathbb{Q}(2^{1/3}) = \{a + b2^{1/3} + c(2^{1/3})^2 / a, b, c \in \mathbb{Q}\}$

Lets determine $Aut(K/\mathbb{Q}) = Aut(\mathbb{Q}(2^{1/3})/\mathbb{Q})$

Let $\sigma \in Aut(K/\mathbb{Q})$.

Then,

$$\sigma(a + b2^{1/3} + c(2^{1/3})^2)$$

$$= \sigma(a) + \sigma(b)\sigma(2^{1/3}) + \sigma(c)\sigma(2^{1/3})^2$$

$$= a + b\sigma(2^{1/3}) + c\sigma(2^{1/3})^2$$

↑ since σ fixes $\mathbb{Q}$

So, σ is determined by what it does to $2^{1/3}$.

By the last thm, $\sigma(2^{1/3})$ is a root of $\min_{2^{1/3}, \mathbb{Q}}(x) = x^3 - 2$.

The roots are $2^{1/3}$, $2^{1/3}w$, $2^{1/3}w^2$ where $w = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ and $w^2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$. So,

$$\sigma(2^{1/3}) \in \{2^{1/3}, 2^{1/3}w, 2^{1/3}w^2\}.$$

Since $\sigma : \mathbb{Q}(2^{1/3}) \to \mathbb{Q}(2^{1/3})$ (in $\mathbb{C}$)

we can't have $\sigma(2^{1/3}) = 2^{1/3}\omega \notin \mathbb{Q}(2^{1/3})$ (in $\mathbb{R}$)

and $\sigma(2^{1/3}) = 2^{1/3}\omega^2 \notin \mathbb{Q}(2^{1/3})$ (in $\mathbb{R}$)

(in $\mathbb{C}$)

Thus, $\sigma(2^{1/3}) = 2^{1/3}$. Thus, $\sigma(a+b2^{1/3}+c2^{2/3}) = a+b2^{1/3}+c2^{2/3}$ $\forall a,b,c \in \mathbb{Q}$

So, σ is the identity function,

Thus, $\mathrm{Aut}(\mathbb{Q}(2^{1/3})/\mathbb{Q}) = \{i\}$

where i is the identity function.

Ex: Let's calculate $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$.

Recall $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$.

Let $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$.

Then, $\sigma(a+b\sqrt{2}) = \sigma(a) + \sigma(b)\sigma(\sqrt{2})$

$= a + b\,\sigma(\sqrt{2})$.

σ fixes $\mathbb{Q}$

By the previous theorem $\sigma(\sqrt{2})$ is a root of $m_{\sqrt{2},\mathbb{Q}}(x) = x^2 - 2$.

So, $\sigma(\sqrt{2}) \in \{\sqrt{2}, -\sqrt{2}\}$

roots of $m_{\sqrt{2},\mathbb{Q}}(x) = x^2 - 2$

Both of these roots are in $\mathbb{Q}(\sqrt{2})$.
So we have two possible functions:

$$\sigma_1(a+b\sqrt{2}) = a+b\sqrt{2}$$
$$\sigma_2(a+b\sqrt{2}) = a-b\sqrt{2}$$

identity function
$i = \sigma_1$

You can check that both of these are isomorphisms. [Or better yet the next thm will guarantee it.]

So,

$$\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{i, \sigma_2\}$$

where i is the identity function and $\sigma_2 : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ is $\sigma_2(a+b\sqrt{2}) = a-b\sqrt{2}$.

Theorem: Let K be the splitting field over F of the polynomial $f(x) \in F[x]$.
Then $|Aut(K/F)| \leq [K:F]$
with equality if $f(x)$ is seperable over F.

Def: Let K/F be a finite extension. Then K is said to be Galois over F and K/F is a Galois extension if $|Aut(K/F)| = [K:F]$.
If K/F is Galois then $Aut(K/F)$ is called the Galois group of K/F and we write $Gal(K/F)$ for $Aut(K/F)$.

Def: If $f(x)$ is a seperable polynomial over F, then the Galois group of $f(x)$ over F is $Gal(K/F)$ where K is a splitting field for $f(x)$ over F.

Ex: $\mathbb{Q}(\sqrt{2})$ is the splitting field of the separable polynomial $x^2 - 2$ over $\mathbb{Q}$.

$\mathbb{Q}(\sqrt{2})$

$|$ 2

$\mathbb{Q}$

$\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \sigma_2\}$

So, $|\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| = 2 = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$.

So, this is a Galois extension and $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \sigma_2\}$.

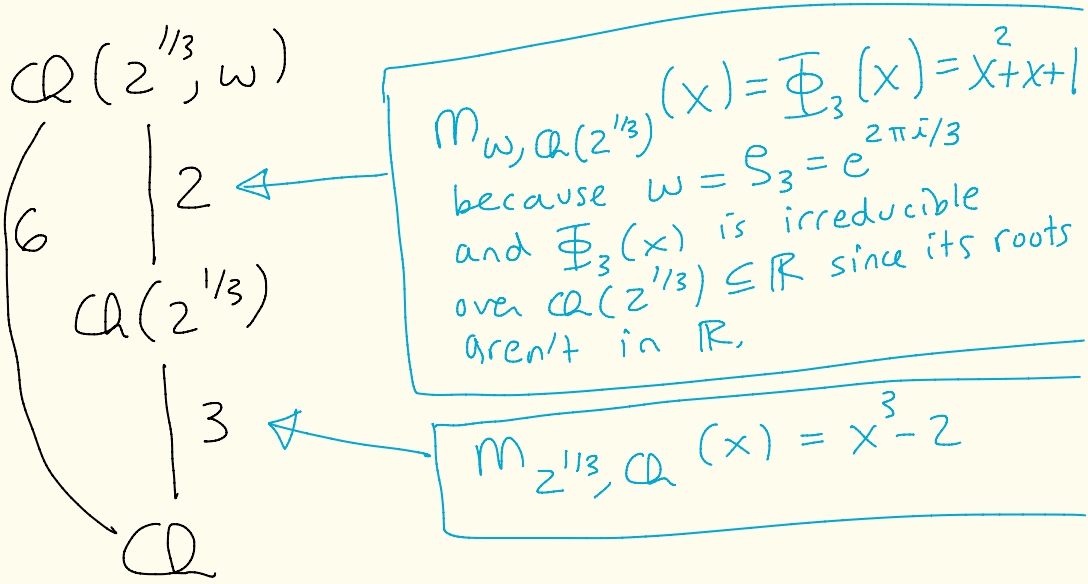
We don't need to check that σ_2 is an isomorphism because since $\mathbb{Q}(\sqrt{2})$ is the splitting field of $x^2 - 2$ over $\mathbb{Q}$ and $x^2 - 2$ is separable we must have $|\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}| = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$

and we only computed two possibilities in the last example - so both σ_1 and σ_2 are in $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$.

Ex: The splitting field of $x^3 - 2$ over $\mathbb{Q}$ is

$K = \mathbb{Q}(2^{1/3}, 2^{1/3}w, 2^{1/3}w^2) = \mathbb{Q}(2^{1/3}, w)$

where $w = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$.



So, $[\mathbb{Q}(2^{1/3}, w) : \mathbb{Q}] = 6$

continued next time....