Content:

Example	Let $\varphi:\mathbb{Q}(\sqrt{5})\to\mathbb{Q}(\sqrt{5})$ be an ismo. Then $\varphi(\frac{p}{q}) = \frac{p}{q}$. $\varphi(\sqrt{5})$ must = ±5.
Definition	Automorphism
Proposition	Aut(K) is a group under composition.
Example	Aut($\mathbb{Q}$) = {Id.}; Aut($\mathbb{Q}(\sqrt{5})$) ≅ $\mathbb{Z}_2$.
Proposition	If K is an extension of $\mathbb{Q}$ and $\varphi \in$ Aut(K), then φ fixes $\mathbb{Q}$.
Theorem	Let E/F be an extension and $f(x) \in F[x]$. Let $\alpha \in E$ be a root of $f(x)$. Let $\varphi \in$ Aut(E). If φ fixes F, the $\varphi(\alpha)$ is a root of $f(x)$.
Note	The theorem says that automorphisms permute roots.
Example	Aut($\mathbb{Q}(\sqrt[3]{5})$) = {Id.}
Example	$p(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$. Let E be splitting field for $p(x)$. If $\varphi \in$ Aut(E), will any permutation work?
Example	Determine Aut(E).
Lemma	Let K be a field and $E = K(\alpha)$. If $\varphi \in$ Aut(E) such that φ fixes K and α, then φ = Id.
Lemma	Let F be a field and $E = F(z_1, z_2, \ldots, z_n)$. If $\varphi \in$ Aut(E) such that φ fixes F and z_i for all i, then φ = Id.
Definition	(1) Gal (E/F); (2) The Galois group of $p(x)$ over F.
Proposition	Gal(E/F) ≤ Aut(E).

Example Let $\varphi:\mathbb{Q}(\sqrt{5})\to\mathbb{Q}(\sqrt{5})$ be an isomorphism. What does φ do to $\mathbb{Q}$ and $\sqrt{5}$? $\varphi(\frac{p}{q}) = \frac{p}{q}$. $\varphi(\sqrt{5})$ must = $\pm\sqrt{5}$.

Proof:
We know $\varphi(1) = 1$, $\varphi(n) = \varphi(1 + \cdots + 1) = \varphi(1) + \cdots + \varphi(1) = n$, $n \in \mathbb{N}$.
And by hmo properties, we have
$\forall\ n \in \mathbb{N}$ $\varphi(-n) = -\varphi(n) = -n$, $\varphi(n^{-1}) = \varphi(n)^{-1} = n^{-1}$,
and $\forall\ ab^{-1} \in \mathbb{Q}$ where $a, b \in \mathbb{Z}$, $b \neq 0$, we have
$\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)\varphi(b)^{-1} = ab^{-1}$.
So φ must fix $\mathbb{Q}$. Where can $\sqrt{5}$ get sent? $\sqrt{5}$ is a root of $x^2 - 5$.
Since $\varphi(\sqrt{5})\varphi(\sqrt{5}) = (\varphi(\sqrt{5}))^2 = \varphi(5) = 5$, then
$\varphi(\sqrt{5})$ must equal $\sqrt{5}$ or $-\sqrt{5}$.

Definition Let F be a field and K an extension of F.
(1) An isomorphism $\varphi:K \to K$ is called an *automorphism* of K.
(2) The set of all automorphisms is denoted *Aut(K).*
(3) If φ *fixes* F then $\varphi(x) = x\ \forall\ x \in F$. (i.e. $\varphi|_F = \mathrm{Id}_F$)

Proposition Aut(K) is a group under composition.

Proof:
$i : K \to K$, the identity map, is an automorphisms, hence Aut(K) $\neq \varnothing$.

Let $\sigma, \tau \in$ Aut(K). We will show $\sigma \circ \tau$ is an automorphism.
$\forall\, j, k \in K$, $(\sigma \circ \tau)(j + k) = \sigma(\tau(j) + \tau(k)) = \sigma(\tau(j)) + \sigma(\tau(k))$, and
$\sigma \circ \tau(jk) = \sigma(\tau(j)\tau(k)) = \sigma(\tau(j))\sigma(\tau(k))$, so $\sigma \circ \tau$ is a homomorphism.

To show $\sigma \circ \tau$ is injective, let $j, k \in K$ such that $\sigma(\tau(j)) = \sigma(\tau(k))$. Then as σ and τ are injective, we have $\sigma(\tau(j)) = \sigma(\tau(k)) \Rightarrow \tau(j) = \tau(k) \Rightarrow j = k$.

To show $\sigma \circ \tau$ is surjective, let $w \in (\sigma \circ \tau)(K)$.
Since σ is surjective, $\exists\, k \in K$ such that $\sigma(k) = w$.
And since τ is surjective $\exists\, j \in K$ such that $\tau(j) = k$.
Hence, $\sigma(\tau(j)) = \sigma(k) = w$, and $\sigma \circ \tau$ is surjective,
So $\sigma \circ \tau \in$ Aut(K). Thus, Aut(K) is closed under composition.

Since $\forall\, k \in K$, $(i \circ \sigma)(k) = i(\sigma(k)) = \sigma(k) = \sigma(i(k)) = (\sigma \circ i)(k)$, then the identity map, i, is the identity of Aut(K).

Claim: $\forall\, \sigma \in$ Aut(K), there is $\tau \in$ Aut(K) such that $\sigma \circ \tau = i = \tau \circ \sigma$.
Define $\tau: K \to K$ by $\tau(k) = j$, where $k = \sigma(j)$. $\forall\, k \in K$.
To show τ is well-defined and injective, let $a, b \in K$.
Then $\tau(a) = c$ and $\tau(b) = d$ for some $c, d \in K$.
And since σ is well-defined and injective, we have
$\tau(a) = \tau(b) \Leftrightarrow c = d \Leftrightarrow \sigma(c) = \sigma(d) \Leftrightarrow a = b$.
To show τ is surjective, let $j \in \tau(K)$.
Since σ is surjective, then $\sigma(j) = k$ for some $k \in K$, and hence $\tau(k) = j$.
Thus, $\tau = \sigma^{-1}$. Hence every element of Aut(K) has an inverse.

$\therefore$ Aut(K) satisfies the axioms of a group under composition.

Example Aut($\mathbb{Q}$) = {Id.}; Aut($\mathbb{Q}(\sqrt{5})$) = $\{\varphi_1 = \text{Id.}, \varphi_2\} \cong \mathbb{Z}_2$.

Proposition If K is an extension of $\mathbb{Q}$ and $\varphi \in$ Aut(K), then φ fixes $\mathbb{Q}$.

Proof: Homework
We know $\varphi(1) = 1_{\varphi(K)}$, so
$\varphi(n) = \varphi(1 + \cdots + 1) = \varphi(1) + \cdots + \varphi(1) = n \bullet 1_{\varphi(K)} = n$, $n \in \mathbb{N}$.
And by hmo properties, we have
$\forall\, n \in \mathbb{N}$ $\varphi(-n) = -\varphi(n) = -n$ and $\varphi(n^{-1}) = \varphi(n)^{-1} = n^{-1}$.
So then $\forall\, w \in \mathbb{Q}$, $w = ab^{-1}$ where $a, b \in \mathbb{Z}$, $b \neq 0$, and we have
$\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)\varphi(b)^{-1} = ab^{-1}$.
So φ must fix $\mathbb{Q}$.

Theorem Let E/F be an extension and $f(x) \in F[x]$. Let $\alpha \in E$ be a root of $f(x)$. Let $\varphi \in \mathrm{Aut}(E)$. If φ fixes F, then $\varphi(\alpha)$ is a root of $f(x)$.

Proof:
Let $f(x) = c_0 + c_1x + c_2x^2 + \cdots + c_nx^n$, where $c_i \in F$.
$0 = \varphi(0) = \varphi(f(\alpha))$
$= \varphi(c_0 + c_1x + c_2x^2 + \cdots + c_nx^n)$
$= \varphi(c_0) + \varphi(c_1)\varphi(x) + \varphi(c_2)\varphi(x^2) + \cdots + \varphi(c_n)\varphi(x^n)$
$= c_0 + c_1\varphi(x) + c_2\varphi(x)^2 + \cdots + c_n\varphi(x)^n$,
$= f(\varphi(\alpha))$.

Note The theorem says that automorphisms permute roots.

Example $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{5})) = \{\mathrm{Id.}\}$
Proof:

Let $f(x) = x^3 - 5$. $X = \{\alpha | f(\alpha) = 0\} = \{\sqrt[3]{5}, \sqrt[3]{5}\, e^{\frac{2\pi i}{3}}, \sqrt[3]{5}\, e^{\frac{4\pi i}{3}}\}$.
If $\varphi \in \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{5}))$, then φ must send $\sqrt[3]{5}$ to another root of $f(x)$.
Since elements in $\mathbb{Q}(\sqrt[3]{5})$ look like $a + b\sqrt[3]{5} + d(\sqrt[3]{5})^2$ and φ fixes $\mathbb{Q}$, then $\varphi(a + b\sqrt[3]{5} + d(\sqrt[3]{5})^2) = \varphi(a) + \varphi(b)\varphi(\sqrt[3]{5}) + \varphi(d)\varphi(\sqrt[3]{5}))^2 =$
$a + b\varphi(\sqrt[3]{5}) + d\varphi(\sqrt[3]{5}))^2$. Thus, we know φ is completely determined by where $\sqrt[3]{5}$ gets sent.
$\varphi|_{Q(\sqrt[3]{5})\cap X}\ \mathbb{Q}(\sqrt[3]{5}) \cap X \to \mathbb{Q}(\sqrt[3]{5}) \cap X = \{\sqrt[3]{5}\}$ is an automorphism.
And so $\varphi(\sqrt[3]{5}) = \sqrt[3]{5}$ (i.e. $\varphi = \mathrm{Id.}$), hence $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{5})) = \{\mathrm{Id.}\}$

Example $p(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$. Let E be a splitting field for $p(x)$.
If $\varphi \in \mathrm{Aut}(E)$, will any permutation work? No.

Proof:
Since $p(x + 1) = x^4 + 5x^3 + 10x^2 + 10x + 5$, and by Eisenstein's Criterion, $p(x + 1)$ is irreducible, then $p(x)$ is irreducible.
Let E be a splitting field for $p(x)$.
Let $\varphi \in \mathrm{Aut}(E)$.
Since $x^5 - 1 = (x - 1)p(x)$, then the roots of $p(x)$ are the primitive 5^{th} roots of unity.
So $X = \{\alpha | p(\alpha) = 0\} = \{e^{\frac{2\pi i}{5}}, e^{\frac{4\pi i}{5}}, e^{\frac{6\pi i}{5}}, e^{\frac{8\pi i}{5}}\} = \{\alpha, \alpha^2, \alpha^3, \alpha^4\}$.
$\varphi|_X : X \to X$. Suppose $\alpha \mapsto \alpha^2 \mapsto \alpha^3 \mapsto \alpha^4 \mapsto \alpha$.
Then $\varphi(\alpha^2) = \alpha^3$
So $\alpha^4 = \alpha^2 \bullet \alpha^2 = \varphi(\alpha)\varphi(\alpha) = \varphi(\alpha^2) = {}^3$. A contradiction.
So this permutation does not give rise to an automorphism.

Example Determine Aut(E) where E is the splitting field for $p(x)$.

$\text{Aut}(E) \cong \mathbb{Z}_4$.

Proof:
You'll show $E = \mathbb{Q}(\alpha)$.
$E = \{c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 \mid c_i \in \mathbb{Q}\}$
Let $\varphi \in \text{Aut}(E)$. φ is completely determined by where α gets sent.
Possible φ's: $\varphi_1(\alpha) = \alpha$, $\varphi_2(\alpha) = \alpha^2$, $\varphi_3(\alpha) = \alpha^3$, $\varphi_4(\alpha) = \alpha^4$.
Since $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(p(x)) \cong \mathbb{Q}(\alpha^i)$, then all possible φ's are verified.
Thus $\text{Aut}(E) = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}$. So then $\text{Aut}(E) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ or $\text{Aut}(E) \cong \mathbb{Z}_4$.
Let's find the order of φ_2.
$\varphi_2 \circ \varphi_2 (\alpha) = \varphi_2(\alpha^2) = \varphi_2(\alpha)^2 = (\alpha^2)^2 = \alpha^4$. Since $\varphi_2 \circ \varphi_2 (\alpha) \neq \alpha$, then $\text{ord}(\varphi_2) > 2$.
Thus $\text{Aut}(E) \cong \mathbb{Z}_4$.

Lemma Let K be a field and $E = K(\alpha)$. If $\varphi \in \text{Aut}(E)$ such that φ fixes K and α, then $\varphi = \text{Id}$.

Proof:
Let $u \in E$. We want to show $\varphi(u) = u$.
Since $\text{Frac}(K[\alpha]) = K(\alpha)$, then

$$u \in \text{K}(\alpha) \Rightarrow u = \frac{f(\alpha)}{g(\alpha)} \text{ where } f(x), g(x) \in K[x].$$

$$\varphi(u) = \varphi\left(\frac{f(\alpha)}{g(\alpha)}\right) = \varphi(f(\alpha)g(\alpha)^{-1})$$
$$= \varphi(f(\alpha))\varphi(g(\alpha))^{-1}$$
$$= f(\varphi(\alpha))g(\varphi(\alpha))^{-1} \text{ since } \varphi \text{ fixes } K$$
$$= f(\alpha)g(\alpha)^{-1} \text{ since } \varphi \text{ fixes } \alpha$$
$$= u.$$

Lemma Let F be a field and $E = F(z_1, z_2, \ldots, z_n)$. If $\sigma \in \text{Aut}(E)$ such that σ fixes F and z_i for all i, then $\sigma = \text{Id}$.

Proof: By induction. Good thing for you to look at.
Since $E = F(z_1, z_2, \ldots, z_{n-1})(z_n)$, it suffices to show this is true for $n = 1$.
For if the result is true for $n = 1$, and we assume the result is true
$\forall\ k < n$ where $n > 1$, then σ fixes F and z_i for $i = 1, 2, \ldots, n - 1$.
We can let $F' = F(z_1, z_2, \ldots, z_{n-1})$ and claim σ fixes F' by our induction hypothesis. Then the base case applies to $F'(z_n) = E$ and we have σ is the identity for E.

By the preceding lemma, we have that the result holds for the base case.

$\therefore$ σ is the identity mapping.

Definition (1) Let E/F be an extension. The *Galois group* of E over F, denoted Gal (E/F), is the set of all automophisms of E that fix F.

(2) Let $p(x) \in F[x]$. The *Galois group of p(x)* over F is defined to be Gal(E/F) where E is a splitting field of $p(x)$.

Proposition Gal$(E/F) \leq$ Aut(E).

Proof:

Clearly Gal$(E/F) \subseteq$ Aut(E).

$i : E \to E$, the identity map, is an automorphism that fixes F, hence Gal$(E/F) \neq \varnothing$.

If $\sigma, \tau \in$ Gal(E/F), then since Aut(E) is a group under composition (see proof above), we know $\sigma \circ \tau \in$ Aut(E).
Since $\sigma, \tau \in$ Gal(E/F), then $\forall\ c \in F$, $(\sigma \circ \tau)(c) = \sigma(\tau(c)) = \sigma(c) = c$.
So $\sigma \circ \tau \in$ Gal(E/F). Hence Gal(E/F) is closed under composition.

Since Gal$(E/F) \subseteq$ Aut(E), i is the identity of Aut(E), and i fixes F, then i is the identity of Gal(E/F).

Since every element σ of Aut(E) has an inverse, σ^{-1}, then if $\sigma \in$ Gal(E/F), we have
$\forall\ c \in F$, $\sigma(c) = c$, and $\sigma^{-1}(c) = \sigma^{-1}(\sigma(c)) = c$, hence $\sigma^{-1} \in$ Gal(E/F).
$\therefore$ Gal(E/F) satisfies all the axioms of a subgroup.