We begin studying **Galois theory**. In Galois theory we consider a field extension $F \leq E$ and try to understand the "symmetries" of the extension, that is the set of field isomorphisms $\psi\colon E \to E$ such that $\psi(a) = a$ for all $a \in F$. It is useful to first analyse the following more general question:

> Given field extensions $F \leq E$ and $F \leq E'$, what are the homomorphisms $\psi\colon E \to E'$ such that $\psi(a) = a$ for all $a \in F$?

Today we will give a general answer in the case where $E = F(\alpha)$ for α algebraic over F. The main insight is that $\psi(\alpha) \in E'$ has to be "conjugate" to α:

Definition. Let F be a field, and let α, β be algebraic over F. Then we say that α and β are **conjugate over** F if $\operatorname{irr}(\alpha, F) = \operatorname{irr}(\beta, F)$.

Example. Let $a, b \in \mathbb{R}$, $b \neq 0$, and consider $a + ib \in \mathbb{C}$. Then

$$(x - (a + ib))(x - (a - ib)) = x^2 - 2ax + a^2 + b^2 \in \mathbb{R}[x],$$

so we have

$$\operatorname{irr}(a + ib, \mathbb{R}) = x^2 - 2ax + a^2 + b^2.$$

Since $b^2 = (-b)^2$, we have $\operatorname{irr}(a + ib, \mathbb{R}) = \operatorname{irr}(a - ib, \mathbb{R})$, which means that $a + ib$ and $a - ib$ are conjugate over $\mathbb{R}$.

Example. If $a, b \in \mathbb{Q}$, $b \neq 0$, one checks similarly that

$$\operatorname{irr}(a + b\sqrt{2}, \mathbb{Q}) = x^2 - 2ax + a^2 - 2b^2.$$

Here $\operatorname{irr}(a + b\sqrt{2}, \mathbb{Q}) = \operatorname{irr}(a - b\sqrt{2}, \mathbb{Q})$, so $a + b\sqrt{2}$ and $a - b\sqrt{2}$ are conjugate over $\mathbb{Q}$.

Theorem. *Let F be a field and let α, β be algebraic over F. The following two conditions are equivalent.*

(1) *α and β are conjugate over F.*
(2) *There exists a field isomorphism $\psi_{\alpha,\beta}\colon F(\alpha) \to F(\beta)$ such that*

$$\psi_{\alpha,\beta}(\alpha) = \beta$$

and

$$\psi_{\alpha,\beta}(a) = a$$

for all $a \in F$.

Proof. (2) $\Rightarrow$ (1) : Assume $\psi_{\alpha,\beta}$ is an isomorphism of fields as above. Let

$$f(x) = \operatorname{irr}(\alpha, F) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \quad c_i \in F$$

Then

$$\begin{aligned} f(\beta) &= \beta^n + c_{n-1}\beta^{n-1} + \cdots + c_0 = \psi_{\alpha,\beta}(\alpha)^n + \psi_{\alpha,\beta}(c_{n-1})\psi_{\alpha,\beta}(\alpha)^{n-1} + \cdots + \psi_{\alpha,\beta}(c_0) \\ &= \psi_{\alpha,\beta}(\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0) = \psi_{\alpha,\beta}(f(\alpha)) = \psi_{\alpha,\beta}(0) = 0, \end{aligned}$$

so β is a zero of $f(x)$. But since $f(x)$ is irreducible and monic, that means $\operatorname{irr}(\beta, F) = f(x)$, so α and β are conjugate over F.

(1) $\Rightarrow$ (2) : Recall that $F(\alpha) \simeq F[x]/\langle \operatorname{irr}(\alpha, F)\rangle$ and $F(\beta) \simeq F[x]/\langle \operatorname{irr}(\beta, F)\rangle$. Since $\operatorname{irr}(\alpha, F) = \operatorname{irr}(\beta, F)$, this gives an isomorphism $F(\alpha) \simeq F(\beta)$, which one can check has the properties that we claim.

□

Theorem. *Let F be a field, let α be algebraic over F, and let $\overline{F}$ be an algebraic closure of F.*

(1) *Let $\psi\colon F(\alpha) \to \overline{F}$ be a homomorphism such that $\psi(a) = a$ for all $a \in F$. Then $\psi(\alpha) \in \overline{F}$ must be a conjugate of α over F.*
(2) *If $\beta \in \overline{F}$ is a conjugate of α, there is a unique homomorphism $\psi_{\alpha,\beta}\colon F(\alpha) \to \overline{F}$ such that $\psi_{\alpha,\beta}(\alpha) = \beta$ and $\psi_{\alpha,\beta}(a) = a$ for all $a \in F$.*

Proof. (1): Let $\beta = \phi(\alpha)$, and let $f(x) = \operatorname{irr}(\alpha, F)$ The same computation as in (2) $\Rightarrow$ (1) in the previous proof shows that

$$f(\beta) = f(\psi(\alpha)) = \psi(f(\alpha)) = \psi(0) = 0.$$

Hence β is a zero of $f(x)$, so $\operatorname{irr}(\beta, F) = f(x) = \operatorname{irr}(\alpha, F)$, which means β is a conjugate of α over F.

(2): Let $\beta \in \overline{F}$ be a conjugate of α over F, then we have $F(\beta) \leq \overline{F}$ and can use the isomorphism $\psi_{\alpha,\beta}\colon F(\alpha) \to F(\beta)$ from the previous theorem. □

Remark. If α and β are conjugate over F and $\deg(\alpha, F) = \deg(\beta, F) = n$, then every $\gamma \in F(\alpha)$ can be written uniquely as

$$\gamma = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}, \quad a_i \in F.$$

The isomorphism $\phi\colon F(\alpha) \to F(\beta)$ constructed above then has the formula

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

Example. The elements $i, -i \in \mathbb{C}$ are conjugate over $\mathbb{R}$. We have $\mathbb{R}(i) = \overline{\mathbb{R}} = \mathbb{C}$. The homomorphism $\psi_{i,-i}\colon \mathbb{R}(i) \to \overline{\mathbb{R}}$ is given by

$$\psi_{i,-i}(a_0 + a_1 i) = a_0 + a_1(-i) = a_0 - a_1 i, \qquad a_0, a_1 \in \mathbb{R}.$$

In other words $\psi_{i,-i}(z) = \bar{z}$, the complex conjugate of z.

Example. In $\overline{\mathbb{Q}}$, the conjugates (over $\mathbb{Q}$) of $\sqrt{2}$ are $\sqrt{2}$ and $-\sqrt{2}$. We therefore get precisely two homomorphisms $\psi\colon \mathbb{Q}(\sqrt{2}) \to \overline{\mathbb{Q}}$ satisfying $\psi(a) = a$ for $a \in \mathbb{Q}$, namely

$$\psi_{\sqrt{2},\sqrt{2}}(a_0 + a_1\sqrt{2}) = a_0 + a_1\sqrt{2} \qquad a_i \in \mathbb{Q}$$

and

$$\psi_{\sqrt{2},-\sqrt{2}}(a_0 + a_1\sqrt{2}) = a_0 - a_1\sqrt{2} \qquad a_i \in \mathbb{Q}$$

1. Automorphisms

Definition. Let E be a field. A field isomorphism $\psi\colon E \to E$ is called an **automorphism** of E.

Definition. Let σ be an autmorphism of E.

- An element $a \in E$ is **fixed** by σ if $\sigma(a) = a$.
- If $F \leq E$ is a subfield such that σ fixes every $a \in F$, we say that σ **fixes** F.
- If S is a set of automorphisms of E such that every $\sigma \in S$ fixes F, we say that S **fixes** F.

Example. The field automorphism $\psi_{i,-i}\colon \mathbb{C} \to \mathbb{C}$ given by $\psi_{i,-i}(a_0 + ia_1) = a_0 - ia_1$ fixes $\mathbb{R}$.

Theorem. *Let E be a field, and let S be a set of automorphisms of E. Let $F = \{a \in E \mid a \text{ is fixed by every } \sigma \in S\}$. Then F is a subfield of E.*

We call F the **fixed field** of S, or if $S = \{\sigma\}$, the fixed field of σ.

Example. The fixed field of $\psi_{i,-i}$ is the set of those $a_0 + ia_1 \in \mathbb{C}$ such that

$$a_0 + a_1 i = \psi_{i,-i}(a_0 + a_1 i) = a_0 - a_1 i,$$

equivalently such that $a_1 = 0$. Hence the fixed field of $\psi_{i,-i}$ is $\mathbb{R}$.

Theorem. *Let E be a field. The set of automorphisms of E forms a group under composition.*

Proof. An automorphism of E is by definition a bijection $\tau\colon E \to E$, hence the automorphisms of E form a subset of the permutations of E. One checks that this is a subgroup (has identity, inverses and closed under the group multiplication). □

Theorem. *Let $F \leq E$ be a field, and let $G(E/F)$ be the set of automorphisms of E which leave F fixed. Then $G(E/F)$ is a subgroup of of the group of automorphisms of E.*

Proof. One checks that the set $G(E/F)$ has the identity, inverses, and is closed under group multiplication. □

Example. Let's compute $G(\mathbb{C}/\mathbb{R})$. Since $\mathbb{C} = \mathbb{R}(i)$, and the conjugates of i over $\mathbb{R}$ are i and $-i$, we have exactly two homomorphisms $\psi\colon \mathbb{C} = \mathbb{R}(i) \to \mathbb{C}$ which fix $\mathbb{R}$, namely

$$\psi_{i,i}(a_0 + a_1 i) = a_0 + a_1 i \qquad a_i \in \mathbb{R}$$

and

$$\psi_{i,-i}(a_0 + a_1 i) = a_0 - a_1 i \qquad a_i \in \mathbb{R}.$$

It is easy to see that these homomorphisms are isomorphisms and so define elements of $G(\mathbb{C}/\mathbb{R})$. Thus $G(\mathbb{C}/\mathbb{R}) = \{\psi_{i,i}, \psi_{i,-i}\}$, the group of two elements, where $\psi_{i,i}$ is the identity element and $\psi_{i,-i}\psi_{i,-i} = \psi_{i,-i} \circ \psi_{i,-i} = \psi_{i,i}$.

Example. Let's consider the automorphism group $G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$. In a previous example its been shown that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, with a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ as a vector space over $\mathbb{Q}$ given by

$$1, \sqrt{2}, \sqrt{3}, \sqrt{6}.$$

Concretely this means that every element $\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ can be written uniquely as

$$\alpha = a_1 + a_2\sqrt{2} + a_3\sqrt{3} + a_4\sqrt{6}, \qquad a_i \in \mathbb{Q}.$$

To compute the group $G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$, let τ be an element of the group. Then by assumption τ fixes $\mathbb{Q}$, so $\tau(a) = a$ for all $a \in \mathbb{Q}$. With α on the form above, we get

$$\begin{aligned}\tau(\alpha) &= \tau(a_1 + a_2\sqrt{2} + a_3\sqrt{3} + a_4\sqrt{6}) \\ &= \tau(a_1) + \tau(a_2)\tau(\sqrt{2}) + \tau(a_3)\tau(\sqrt{3}) + \tau(a_4)\tau(\sqrt{6}) \\ &= a_1 + a_2\tau(\sqrt{2}) + a_3\tau(\sqrt{3}) + a_4(\tau\sqrt{6}).\end{aligned}$$

Moreover $\sqrt{6} = \sqrt{2}\sqrt{3}$ gives

$$\tau(\sqrt{6}) = \tau(\sqrt{2}\sqrt{3}) = \tau(\sqrt{2})\tau(\sqrt{3}),$$

and so

$$\tau(\alpha) = a_1 + a_2\tau(\sqrt{2}) + a_3\tau(\sqrt{3}) + a_4\tau(\sqrt{2})\tau(\sqrt{3}).$$

The upshot is that τ is completely determined by the value of $\tau(\sqrt{2})$ and $\tau(\sqrt{3})$.

We must have $\tau(\sqrt{2})$ a conugate of $\sqrt{2}$ over $\mathbb{Q}$, and $\tau(\sqrt{3})$ a conjugate of $\sqrt{3}$ over $\mathbb{Q}$. This means $\tau(\sqrt{2}) = \pm\sqrt{2}$ and $\tau(\sqrt{3}) = \pm\sqrt{3}$.

We check that each of these four possiblities are achieved letting $\tau_{00}, \tau_{01}, \tau_{10}, \tau_{11}$ be defined by

$$\tau_{ij}(a_1 + a_2\sqrt{2} + a_3\sqrt{3} + a_4\sqrt{6}) = a_1 + (-1)^i a_2\sqrt{2} + (-1)^j a_3\sqrt{3} + (-1)^{i+j}\sqrt{6},$$

where each one can be seen to give an automorphism of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ fixing $\mathbb{Q}$. Computing the compositions of the τ_{ij} gives the multiplication table

	τ_{00}	τ_{01}	τ_{10}	τ_{11}
τ_{00}	τ_{00}	τ_{01}	τ_{10}	τ_{11}
τ_{01}	τ_{01}	τ_{00}	τ_{11}	τ_{10}
τ_{10}	τ_{10}	τ_{11}	τ_{00}	τ_{01}
τ_{11}	τ_{11}	τ_{01}	τ_{10}	τ_{00}

, from which we see that

$$G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{\tau_{00}, \tau_{01}, \tau_{10}, \tau_{11}\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Example. Let F be a finite field. Then there is a prime $p = \text{char}(F)$ such that $\mathbb{Z}_p \leq F$. We know that for $\alpha, \beta \in F$ we have

$$(\alpha + \beta)^p = \alpha^p + \beta^p.$$

This means that the map $Fr\colon F \to F$ given by

$$Fr(\alpha) = \alpha^p$$

is in fact a ring homomorphism.

Since F is a field, $\ker Fr = 0$ or $\ker Fr = F$, and since $Fr(1) = 1^p \neq 0$, we have $\ker Fr = 0$. This means that Fr is one-to-one, and since F is finite, it follows that Fr must also be onto. Hence Fr is an automorphism of F.

One can check that the fixed field of Fr is $\mathbb{Z}_p$, and so $Fr \in G(F/\mathbb{Z}_p)$.