SECTION 49 – THE ISOMORPHISM EXTENSION THEOREM

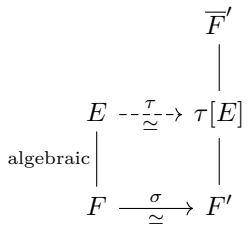
Remark. For us a field homomorphism $\psi\colon E \to E'$ will always be assumed to be such that $\psi(1) = 1$. Since E is a field, the only ideals of E are $\{0\}$ and E, and with the assumption that $\psi(1) = 1 \neq 0$ we must have $\ker \psi = \{0\}$. Then ψ is one-to-one, and in particular we have an isomorphism

$$E \simeq \psi[E] \leq E'.$$

Thus every field homomorphism gives an isomorphism of the source onto a subfield of the target.

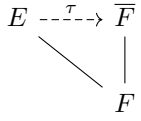
Theorem (The isomorphism extension theorem)**.** *Let $F \leq E$ be an algebraic field extension. Let $\sigma\colon F \to F'$ be a field isomorphism, and let $\overline{F}'$ be an algebraic closure of F'. Then there exists a field homomorphism $\tau\colon E \to \overline{F}'$ such that*

$$\tau(a) = \sigma(a), \qquad \forall a \in F.$$



Corollary. *For every algebraic field extension $F \leq E$ and algebraic closure $\overline{F}$, we can find a field homomorphism $\tau\colon E \to \overline{F}$ such that*

$$\tau(a) = a \qquad \forall a \in F.$$



Proof. Take $F = F'$ and let $\sigma(a) = a$ in the isomorphism extension theorem. □

Remark. We can identify E with $\tau[E] \leq \overline{F}$. Hence every algebraic extension E of F can be thought of as a subfield of $\overline{F}$, and we'll mostly use this without further comment.

Corollary. *Let F be a field, let $\sigma\colon F \to F'$ be an isomorphism, and let $\overline{F}$ and $\overline{F}'$ be algebraic closures of F and F'. Then there exist an isomorphism $\tau\colon \overline{F} \to \overline{F}'$ such that*

$$\tau(a) = \sigma(a) \qquad \forall a \in F$$

$$\begin{array}{ccc} \overline{F} & \xrightarrow[\simeq]{\tau} & \overline{F}' \\ | & & | \\ F & \xrightarrow[\simeq]{\sigma} & F' \end{array}$$

Proof. The isomorphism extension theorem gives a τ which extends σ, and we only need to prove that τ is an isomorphism.

We have the tower of fields $F' \leq \tau[\overline{F}] \leq \overline{F}'$. The extension $F \leq \overline{F}'$ is algebraic, hence the extension $\tau[\overline{F}] \leq F'$ is algebraic. But $\tau[\overline{F}] \simeq \overline{F}$ is algebraically closed, so has no proper algebraic extensions. Hence $\tau[\overline{F}] = \overline{F}'$, which means that τ is an isomorphism. □

Proof of the isomorphism extension theorem. We will make two simplifications. Firstly, we will assume that $F = F'$ and that $\sigma(a) = a$. The general case is only slightly more complicated but involves way more notation.

Secondly, we will only treat the special case where $F \leq E$ is finite.[1] Then we can write $E = F(\alpha_1, \ldots, \alpha_n)$ where each α_i is algebraic over F. We then construct our τ by extending it one step at a time.

$$\begin{array}{ccc} & & \overline{F} \\ & & | \\ F(\alpha_1, \ldots, \alpha_n) & \xrightarrow{\tau_n} & \tau_n[F(\alpha_1, \ldots, \alpha_n)] \\ | & & | \\ \vdots & & \vdots \\ | & & | \\ F(\alpha_1, \alpha_2) & \xrightarrow{\tau_2} & \tau_2[F(\alpha_1, \alpha_2)] \\ | & & | \\ F(\alpha_1) & \xrightarrow{\tau_1} & \tau_1[F(\alpha_1)] \\ | & & | \\ F & = & F \end{array}$$

To construct τ_1, let $f(x) = \operatorname{irr}(\alpha_1, F) \in F[x]$. Since $\overline{F}$ is algebraically closed, there exists a $\beta \in \overline{F}$ such that $f(\beta) = 0$. Since $f(x)$ is irreducible, we then have that $\operatorname{irr}(\beta, F) = f(x)$, so α and β are conjugate over F. Then from last lecture we know there is a unique homomorphism $\tau_1 \colon F(\alpha_1) \to \overline{F}$ such that $\tau_1(\alpha) = \beta$ and $\tau_1(a) = a$ for all $a \in F$.

This argument proves the isomorphism extension theorem for the case of simple extensions. We can then use this to extend τ_1 to a $\tau_2 \colon F(\alpha_1, \alpha_2) \to \overline{F}$, and so on all the way to $\tau_n \colon F(\alpha_1, \ldots, \alpha_n) \to \overline{F}$. □

[1] The general case requires a very different argument using Zorn's lemma.

1. Index of a finite extension

Let $F \leq E$ be a finite field extension, and assume $E \leq \overline{F}$. We are interested in $G(E/F)$, the automorphism group of E over F. This set of automorphisms sits inside a bigger set, namely the set of field homomorphisms $\tau\colon E \to \overline{F}$ which fix F. We try to understand the cardinality of this second set.

Theorem. *Let $F \leq E$ be a finite field extension, let $\sigma\colon F \to F'$ be an isomorphism, and let $\overline{F}'$ be an algebraic closure of F. Let S be the set of all field homomorphisms $\psi\colon E \to \overline{F}'$ such that*

$$\psi(a) = \tau(a) \qquad \forall a \in F.$$

Then

1. *The cardinality of S only depends on $F \leq E$, and not on τ, F' or $\overline{F}'$*
2. *The cardinality of S is finite.*

Proof. (1): Omitted.

(2): Since $F \leq E$ is finite, we can write $E = F(\alpha_1, \ldots, \alpha_n)$ with α_i algebraic over F. By (1) we may assume that $F = F'$ and $\sigma(a) = a$. A homomorphisms $\tau\colon F(\alpha_1, \ldots, \alpha_n) \to \overline{F}$ fixing F is determined by the value of $\tau(\alpha_i)$. For each i, let $\beta_i = \tau(\alpha_i)$. Since τ gives a homomorphism $F(\alpha_i) \to \overline{F}$ fixing F, we know that β_i must be a conjugate of α_i. This means that β_i is a zero of $\operatorname{irr}(\alpha_i, F)$. There are at most $\deg(\alpha_i, F)$ zeros of $\operatorname{irr}(\alpha_i, F)$ in $\overline{F}$, so there are at most $\deg(\alpha_i, F)$ possible choices for β_i.

Hence there are finitely many choices for the β_i, and so finitely many choices for the homomorphism τ. □

Example. To illustrate the above proof, consider $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. A homomorphism $\tau\colon \mathbb{Q}(\sqrt{2}, \sqrt{3}) \to \overline{\mathbb{Q}}$ must send $\sqrt{2}$ to a conjugate of $\sqrt{2}$ and $\sqrt{3}$ to a conjugate of $\sqrt{3}$. Since both $\sqrt{2}$ and $\sqrt{3}$ have two conjugates, there are at most $(2)(2) = 4$ homomorphisms τ.

Definition. Let $F \leq E$ be a finite field extension. The number of field homomorphisms $\tau\colon E \to \overline{F}$ fixing F is called the **index** of E over F, and denoted $\{E : F\}$.

Example. We compute $\{\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\}$. The element $\sqrt{2}$ has exactly two conjugates $\sqrt{2}, -\sqrt{2}$ in $\overline{\mathbb{Q}}$ over $\mathbb{Q}$. Therefore there are exactly two homomorphisms

$$\psi_{\sqrt{2},\sqrt{2}}\colon \mathbb{Q}(\sqrt{2}) \to \overline{\mathbb{Q}}$$
$$\psi_{\sqrt{2},-\sqrt{2}}\colon \mathbb{Q}(\sqrt{2}) \to \overline{\mathbb{Q}},$$

which means that $\{\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\} = 2$.

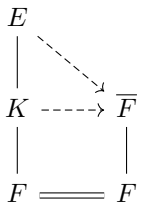
Remark. For a finite field extension $F \leq E$, we have $|G(E/F)| \leq \{E : F\}$.

Proof. We can find an inclusion of E as a subfield of $\overline{F}$. Then every automorphism of E fixing F is in particular a field homomorphism $\tau\colon E \to \overline{F}$ fixing F, so the number of automorphisms is $\leq \{E : F\}$. □

Theorem. *Let $F \leq K \leq E$ be a tower of finite field extensions. Then*

$$\{E : F\} = \{E : K\}\{K : F\}.$$

Proof. The left hand side gives the number of homomorphisms $\psi\colon E \to \overline{F}$ fixing F. Every such homomorphism can be obtained by first giving an extension $\psi_K : K \to \overline{F}$ fixing K, and then giving a homomorpism $\psi\colon E \to \overline{F}$ such that $\psi(b) = \psi_K(b)$ for all $b \in K$. There are exactly $\{K : F\}$ choices for ψ_K, and given ψ_K there are exactly $\{E : K\}$ choices for ψ.



□

Example. Consider $\mathbb{Q} < \mathbb{Q}(\sqrt{2}, \sqrt{3})$. In a previous example we have seen that there are precisely 4 homomorphisms $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \to \overline{\mathbb{Q}}$ fixing $\mathbb{Q}$, concretely these are $\psi_{00}, \psi_{01}, \psi_{10}, \psi_{11}$ with

$$\psi_{ij}(a_1+a_2\sqrt{2}+a_3\sqrt{3}+a_4\sqrt{6}) = a_1+(-1)^i a_2\sqrt{2}+(-1)^j a_3\sqrt{3}+(-1)^{i+j}a_4\sqrt{6} \quad a_i \in \mathbb{Q}.$$

This means that $\{\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}\}$. Alternatively, we could had computed

$$\{\mathbb{Q}(\sqrt{2}, \sqrt{3} : \mathbb{Q}\} = \{\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})\}\{\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\} = (2)(2) = 4$$

(here we omit the computation of $\{\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})\} = 2$).

Example. Consider $\mathbb{Q} < \mathbb{Q}(\sqrt[3]{2})$. The number of field homomorphisms $\tau\colon \mathbb{Q}(\sqrt[3]{2}) \to \overline{\mathbb{Q}}$ fixing $\mathbb{Q}$ equals the number of conjugates of $\sqrt[3]{2}$. The conjugates of $\sqrt[3]{2}$ over $\mathbb{Q}$ must all be zeros of $\mathrm{irr}(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$, and conversely all zeros of $x^3 - 2$ are conjugates to $\sqrt[3]{2}$ over $\mathbb{Q}$.

We know that the complex zeros of $x^3 - 2$ are $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$, where $\omega = e^{i\frac{2\pi}{3}}$. Hence we get 3 field homomorphisms $\psi_{\sqrt[3]{2},\sqrt[3]{2}}, \psi_{\sqrt[3]{2},\omega\sqrt[3]{2}}, \psi_{\sqrt[3]{2},\omega^2\sqrt[3]{2}}\colon \mathbb{Q}(\sqrt[3]{2}) \to \overline{\mathbb{Q}}$, and so $\{\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\} = 3$.

The only homomorphism which gives an automorphism of $\mathbb{Q}(\sqrt[3]{2})$ is $\psi_{\sqrt[3]{2},\sqrt[3]{2}}$, since $\mathbb{Q}(\sqrt[3]{2}) \leq \mathbb{R}$ and $\psi_{\sqrt[3]{2},\omega^i\sqrt[3]{2}}(\sqrt[3]{2}) = \omega^i\sqrt[3]{2} \notin \mathbb{R}$ for $i = 1, 2$.

Hence we have $|G(\mathbb{Q}(\sqrt[3]{2}/\mathbb{Q})| = 1 < \{\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\} = 3$.