MATH 416, Modern Algebra II

Volodymyr Nekrashevych

2020, April 2

Extensions of isomorphisms

Let $F \subset E$ be a field extension. We know that if $\alpha, \beta \in E$ are conjugate in E, then there exists an isomorphism $\phi : F(\alpha) \longrightarrow F(\beta)$ fixing F. Can we extend ϕ to an automorphism of E?

Theorem 1 (Isomorphism Extension Theorem)

Let E be an algebraic extension of a field F. Let $\sigma : F \longrightarrow F'$ be an isomorphism of feilds. Let $\overline{F'}$ be an algebraic closure of F'. Then there exists an isomorphism $\tau : E \longrightarrow E'$, where E' is a subfield of $\overline{F'}$ such that $\tau(a) = \sigma(a)$ for all $a \in F$. In other words, σ can be extended to an isomorphism from E to a subfield of $\overline{F'}$.

The proof is straightforward, if one uses transfinite induction or Zorn's Lemma. The idea is to extend σ to $F(\alpha_1)$, then to $F(\alpha_1)(\alpha_2)$, etc..

Uniqueness of algebraic closures

Corollary 2

Let $\overline{F}_1$ and $\overline{F}_2$ be two algebraic closures of F. Then there exists an isomorphism $\alpha : \overline{F}_1 \longrightarrow \overline{F}_2$ fixing F.

Proof: An isomorphism $\tau : \overline{F}_1 \longrightarrow \tau(\overline{F}_1) \subset \overline{F}_2$ exists by the Isomorphism Extension Theorem. But by the same theorem, the inverse $\tau^{-1} : \tau(\overline{F}_1) \longrightarrow \overline{F}_1$ can be extended to an isomorphism from the whole $\overline{F}_2$ to a subfield of $\overline{F}_1$. But τ^{-1} is already onto, there is nowhere to extend anymore. So, the only possibility is that $\tau(\overline{F}_1)$ is the whole $\overline{F}_2$, i.e., that τ is onto.

Counting isomorphisms

Theorem 3

Let $F \subset E$ be a finite field extension. Let $\sigma : F \longrightarrow F'$ be an isomorphism of fields. Then the number of extensions of σ to an isomorphism $\tau : E \longrightarrow \tau(E) \subset \overline{F'}$ is finite and depends only on $F \subset E$.

Proof: Let us show at first that the number of extensions is finite. Since the extension $F \subset E$ is finite, we have $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for some algebraic elements $\alpha_i \in E$. If α_i is a root of a polynomial $f_i(x) \in F[x]$, then $\tau(\alpha_i)$ must be a root of $\sigma(f_i(x)) \in F'[x]$. But there are only a finite number of roots of $\sigma(f_i(x))$ in $\overline{F'}$, therefore there are only a finite number of possible values for $\tau(\alpha_i)$. But if we know all $\tau(\alpha_i)$, then we know τ. It follows that there is only a finite number of possibilities for τ.

The fact that the number of possible extensions does not depend on F', σ, or $\overline{F'}$ follows from the uniqueness of the algebraic closure and the extension theorem. Namely, if F'' is another field, and $\sigma' : F \longrightarrow F''$ is another isomorphism, then we can identify F' with F'' by the isomorphism $\sigma'' \circ \sigma^{-1} : F' \longrightarrow F''$. Then we can extend this isomorphism to an isomorphism of the algebraic closures. This will identify F' with F'', $\overline{F'}$ with $\overline{F''}$, so must be the same in both cases.

Denote by $\{E : F\}$ the number of possible extensions of an isomorphism $\sigma : F \longrightarrow F'$ to an isomorphism $\tau : E \longrightarrow \tau(E) \subset \overline{F'}$. We know that this number depends only on the extension $F \subset E$. We call it *index* of the extension. Note, that since it does not depend on σ and F', we may take $\sigma : F \longrightarrow F$ to be the identical isomorphism $\sigma(x) = x$. Then $\{E : F\}$ is defined as the number of isomorphisms $\tau : E \longrightarrow \tau(E) \subset \overline{F}$ such that $\tau(x) = x$ for all $x \in F$.

Theorem 4

If $F \subset E \subset K$, then $\{K : F\} = \{K : E\}\{E : F\}$.

Proof: There are $\{E : F\}$ ways to extend the identity isomorphism $F \longrightarrow F$ to an isomorphism $\sigma : E \longrightarrow \sigma(E) \subset \overline{F}$. **Each** of them can be extended to an isomorphism $\tau : K \longrightarrow \tau(K) \subset \overline{E} = \overline{F}$ $\{K : E\}$ times. This equality suggests that $\{E : F\}$ might be equal to $[E : F]$. It is often true, but not always.

An example.

Consider the field $\mathbb{Q}(\sqrt{2},\sqrt{3})$. Recall that we have automorphisms of $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2},\sqrt{3})$ given by

$$\sigma_{\sqrt{2}}(\sqrt{2}) = -\sqrt{2}, \qquad \sigma_{\sqrt{2}}(\sqrt{3}) = \sqrt{3},$$

$$\sigma_{\sqrt{3}}(\sqrt{2}) = \sqrt{2}, \qquad \sigma_{\sqrt{3}}(\sqrt{3}) = -\sqrt{3}.$$

and their composition

$$\sqrt{2} \mapsto -\sqrt{2}, \qquad \sqrt{3} \mapsto -\sqrt{3}.$$

An example.

The identity automorphism $\mathbb{Q} \longrightarrow \mathbb{Q}$ can be extended to $\mathbb{Q}(\sqrt{2})$ in two ways: as identity or as $\sigma_{\sqrt{2}}$, since any extension must map the root $\sqrt{2}$ of $x^2 - 2$ to a root of $x^2 - 2$. We have, therefore, $\{\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\} = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Similarly, an extension of the **identity** automorphism on $\mathbb{Q}(\sqrt{2})$ to an automorphism of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ must be either identity or $\sigma_{\sqrt{3}}$ for a similar reason. It follows that $\{\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})\} = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$. We have also seen that extensions of the identity automorphism of $\mathbb{Q}$ to $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is necessarily one of the automorphisms $Id, \sigma_{\sqrt{2}}, \sigma_{\sqrt{3}}, \sigma_{\sqrt{2}}\sigma_{\sqrt{3}}$, so $\{\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}\} = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

Splitting field

Let F be a field, and let $\overline{F}$ be its algebraic closure. Let $\{f_i\}$ be a collection of polynomials in $F[x]$. Then the field generated by F and **all** roots of the polynomials f_i is called the *splitting field* of the collection. A field $K \supset F$ is called a *splitting filed over* F if it is the splitting field of some collection of polynomials from $F[x]$.

Examples: $\mathbb{Q}(\sqrt{2})$ is the splitting field of x^2-2 over $\mathbb{Q}$. $\mathbb{Q}(\sqrt[3]{2})$ is **not** the splitting field of x^3-2, since it does not contain the other roots of x^3-2. The splitting field of x^3-2 is $\mathbb{Q}\left(\sqrt[3]{2}, -\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)$ and has degree 6 over $\mathbb{Q}$.

Theorem 5

A field E, where $F \subset E \subset \overline{F}$ is a splitting field over F if and only if every automorphism σ of $\overline{F}$ fixing F is an automorphism of E, i.e., satisfies $\sigma(E) = E$.

Proof: Suppose that E is the splitting field of a collection $\{f_i\}$ of polynomials in $F[x]$. Every automorphism $\sigma : \overline{F} \longrightarrow \overline{F}$ fixing every element of F will fix every f_i (since their coefficients are in F). Therefore, σ will just permute the roots of f_i. But E is generated by F and the roots, so $\sigma(E) = E$.

Theorem 6

A field E, where $F \subset E \subset \overline{F}$ is a splitting field over F if and only if every automorphism σ of $\overline{F}$ fixing F is an automorphism of E, i.e., satisfies $\sigma(E) = E$.

Proof: Suppose now that every automorphism of $\overline{F}$ fixing F leaves E invariant. Let $\alpha \in E$. Since $E \subset \overline{F}$, α is algebraic, hence is a root of a polynomial $f(x) \in F[x]$. Take the irreducible polynomial $g(x) \in F[x]$ for which α is a root. Let β be another root of $g(x)$. Then $\alpha \mapsto \beta$ can be extended to an isomorphism $\sigma : F(\alpha) \longrightarrow F(\beta)$ fixing F. By the extension theorem, σ can be extended to an automorphism τ of $\overline{F}$. Then, by our assumption, $\tau(E) = E$. But $\tau(\alpha) = \beta$. This shows that $\beta \in E$. We have proved that E contains **all** roots of $g(x)$. We can take then the set of all irreducible polynomials $g(x) \in F[x]$ with a root in E, then E will be equal to the set of all their roots, in particular it will be generated by them, so it is a splitting field.