Part X. Automorphisms and Galois Theory

Section X.48. Automorphisms of Fields

Note. In this section, we define an automorphism of a field as an isomorphism of the field with itself. We'll see that the set of all automorphisms of a field form a group (under function composition). We are particularly interested in automorphisms which fix subfields of the given field.

Definition 48.1. Let E be an algebraic extension of field F. Two elements $\alpha, \beta \in E$ are *conjugate* over F if $\mathrm{irr}(\alpha, F) = \mathrm{irr}(\beta, F)$; that is, if α and β are zeros of the same irreducible polynomial over F.

Note. The terminology "conjugate" comes from complex analysis. If z is a complex zero of $p(x) = a_{,}x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1 + a_0 \in \mathbb{R}[x]$, then so is $\overline{z}$:

$$p(z) = a_nz^n + a_{n-1}z^{n-1} + \cdots + a_2z^2 + a_1z + a_0 = 0$$

implies

$$\overline{a_nz^n + a_{n-1}z^{n-1} + \cdots + a_2z^2 + a_1z + a_0} = \overline{0}$$

or

$$a_n(\overline{z})^n + a_{n-1}(\overline{z})^{n-1} + \cdots + a_2(\overline{z})^2 + a_1\overline{z} + a_0 = \overline{0} = 0.$$

Theorem 48.3. The Conjugation Isomorphisms.

Let F be a field and let α and β be algebraic over F with $\deg(\alpha, F) = n$. The map $\psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$ defined by

$$\psi_{\alpha,\beta}(c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}) = c_0 + c_1\beta + c_2\beta^2 + \cdots + c_{n-1}\beta^{n-1}$$

for $c_i \in F$ is an isomorphism of $F(\alpha)$ onto $F(\beta)$ if and only if α and β are conjugate over F. (Notice that $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis of $F(\alpha)$ [and similarly for $\{1, \beta, \beta^2, \ldots, \beta^{n-1}\}$for $F(\beta)$] by Theorem 30.23.)

Note. The following result is the "cornerstone" of the proof of the Isomorphism Extension Theorem (Theorem 49.3) which implies the uniqueness of the algebraic closure of a field.

Corollary 48.5. Let α be algebraic over a field F. Every isomorphism ψ mapping $F(\alpha)$ onto a subfield of $\overline{F}$ such that $\psi(a) = a$ for $a \in F$, maps α onto a conjugate β of α over F. Conversely, for each conjugate β of α over F, there exists exactly one isomorphism $\psi_{\alpha,\beta}$ of $F(\alpha)$ onto a subfield of $\overline{F}$ mapping α onto β and mapping each $a \in F$ onto itself.

Note. The following is an algebraic proof (based on mappings) of the claim made above about complex conjugates.

Corollary 48.6. Let $f(x) \in \mathbb{R}[x]$. If $f(a+ib) = 0$ for $a+ib \in \mathbb{C}$, where $a, b \in \mathbb{R}$, then $f(a-ib) = 0$.

Example 48.7. Consider $\mathbb{Q}(\sqrt{2})$. $\sqrt{2}$ and $-\sqrt{2}$ are conjugate over $\mathbb{Q}$ and $\psi_{\sqrt{2},-\sqrt{2}} : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ defined by $\psi_{\sqrt{2},-\sqrt{2}}(a + b\sqrt{2}) = a - b\sqrt{2}$ is an isomorphism.

Note. In the proof of Corollary 48.6, $\psi_{i,-i}$ is an isomorphism of $\mathbb{C}$ with itself which fixes $\mathbb{R}$. In Example 48.7, $\psi_{\sqrt{2},-\sqrt{2}}$ is an isomorphism of $\mathbb{Q}(\sqrt{2})$ with itself which fixes $\mathbb{Q}$. We are interested in such isomorphisms and the subfields which they fix.

Definition 48.8. An isomorphism of a field onto itself is an *automorphism* of the field.

Definition 48.9. If σ is an isomorphism of a field E onto some field, then an element a of E is left *fixed* by σ if $\sigma(a) = a$ (and so a is also in the "some field"). A collection S of isomorphisms of E leaves a *subfield F of E fixed* if each $\alpha \in F$ is fixed by every $\sigma \in S$. If $\{\sigma\}$ leaves F fixed, then σ leaves *field F fixed.*

Note. The text comments that "…much of our preceding work is now being brought together. The next three theorems …form the foundation of everything that follows." (See page 418.)

Theorem 48.11. Let $\{\sigma_i \mid i \in I\}$ be a collection of automorphisms of a field E. Then the set $E_{\{\sigma_i\}}$ of all $a \in E$ fixed by every σ_i for $i \in I$ forms a subfield of E.

Definition 48.12. The field $E_{\{\sigma_i\}}$ of Theorem 48.11 is the *fixed field of* $\{\sigma_i \mid i \in I\}$. For a single automorphism σ, we call $E_{\{\sigma\}}$ the *fixed field of* σ.

Note. Since an automorphism of a field E to itself is a one to one and onto mapping, then it is a permutation of set E. We know that the compositions of permutations are again permutations. It turns out that the composition of automorphisms are automorphisms.

Theorem 48.14. The set of all automorphisms of a field E is a group under function composition.

Theorem 48.15. Let E be a field and F a subfield of E. Then the set of all automorphisms of E leaving F fixed, denoted $G(E/F)$, forms a subgroup of the group of all automorphisms of E. Furthermore, $F \leq E_{G(E/F)}$.

Note. The notation "$G(E/F)$" for the set of all automorphisms of E which fix F is a bit confusing—do not confuse this with some sort of quotient (though it is true that F is a subfield of E).

Definition 48.16. The group $G(E/F)$ of Theorem 48.15 is the group of *automorphisms of E leaving F fixed*, or the *group of E over F*.

Example 48.17. Consider $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Since $\sqrt{2}$ and $-\sqrt{2}$ are conjugates then $\psi_{\sqrt{2},-\sqrt{2}}$ is an automorphism. Similarly, $\psi_{\sqrt{3},-\sqrt{3}}$ is an automorphism. We can compose these to get $\psi_{\sqrt{2},-\sqrt{2}}\, \psi_{\sqrt{3},-\sqrt{3}}(a + b\sqrt{2} + c\sqrt{3}) = a - b\sqrt{2} - c\sqrt{3}$. Also, of course, the identity ι is an automorphism. Each of these fixes $\mathbb{Q}$, $\psi_{\sqrt{2},-\sqrt{2}}$ fixes $\mathbb{Q}(\sqrt{3})$, and $\psi_{\sqrt{3},-\sqrt{3}}$ fixes $\mathbb{Q}(\sqrt{2})$. A basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$ is $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ and an automorphism of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ which fixes $\mathbb{Q}$ is determined by its behavior on $\sqrt{2}$ and $\sqrt{3}$ (notice that these together determine the behavior on $\sqrt{6}$). So the 4 automorphisms above are the only such automorphisms. Denote $\sigma_1 = \psi_{\sqrt{2},-\sqrt{2}}$, $\sigma_2 = \psi_{\sqrt{3},-\sqrt{3}}$, and $\sigma_3 = \psi_{\sqrt{2},-\sqrt{2}}\, \psi_{\sqrt{3},-\sqrt{3}}$. Then the group $G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ has the table:

	ι	σ_1	σ_2	σ_3
ι	ι	σ_1	σ_2	σ_3
σ_1	σ_1	ι	σ_3	σ_2
σ_2	σ_2	σ_3	ι	σ_1
σ_3	σ_3	σ_2	σ_1	ι

In fact, $G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong V$ (the Klein 4-group). Notice that $|G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})| = 4$ and $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. The fact that both of these are the same is not a coincidence (as we'll see in Corollary 49.10).

Theorem 48.19. Let F be a finite field of characteristic p. Then the map $\sigma_p : F \to F$ defined by $\sigma_p(a) = a^p$ for all $a \in F$ is an automorphism of F, called the *Frobenius automorphism* of F. Also, $F_{\{\sigma_p\}} \cong \mathbb{Z}_p$.

Note. A common modern algebra joke is to refer to a field of characteristic p as satisfying "freshman exponentiation" due to the fact that $(a+b)^p = a^p + b^p$.

Revised: 3/30/2014