

## Section 48: Automorphisms of Fields

**Def:** Let  $E$  be an algebraic extension of a field  $F$ . Two elements  $\alpha, \beta \in E$  are *conjugate* over  $F$  if  $\text{irr}(\alpha, F) = \text{irr}(\beta, F)$ , that is, if  $\alpha$  and  $\beta$  are zeros of the same irreducible polynomial over  $F$ .

**Example:** Conjugate complex numbers  $a + bi$  and  $a - bi$  are roots of the same polynomial.

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

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

for  $c_i \in F$  is an isomorphism of  $F(\alpha)$  onto  $F(\beta)$  if and only if  $\alpha$  and  $\beta$  are conjugate over  $F$ .

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

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

**Def:** An isomorphism of a field onto itself is an *automorphism* of the field.

**Def:** If  $\sigma$  is an isomorphism of a field  $E$  onto some field, then an element  $a$  of  $E$  is *left fixed* by  $\sigma$  if  $\sigma(a) = a$ . A collection  $S$  of isomorphisms of  $E$  *leaves* a subfield  $F$  of  $E$  *fixed* if each  $a \in F$  is left fixed by every  $\sigma \in S$ . If  $\{\sigma\}$  leaves  $F$  fixed, then  $\sigma$  leaves  $F$  fixed.

**Thm.** Let  $\{\sigma_i | i \in I\}$  be a collection of automorphisms of a field  $E$ . Then the set  $E_{\{\sigma_i\}}$  of all  $a \in E$  left fixed by every  $\sigma_i$  for  $i \in I$  forms a subfield of  $E$ .

**Def:** The field  $E_{\{\sigma_i\}}$  is the *fixed field* of  $\{\sigma_i | i \in I\}$ . For a single automorphism  $\sigma$ , we shall refer to  $E_{\{\sigma\}}$  as the *fixed subfield* of  $\sigma$ .

**Thm.** The set of all automorphisms of a field  $E$  is a group under function composition.

**Note:** These automorphisms are basically permutation groups of the field.

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

**Def:** The group  $G(E/F)$  of the preceding theorem is the *group of automorphisms* of  $E$  leaving  $F$  fixed, or, the *group of  $E$  over  $F$* .

**Note:** The notation  $G(E/F)$  is a little misleading since it is not useful to think of this group as a quotient space. Instead think of it as referring to that  $E$  is an extension field of  $F$ .