of n equations in $n+1$ unknowns $x_1, \dots, x_{n+1}$ has a solution $\beta_1, \dots, \beta_{n+1}$ in K where not all the β_i, $i = 1, 2, \dots, n+1$ are 0. If all the elements of the solution $\beta_1, \dots, \beta_{n+1}$ were elements of F then the first equation (recall $\sigma_1 = 1$ is the identity automorphism) would contradict the linear independence over F of $\alpha_1, \alpha_2, \dots, \alpha_{n+1}$. Hence at least one β_i, $i = 1, 2, \dots, n+1$, is not an element of F.

Among all the nontrivial solutions $(\beta_1, \dots, \beta_{n+1})$ of the system (5) choose one with the minimal number r of nonzero β_i. By renumbering if necessary we may assume $\beta_1, \dots, \beta_r$ are nonzero. Dividing the equations by β_r we may also assume $\beta_r = 1$. We have already seen that at least one of $\beta_1, \dots, \beta_{r-1}, 1$ is not an element of F (which shows in particular that $r > 1$), say $\beta_1 \notin F$. Then our system of equations reads

$$\begin{gathered}\sigma_1(\alpha_1)\beta_1 + \cdots + \sigma_1(\alpha_{r-1})\beta_{r-1} + \sigma_1(\alpha_r) = 0 \\ \vdots \\ \sigma_n(\alpha_1)\beta_1 + \cdots + \sigma_n(\alpha_{r-1})\beta_{r-1} + \sigma_n(\alpha_r) = 0\end{gathered} \tag{14.6}$$

or more briefly

$$\sigma_i(\alpha_1)\beta_1 + \cdots + \sigma_i(\alpha_{r-1})\beta_{r-1} + \sigma_i(\alpha_r) = 0 \qquad i = 1, 2, \dots, n. \tag{14.7}$$

Since $\beta_1 \notin F$, there is an automorphism σ_{k_0} ($k_0 \in \{1, 2, \dots, n\}$) with $\sigma_{k_0}\beta_1 \neq \beta_1$. If we apply the automorphism σ_{k_0} to the equations in (6), we obtain the system of equations

$$\sigma_{k_0}\sigma_j(\alpha_1)\sigma_{k_0}(\beta_1) + \cdots + \sigma_{k_0}\sigma_j(\alpha_{r-1})\sigma_{k_0}(\beta_{r-1}) + \sigma_{k_0}\sigma_j(\alpha_r) = 0 \tag{14.8}$$

for $j = 1, 2, \dots, n$. But the elements

$$\sigma_{k_0}\sigma_1,\ \sigma_{k_0}\sigma_2,\ \dots,\ \sigma_{k_0}\sigma_n$$

are the same as the elements

$$\sigma_1,\ \sigma_2,\ \dots,\ \sigma_n$$

in some order since these elements form a *group*. In other words, if we define the index i by $\sigma_{k_0}\sigma_j = \sigma_i$ then i and j both run over the set $\{1, 2, \dots, n\}$. Hence the equations in (8) can be written

$$\sigma_i(\alpha_1)\sigma_{k_0}(\beta_1) + \cdots + \sigma_i(\alpha_{r-1})\sigma_{k_0}(\beta_{r-1}) + \sigma_i(\alpha_r) = 0. \tag{14.8$'$}$$

If we now subtract the equations in (8′) from those in (7) we obtain the system

$$\sigma_i(\alpha_1)[\beta_1 - \sigma_{k_0}(\beta_1)] + \cdots + \sigma_i(\alpha_{r-1})[\beta_{r-1} - \sigma_{k_0}(\beta_{r-1})] = 0$$

for $i = 1, 2, \dots, n$. But this is a solution to the system of equations (5) with

$$x_1 = \beta_1 - \sigma_{k_0}(\beta_1) \neq 0$$

(by the choice of k_0), hence is nontrivial and has fewer than r nonzero x_i. This is a contradiction and completes the proof.

Our first use of this result is to prove that the inequality of Proposition 5 holds for any finite extension K/F.

Corollary 10. Let K/F be any finite extension. Then

$$|\mathrm{Aut}(K/F)| \leq [K : F]$$

with equality if and only if F is the fixed field of $\mathrm{Aut}(K/F)$. Put another way, K/F is Galois if and only if F is the fixed field of $\mathrm{Aut}(K/F)$.

Proof: Let F_1 be the fixed field of $\mathrm{Aut}(K/F)$, so that

$$F \subseteq F_1 \subseteq K.$$

By Theorem 9, $[K : F_1] = |\mathrm{Aut}(K/F)|$. Hence $[K : F] = |\mathrm{Aut}(K/F)|[F_1 : F]$, which proves the corollary.

Corollary 11. Let G be a finite subgroup of automorphisms of a field K and let F be the fixed field. Then every automorphism of K fixing F is contained in G, i.e., $\mathrm{Aut}(K/F) = G$, so that K/F is Galois, with Galois group G.

Proof: By definition F is fixed by all the elements of G so we have $G \leq \mathrm{Aut}(K/F)$ (and the question is whether there are any automorphisms of K fixing F not in G i.e., whether this containment is proper). Hence $|G| \leq |\mathrm{Aut}(K/F)|$. By the theorem we have $|G| = [K : F]$ and by the previous corollary $|\mathrm{Aut}(K/F)| \leq [K : F]$. This gives

$$[K : F] = |G| \leq |\mathrm{Aut}(K/F)| \leq [K : F]$$

and it follows that we must have equalities throughout, proving the corollary.

Corollary 12. If $G_1 \neq G_2$ are distinct finite subgroups of automorphisms of a field K then their fixed fields are also distinct.

Proof: Suppose F_1 is the fixed field of G_1 and F_2 is the fixed field of G_2. If $F_1 = F_2$ then by definition F_1 is fixed by G_2. By the previous corollary any automorphism fixing F_1 is contained in G_1, hence $G_2 \leq G_1$. Similarly $G_1 \leq G_2$ and so $G_1 = G_2$.

By the corollaries above we see that taking the fixed fields for distinct finite subgroups of $\mathrm{Aut}(K)$ gives distinct subfields of K over which K is Galois. Further, the degrees of the extensions are given by the orders of the subgroups. We saw this explicitly for the fields $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $K = \mathbb{Q}(\sqrt[3]{2}, \rho)$ above. A portion of the Fundamental Theorem states that these are *all* the subfields of K.

The next result provides the converse of Proposition 5 and characterizes Galois extensions.

Theorem 13. The extension K/F is Galois if and only if K is the splitting field of some separable polynomial over F. Furthermore, if this is the case then every irreducible polynomial with coefficients in F which has a root in K is separable and has all its roots in K (so in particular K/F is a separable extension).

Proof: Proposition 5 proves that the splitting field of a separable polynomial is Galois.

We now show that if K/F is Galois then every irreducible polynomial $p(x)$ in $F[x]$ having a root in K splits completely in K. Set $G = \mathrm{Gal}(K/F)$. Let $\alpha \in K$ be a root of $p(x)$ and consider the elements

$$\alpha, \sigma_2(\alpha), \dots, \sigma_n(\alpha) \in K \tag{14.9}$$

where $\{1, \sigma_2, \dots, \sigma_n\}$ are the elements of $\mathrm{Gal}(K/F)$. Let

$$\alpha, \alpha_2, \alpha_3, \dots, \alpha_r$$

denote the *distinct* elements in (9). If $\tau \in G$ then since G is a group the elements $\{\tau, \tau\sigma_2, \dots, \tau\sigma_n\}$ are the same as the elements $\{1, \sigma_2, \dots, \sigma_n\}$ in some order. It follows that applying $\tau \in G$ to the elements in (9) simply permutes them, so in particular applying τ to $\alpha, \alpha_2, \alpha_3, \dots, \alpha_r$ also permutes these elements. The polynomial

$$f(x) = (x - \alpha)(x - \alpha_2) \cdots (x - \alpha_r)$$

therefore has coefficients which are fixed by all the elements of G since the elements of G simply permute the factors. Hence the coefficients lie in the fixed field of G, which by Corollary 10 is the field F. Hence $f(x) \in F[x]$.

Since $p(x)$ is irreducible and has α as a root, $p(x)$ is the minimal polynomial for α over F, hence divides any polynomial with coefficients in F having α as a root (this is Proposition 13.9). It follows that $p(x)$ divides $f(x)$ in $F[x]$ and since $f(x)$ obviously divides $p(x)$ in $K[x]$ by Proposition 2, we have

$$p(x) = f(x).$$

In particular, this shows that $p(x)$ is separable and that all its roots lie in K (in fact they are among the elements $\alpha, \sigma_2\alpha, \dots, \sigma_n\alpha$), proving the last statement of the theorem.

To complete the proof, suppose K/F is Galois and let $\omega_1, \omega_2, \dots, \omega_n$ be a basis for K/F. Let $p_i(x)$ be the minimal polynomial for ω_i over F, $i = 1, 2, \dots, n$. Then by what we have just proved, $p_i(x)$ is separable and has all its roots in K. Let $g(x)$ be the polynomial obtained by removing any multiple factors in the product $p_1(x) \cdots p_n(x)$ (the "squarefree part"). Then the splitting field of the two polynomials is the same and this field is K (all the roots lie in K, so K contains the splitting field, but $\omega_1, \omega_2, \dots, \omega_n$ are among the roots, so the splitting field contains K). Hence K is the splitting field of the separable polynomial $g(x)$.

Definition. Let K/F be a Galois extension. If $\alpha \in K$ the elements $\sigma\alpha$ for σ in $\mathrm{Gal}(K/F)$ are called the *conjugates* (or *Galois conjugates*) of α over F. If E is a subfield of K containing F, the field $\sigma(E)$ is called the *conjugate field* of E over F.

The proof of the theorem shows that in a Galois extension K/F the other roots of the minimal polynomial over F of any element $\alpha \in K$ are precisely the distinct conjugates of α under the Galois group of K/F.

The second statement in this theorem also shows that K is not Galois over F if we can find even one irreducible polynomial over F having a root in K but not having *all* its roots in K. This justifies in a very strong sense the intuition from earlier examples that Galois extensions are extensions with "enough" distinct roots of irreducible polynomials (namely, if it contains one root then it contains all the roots).

Finally, notice that we now have 4 characterizations of Galois extensions K/F:

(1) splitting fields of separable polynomials over F

(2) fields where F is precisely the set of elements fixed by $\text{Aut}(K/F)$ (in general, the fixed field may be larger than F)

(3) fields with $[K : F] = |\text{Aut}(K/F)|$ (the original definition)

(4) finite, normal and separable extensions.

Theorem 14. *(Fundamental Theorem of Galois Theory)* Let K/F be a Galois extension and set $G = \text{Gal}(K/F)$. Then there is a bijection

$$\left\{\begin{array}{cc} & K \\ \text{subfields } E & | \\ \text{of } K & E \\ \text{containing } F & | \\ & F \end{array}\right\} \longleftrightarrow \left\{\begin{array}{cc} & 1 \\ \text{subgroups } H & | \\ \text{of } G & H \\ & | \\ & G \end{array}\right\}$$

given by the correspondences

$$\begin{array}{ccc} E & \longrightarrow & \left\{\begin{array}{c} \text{the elements of } G \\ \text{fixing } E \end{array}\right\} \\ \left\{\begin{array}{c} \text{the fixed field} \\ \text{of } H \end{array}\right\} & \longleftarrow & H \end{array}$$

which are inverse to each other. Under this correspondence,

(1) (inclusion reversing) If E_1, E_2 correspond to H_1, H_2, respectively, then $E_1 \subseteq E_2$ if and only if $H_2 \leq H_1$

(2) $[K : E] = |H|$ and $[E : F] = |G : H|$, the index of H in G:

$$\begin{array}{ll} K & \\ |\ \} & |H| \\ E & \\ |\ \} & |G : H| \\ F & \end{array}$$

(3) K/E is always Galois, with Galois group $\text{Gal}(K/E) = H$:

$$\begin{array}{ll} K & \\ | & H \\ E & \end{array}$$

(4) E is Galois over F if and only if H is a normal subgroup in G. If this is the case, then the Galois group is isomorphic to the quotient group

$$\text{Gal}(E/F) \cong G/H.$$

More generally, even if H is not necessarily normal in G, the isomorphisms of E (into a fixed algebraic closure of F containing K) which fix F are in one to one correspondence with the cosets $\{\sigma H\}$ of H in G.

(5) If E_1, E_2 correspond to H_1, H_2, respectively, then the intersection $E_1 \cap E_2$ corresponds to the group $\langle H_1, H_2 \rangle$ generated by H_1 and H_2 and the composite field E_1E_2 corresponds to the intersection $H_1 \cap H_2$. Hence the lattice of subfields