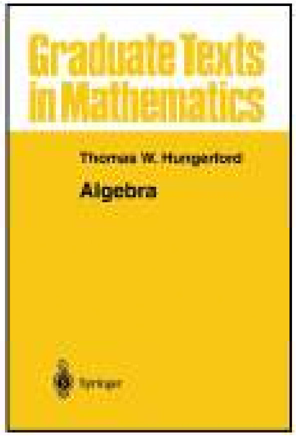
# Modern Algebra

**Chapter V. Fields and Galois Theory**

V.2. The Fundamental Theorem (of Galois Theory)—Proofs of Theorems








## Theorem V.2.2

**Theorem V.2.2.** Let $F$ be an extension field of $K$ and $K[x]$. If $u \in F$ is a root of $f$ and $\sigma \in \text{Aut}_K(F)$, then $\sigma(u) \in F$ is also a root of $f$.

**Proof.** Let $f = \sum_{i=0}^n k_i x^i$. Since $\sigma$ fixes $K$, $\sigma(0) = 0$ and so $f(u) = 0$ implies

$$0 = \sigma(0) = \sigma(f(u)) = \sigma\left(\sum_{i=0}^n k_i x^i\right)$$

$$= \sum_{i=0}^n \sigma(k_i)\sigma(u^i) = \sum_{i=0}^n k_i(\sigma(u))^i = f(\sigma(u)).$$

$\square$





## Lemma V.2.6

**Lemma V.2.6.** Let $F$ be an extension field of $K$ with intermediate fields $L$ and $M$ (say $K \subset L \subset M \subset F$). Let $H$ and $J$ be subgroups of $G = \text{Aut}_K(F)$. Then:

(i) $F' = 1$ (the identity group) and $K' = G$;
(i′) $1' = F$;
(ii) $L \subset M$ implies $M' < L'$;
(ii′) $H < J$ implies $J' \subset H'$;
(iii) $L \subset L''$ and $H < H''$ (where $L'' = (L')'$ and $H'' = (H')'$);
(iv) $L' = L'''$ and $H' = H'''$.

**Proof. (i)** Now $F' = \text{Aut}_F(F)$ is the group of automorphisms of $F$ which fix $F$ and hence must consist only of the identity permutation and so $F'$ is the "identity group." Next, $K' = \text{Aut}_K(F) = G$, since we denote $\text{Aut}_K(F)$ as $G$.

**(i′)** $1'$ is the fixed field of the identity group. $F$ is the "universal field" and the identity group fixes all of $F$; i.e., $1' = F$.





## Lemma V.2.6 (ii)

**Lemma V.2.6.** Let $F$ be an extension field of $K$ with intermediate fields $L$ and $M$ (say $K \subset L \subset M \subset F$). Let $H$ and $J$ be subgroups of $G = \text{Aut}_K(F)$. Then:

(ii) $L \subset M$ implies $M' < L'$;
(ii′) $H < J$ implies $J' \subset H'$.

**Proof. (ii)** Suppose the intermediate fields $L, M$ satisfy $L \subset M$. An element of $M' = \text{Aut}_M(F)$ fixes $M$ and with $L \subset M$ such an element must also fix $L$ and so the element is in $L' = \text{Aut}_L(F)$. So $M' < L'$.

**(ii′)** Suppose subgroups $H, J$ of $G = \text{Aut}_K(F)$ satisfy $H < J$. Now an element of $J'$ (the fixed field of $J$) is fixed by every element of $J$ and, since $H < J$, also fixed by every element of $H$. So an element of $J'$ is also an element of $H'$. That is, $J' \subset H'$.

# Lemma V.2.6 (iii)

**Lemma V.2.6.** Let $F$ be an extension field of $K$ with intermediate fields $L$ and $M$ (say $K \subset L \subset M \subset F$). Let $H$ and $J$ be subgroups of $G = \mathrm{Aut}_K(F)$. Then:

(iii) $L \subset L''$ and $H < H''$ (where $L'' = (L')'$ and $H'' = (H')'$).

**Proof. (iii)** Let $L$ be an intermediate field. Then $L' = \mathrm{Aut}_L(F)$ is a group, and $L''$ is the fixed field of $L'$. Now any element of $L$ is fixed by $L' = \mathrm{Aut}_L(F)$. Also, $L''$ includes everything in $F$ fixed by the elements of $L' = \mathrm{Aut}_L(F)$. So $L''$ includes all of $L$ (and possibly more); $L \subset L''$.

Let $H$ by a subgroup of $G = \mathrm{Aut}_K(F)$. Then $H'$ is the fixed field of $H$. Now $(H')' = H''$ is the group of permutations of $F$ which fix $H'$. So every element of $H$ fixes all of $H'$ and such an element is therefore also in $H''$. So $H < H''$.





# Lemma V.2.6 (iv)

**Lemma V.2.6.** Let $F$ be an extension field of $K$ with intermediate fields $L$ and $M$ (say $K \subset L \subset M \subset F$). Let $H$ and $J$ be subgroups of $G = \mathrm{Aut}_K(F)$. Then:

(iv) $L' = L'''$ and $H' = H'''$.

**Proof. (iv)** Let $L$ be an intermediate field. By (iii), $L \subset L''$ and so by (ii), $L''' < L'$. Now $L'$ is a subgroup of $G = \mathrm{Aut}_K(F)$ and so by (iii) (with $H$ replaced with $L'$) we have $L' < L'''$, and so $L' = L'''$.

Let $H$ be a subgroup of $G = \mathrm{Aut}_K(F)$. By (iii), $H < H''$ and so by (ii′), $H''' \subset H'$. Now $H'$ is an intermediate field so by (iii) (with $L$ replaced with $H'$) we have $H' \subset H'''$, and so $H' = H'''$. □





# Lemma V.2.8

**Lemma V.2.8.** Let $F$ be an extension field of $K$ and $L, M$ intermediate fields with $L \subset M$. If $M : L$ is finite, then $[L' : M'] \le [M : L]$. In particular, if $[F : K]$ is finite, then $|\mathrm{Aut}_K(F)| \le [F : K]$.

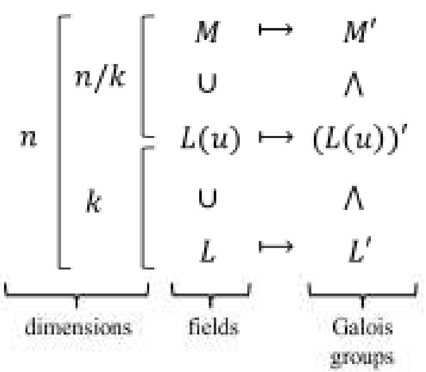
**Proof.** (Notice that $[M : L]$ and $[F : K]$ are dimensions of vector spaces; $[L' : M']$, the index of $L'$ over $M'$, is the number of cosets of $L$ in $M$.) Since $[M : L]$ is finite, we give a proof based on induction. Let $n = [M : L]$. If $n = 1$ then $M + L$ and so $M' = L'$ and $[L' : M'] = 1$, so the result holds. Let $n > 1$ and suppose the theorem holds for all $i < n$. Since $n > 1$, there is some $u \in M$ with $u \notin L$. Since $[M : L]$ is finite, then $u$ is algebraic over $L$ by Theorem V.1.11. Let $f \in L[x]$ be the irreducible monic polynomial of $u$, say of degree $k > 1$. By Theorem V.1.6(iii), $[L(u) : L] = k$. By Theorem V.1.1, $[M : L] = [M : L(u)][L(u) : L]$ and so $[M : L(u)] = n/k$.





# Lemma V.2.8 (continued 1)

**Proof (continued).** Schematically:




We now consider two cases.
Case 1. If $k < n$ then $1 < n/k < n$; and
Case 2. If $k = n$.

## Lemma V.2.8 (continued 2)

**Lemma V.2.8.** Let $F$ be an extension field of $K$ and $L, M$ intermediate fields with $L \subset M$. If $M : L$ is finite, then $[L' : M'] \leq [M : L]$. In particular, if $[F : K]$ is finite, then $|\mathrm{Aut}_K(F)| \leq [F : K]$.

**Proof (continued).**
Case 1. If $k < n$ then $1 < n/k < n$. By the induction hypothesis, since $i = n/k < n$, we have that $L \subset L(u)$ implies $[L' : (L(u))'] \leq [L(u) : L] = k$, and that $L(U) \subset M$ implies $[(L(u))' : M'] \leq [M : L(u)] = n/k$. Hence

$$\begin{aligned} [L' : M'] &= [L' : (L(u))'][(L(u))' : M'] \text{ by Theorem V.1.1} \\ &\leq k(n/k) = n = [M : L] \end{aligned}$$

and the theorem holds in this case.





## Lemma V.2.8 (continued 3)

**Lemma V.2.8.** Let $F$ be an extension field of $K$ and $L, M$ intermediate fields with $L \subset M$. If $M : L$ is finite, then $[L' : M'] \leq [M : L]$. In particular, if $[F : K]$ is finite, then $|\mathrm{Aut}_K(F)| \leq [F : K]$.

**Proof (continued).**
Case 2. On the other hand, if $k = n$ then by Theorem V.1.1, $[M : L] = [M : L(u)][L(u) : L]$ and so $[M" L(u)] = 1$ (as above). So $M = L(u)$. In the final part of the proof, we will construct an injective map from the set $S$ of all left costs of $M'$ in $L'$ (of which there are $[L' : M']$ such cosets) to the set $T$ of all distinct roots in $F$ of the polynomial $f \in L[x]$ (of which there are at most $k \leq n$ such roots by Theorem III.6.7). So we have $|S| = [L' : M']$ and $|T| \leq n$, the existence of the injective map from $S$ to $T$ gives that $|S| \leq |T|$ and it will then follow that $[L' : M'] = |S| \leq |T| \leq n = [M : L]$, establishing the theorem in this second case.





## Lemma V.2.8 (continued 4)

**Proof (continued).** Now for the construction of the injective map from $S$ to $T$. Let $\tau \in L'$ and $\tau M'$ a left coset of $M'$ in $L'$. If $\sigma \in M' = \mathrm{Aut}_M(F)$, then since $u \in M$ (by choice, above) we have that $\sigma(u) = u$ and so $\tau\sigma(u) = \tau(u)$; so every element of the coset $\tau M'$ (this is a group element which acts on elements of $F$, $u$ in particular) has the same effect on $u$ and maps $u \mapsto \tau(u)$ (that is, there is independence of element $\sigma \in M'$). Since $\tau \in L' = \mathrm{Aut}_L(F)$ (because $\tau M'$ is a coset in $L'$) and $u$ is a root of $f \in L[x]$, then $\tau(u)$ is also a root of $f$ by Theorem V.2.2. This implies that the map $S \mapsto T$ given by $\tau M' \mapsto \tau(u)$ is well-defined (HMMMM; that is, the mapping actually produces an element of $T$, the set of roots of $f$). If $\tau(u) = \tau_0(u)$ for $\tau, \tau_0 \in L'$ then $\tau_0^{-1}\tau(u) = u$ ($L'$ is a group of permutations, so inverses exist) and hence $\tau_0\tau$ fixes $u$. Since $\tau, \tau_0 \in L' = \mathrm{Aut}_L(F)$ then certainly $\tau, \tau_0$, and $\tau_0^{-1}$ fixes $L$, so $\tau_o^{-1}\tau$ fixes $L(u) = M$ elementwise (recall that a basis for $L(u) = M$ over $L$ is $\{1, u, u^2, \ldots, u^{k-1}\}$ by Theorem V.1.6(iv)) and $\tau_0\tau \in M'$.





## Lemma V.2.8 (continued 5)

**Lemma V.2.8.** Let $F$ be an extension field of $K$ and $L, M$ intermediate fields with $L \subset M$. If $M : L$ is finite, then $[L' : M'] \leq [M : L]$. In particular, if $[F : K]$ is finite, then $|\mathrm{Aut}_K(F)| \leq [F : K]$.

**Proof (continued).** Consequently by Corollary V.4.3(iii), $\tau_0 M' = \tau M'$ and so the map $S \to T$ is one to one (injective) and this completes the second case of the induction. Therefore $[L' : M'] \leq [M : L]$.

For the "in particular" part of the proof, notice that $\mathrm{Aut}_K(F) \cong \mathrm{Aut}_K(F)/1$ (where "1" is the trivial "identity group"). So $|\mathrm{Aut}_K(F)| = [\mathrm{Aut}_K(F) : 1]$. Also, in the prime notation $K' = \mathrm{Aut}_K(F)$ and $F' = \mathrm{Aut}_F(F) = 1$, so $|\mathrm{Aut}_K(F)| = [\mathrm{Aut}_K(F) : 1] = [K' : F'] \leq [F : K]$ with $L = K$ and $M = F$, from the above result. □

## Lemma V.2.9

**Lemma V.2.9.** Let $F$ be an extension field of $K$ and let $H, J$ be subgroups of the Galois group $\mathrm{Aut}_K(F)$ with $H < J$. If $[J : H]$ is finite, then $[H' : J'] \le [J : H]$.

**Proof.** (Notice that $[H' : J']$ is the dimension of field $H'$ as a vector space over field $J'$; the index $[J : H]$ is the number of cosets of $H$ in $J$.) Let the number of cosets of $H$ in $J$ by $[J : H] = n$. ASSUME $[H' : J'] > n$. Then a basis of $H'$ over $J'$ has more than $n$ elements (as basis is a linearly independent spanning set; see page 181) and so there exist $u_1, u_2, \ldots, u_{n+1} \in H'$ that are linearly independent over $J'$. Let $\{\tau_1, \tau_2, \ldots, \tau_n\}$ be a complete set of representatives of the $n$ left cosets of $H$ in $J$. That is, $J = \tau_1 H \cup \tau_2 H \cup \cdots \cup \tau_n H$ (since cosets of a subgroup partition the group; Corollary I.4.3(i),(ii)) and $\tau_i^{-1}\tau_j \in H$ if and only if $i = j$ by Corollary I.4.3(iii). Consider the system of $n$ homogeneous linear equations in $n+1$ unknowns with coefficients $\tau_i(u_j)$ in field $F$:





## Lemma V.2.9 (continued 1)

$$\begin{aligned}
\tau_1(u_1)x_1 + \tau_1(u_2)x_2 + \tau_1(u_3)x_3 + \cdots + \tau_1(u_{n+1})x_{n+1} &= 0\\
\tau_2(u_1)x_1 + \tau_2(u_2)x_2 + \tau_2(u_3)x_3 + \cdots + \tau_2(u_{n+1})x_{n+1} &= 0\\
\tau_3(u_1)x_1 + \tau_3(u_2)x_2 + \tau_3(u_3)x_3 + \cdots + \tau_3(u_{n+1})x_{n+1} &= 0\\
&\vdots \qquad (1)\\
\tau_n(u_1)x_1 + \tau_n(u_2)x_2 + \tau_n(u_3)x_3 + \cdots + \tau_n(u_{n+1})x_{n+1} &= 0.
\end{aligned}$$

Such a system ($n$ homogeneous equations in $n+1$ unknowns) has a nontrivial solution as will be shown in Exercise VII.2.4(d) (see also Lemma 5.1.1 of *Real Analysis with an Introduction to Wavelets*, Don Hong, Jianzhong Wang, and Robert Gardner, Academic Press/Elsevier Press, 2005). Among all such nontrivial solutions choose one, say $x_1 = a_1, x_2 = a_2, \ldots, x_{n+1} = a_{n+1}$ with a minimal number of nonzero $a_i$. By reindexing if necessary we may assume that $x_1 = a_1$, $x_2 = a_2$, …, $x_r = a_r$ and $x_{r+1} = x_{r+1} = \cdots x_{n+1} = 0$ where $a_r \ne 0$. Since each multiple of a solution is also a solution then we may also assume $a_1 = 1_F$.





## Lemma V.2.9 (continued 2)

**Proof (continued).** In the conclusion of the proof below, we will show that the hypothesis that $u_1, u_2, \ldots, u_{n+1} \in H'$ are linearly independent over $J'$ implies that there exists $\sigma \in J$ such that $x_1 = \sigma a_1, x_2 = \sigma a_2, \ldots, x_r = \sigma a_r$ and $x_{r+1} = x_{r+2} = \cdots = x_{n+1} = 0$ is also a nontrivial solution to the system of equations (1) and $\sigma a_2 = a_2$. Since the difference of two solutions is also a solution (since the system (1) is linear and homogeneous) then

$$\begin{aligned} x_1 = a_1 - \sigma a_1, x_2 = a_2 - \sigma a_2, \ldots, x_t = a_r - \sigma a_r, \text{ and}\\ x_{r+1} = x_{r+2} = \cdots = x_{n+1} = 0 \qquad (*)\end{aligned}$$

is also a solution of the system of equations (1). But since $a_1 - \sigma a_1 = 1_F - 1_F = 0$ ($\sigma \in J < \mathrm{Aut}_K(F)$ implies that $\sigma$ fixes the elements of $K$, including the multiplicative identity) and $a_2 \ne \sigma a_2$ then $x_1 = 0$, $x_2 = a_2 - \sigma a_2 \ne 0$, $x_3 = a_3 - \sigma a_3$, …, $x_r = a_r - \sigma a_r$ and $x_{r+1} = x_{r+2} = \cdots = x_{n+1} = 0$ is a nontrivial solution of the system of equations (1) (since $x_2 \ne 0$) with at most $r-1$ nonzero entries, a CONTRADICTION to the minimality of $r$ of nonzero terms is a nontrivial solution to the system of equations (1).





## Lemma V.2.9 (continued 3)

**Proof (continued).** This contradiction shows that the assumption $[H' : J'] > n$ is false, and hence $[H' : J'] \le n$.

To complete the proof, we must find $\sigma \in J$ with the desired properties. Now $\{\tau_1, \tau_2, \ldots, \tau_n\}$ is a set of representatives of the cosets of $H$, then exactly one of the $\tau_j$, say $\tau_1$, is in $H$ itself. Since $H' = \mathrm{Aut}_H(F)$, then $\tau_1$ fixes the elements of $H'$ and so $\tau_1(u_i) = u_i \in H'$ for all $i = 1, 2, \ldots, n+1$. So the first equation in the system of equations (1) becomes $u_1 a_1 + a_2 a_2 + \cdots + u_r a_r = 0$. Now each $a_i$ is nonzero for $1 \le i \le r$ and the $u_i$ are linearly independent over $J'$. So it must be that some $a_i$ is not in $J'$, say $a_2 \notin J'$. Since $J'$ is the fixed field of $J$, then there is some $\sigma \in J$ such that $\sigma a_2 \ne a_2$ (that is, $\sigma$ does not fix $a_2$).

## Lemma V.2.9 (continued 4)

**Proof (continued).** Next, consider a second system of equations (which we will show to be equivalent to [that is, have the identical solutions as] the first system of equations (1)):

$$\begin{aligned}
\sigma\tau_1(u_1)x_1 + \sigma\tau_1(u_2)x_2 + \sigma\tau_1(u_3)x_3 + \cdots + \sigma\tau_1(u_{n+1})x_{n+1} &= 0\\
\sigma\tau_2(u_1)x_1 + \sigma\tau_2(u_2)x_2 + \sigma\tau_2(u_3)x_3 + \cdots + \sigma\tau_2(u_{n+1})x_{n+1} &= 0\\
\sigma\tau_3(u_1)x_1 + \sigma\tau_3(u_2)x_2 + \sigma\tau_3(u_3)x_3 + \cdots + \sigma\tau_3(u_{n+1})x_{n+1} &= 0\\
&\vdots \qquad (2)\\
\sigma\tau_n(u_1)x_1 + \sigma\tau_n(u_2)x_2 + \sigma\tau_n(u_3)x_3 + \cdots + \sigma\tau_n(u_{n+1})x_{n+1} &= 0.
\end{aligned}$$

Since $\sigma \in J < \mathrm{Aut}_K(F)$ then $\sigma(0) = 0$ and if we apply $\sigma$ to each of the equations in the first system (1), then we get the second system (2). Since $x_1 = 1_1, x_2 = a_2, \ldots, x_r = a_r$ and $x_{r+1} = x_{r+2} = \cdots x_{n+1} = 0$ is a solution of system (1), then $x_1 = \sigma a_1, x_2 = \sigma a_2, \ldots, x_r = \sigma a_r$ and $x_{r+1} = x_{r+2} = \cdots = x_{n+1} = 0$ is a solution of system (2).





## Lemma V.2.9 (continued 5)

**Proof (continued).** We claim that system (2), except for the order of the equations, is identical with system (1) (so that $x_1 = \sigma a_1, x_2 = \sigma a_2, \ldots, x_r = \sigma a_r$ and $x_{r+1} = x_{r+1} = \cdots = x_{n+1} = 0$ is a solution of system (1); this will show that $\sigma$ satisfies the conditions mentioned above). We make two claims:

**(i)** For any $\sigma \in J$, the set $\{\sigma\tau_1, \sigma\tau_2, \ldots, \sigma\tau_n\} \subset J$ is a complete set of coset representatives of the cosets of $H$ in $J$.

Sub-Proof. First, since each $\tau_i \in J$ and $\sigma \in J$, then $\sigma\tau_i \in J$. Now $\sigma\tau_i H = \sigma\tau_i H$ if and only if $(\sigma\tau_i)^{-1}(\sigma\tau_j) \in H$ by Theorem I.4.3(iii); that is, $\tau_i^{-1}\sigma^{-1}\sigma\tau_j = \tau_i^{-1}\tau_j \in H$. Again by Theorem I.4.3(iii), $\tau_i^{-1}\tau_j \in H$ if only if $\tau_i H = \tau_j H$. So $\sigma\tau_i H = \sigma\tau_j H$ if and only if $\tau_i H = \tau_j H$. Since $\{\tau_1, \tau_2, \ldots, \tau_n\}$ is a complete set of representatives of the left cosets of $H$ in $J$, then so is $\{\sigma\tau_1, \sigma\tau_2, \ldots, \sigma\tau_n\}$. *Sub-Q.E.D.*





## Lemma V.2.9 (continued 6)

**Proof (continued).**
**(ii)** If $\zeta$ and $\theta$ are both elements in the same coset of $H$ in $J$, then (since $u_i \in H'$) $\zeta(u_i) = \theta(u_i)$ for $i = 1, 2, \ldots n+1$.

Sub-Proof. Let $\zeta, \theta \in aH$. Then $\zeta = ah_1$ and $\theta = ah_2$ for some $h_1, h_2 \in H$. Since $H'$ is the fixed field of $H$ and each $u_i \in H'$, then $\zeta(u_i) = (ah_1)(u_i) = ah_1(u_i) = au_i$ and $\theta(u_i) = (ah_2)(u_i) = ah_2(u_i) = au_i$. So $\zeta(u_i) = \theta(u_i)$ for $i = 1, 2, \ldots, n+1$. *Sub-Q.E.D.*

It now follows from claim (i) that there is some reordering $i_1, i_2, \ldots, i_{n+1}$ of $1, 2, \ldots, n+1$ so that for each $k = 1, 2, \ldots, n+1$, $\sigma\tau_k$ and $\tau_{i_k}$ are in the same coset of $H$ in $J$. By (ii), the $k$th equation of system (2) (with coefficients $\sigma\tau_k(u_i)$) is identical with the $i_k$th equation of system (1) (with coefficients $\tau_{i_k}(u_i)$). So we have, in particular, that the solution $x_1 = a_1, x_2 = a_2, \ldots, x_r = a_r$ and $x_{r+1} = x_{r+2} = \cdots x_{n+1} = 0$ of system (2) is also a solution of system (1). We can now pick up at step $(*)$ and complete the proof by contradiction. □





## Lemma V.2.10

**Lemma V.2.10.** Let $F$ be an extension field of $K, L$ and $M$ intermediate fields with $L \subset M$, and $H, J$ subgroups of the Galois group $\mathrm{Aut}_K(F)$ with $H < J$.

(i) If $L$ is closed and $[M : L]$ finite, then $M$ is closed and $[L' : M'] = [M : L]$;

(ii) if $H$ is closed and $[J : H]$ finite, then $J$ is closed and $[H' : J'] = [J : H]$;

(iii) if $F$ is a finite dimensional Galois extension of $K$, then all intermediate fields and and all subgroups of the Galois group are closed and $\mathrm{Aut}_K(F)$ has order $[F : K]$.

**Proof. (i)** By Lemma V.2.6(iii), $M \subset M''$. Since $L \subset M \subset M''$, by Theorem V.1.2 we have $[M'' : L] = [M'' : M][M : L]$ and so $[M : L] \le [M'' : L]$. Now $[L' : M'] \le [M : L]$ By Lemma V.2.8 and $[M'' : L''] \le [L' : M']$ by Lemma V.2.9.

# Lemma V.2.10 (continued 1)

**Lemma V.2.10.** Let $F$ be an extension field of $K$, $L$ and $M$ intermediate fields with $L \subset M$, and $H, J$ subgroups of the Galois group $\mathrm{Aut}_K(F)$ with $H < J$.

(i) If $L$ is closed and $[M : L]$ finite, then $M$ is closed and $[L' : M'] = [M : L]$.

**Proof (continued). (i)** Combining these inequalities gives

$$\begin{aligned} [M : L] \leq [M'' : L] &= [M'' : L''] \text{ since } L'' = L \\ &\leq [L' : M'] \leq [M : L]. \end{aligned}$$

Therefore the inequalities reduce to equalities and $[L' : M'] = [M : L]$. Also, $[M'' : L] = [M : L]$ so the dimension of $M''$ over $L$ is the same as the dimension of $M$ over $L$. Also, by Lemma V.2.6(iii), $M \subset M''$ and so $M = M''$ and $M$ is closed.





# Lemma V.2.10 (continued 2)

**Lemma V.2.10.** Let $F$ be an extension field of $K$, $L$ and $M$ intermediate fields with $L \subset M$, and $H, J$ subgroups of the Galois group $\mathrm{Aut}_K(F)$ with $H < J$.

(ii) if $H$ is closed and $[J : H]$ finite, then $J$ is closed and $[H' : J'] = [J : H]$.

**Proof. (ii)** By Lemma V.2.6(iii), $J < J''$. Since $H < J < J''$ then the number of cosets of $H$ in $J$, $[J : H]$ is less than or equal to the number of cosets of $H$ in $J''$, $[J'' : H]$; that is, $[J : H] \leq [J'' : H]$. So

$$\begin{aligned} [J : H] &\leq [J'' : H] = [J'' : H''] \text{ since } H = H'' \\ &\leq [H' : J'] \text{ by Lemma V.2.8} \\ &\leq [J : H] \text{ by Lemma V.2.9.} \end{aligned}$$

So we have $[H' : J'] = [J : H]$ as claimed. Also, $[J'' : H] = [J : H]$ and so the number of cosets of $H$ in $J$ equals the number of cosets of $H$ in $J''$. Therefore $|J| = |J''|$; also $J \subset J''$ so we must have $J = J''$.





# Lemma V.2.10 (continued 3)

**Lemma V.2.10.** Let $F$ be an extension field of $K$, $L$ and $M$ intermediate fields with $L \subset M$, and $H, J$ subgroups of the Galois group $\mathrm{Aut}_K(F)$ with $H < J$.

(iii) if $F$ is a finite dimensional Galois extension of $K$, then all intermediate fields and and all subgroups of the Galois group are closed and $\mathrm{Aut}_K(F)$ has order $[F : K]$.

**Proof. (iii)** If $E$ is an intermediate field, $K \subset E \subset F$, then $[F : K] = [F : E][E : K]$ by Theorem V.1.2 and since $[F : K]$ is hypothesized to be finite, then $[E : K]$ is finite. Since $F$ is Galois over $K$ then $K$ is closed (see the note on page 246 right after the definition of closed). So every intermediate field is closed. Now (i) (with $L = K$ and $M = E$) implies that $E$ is closed and $[K' : E'] = [E : K]$. In particular, if $E = F$ then $|\mathrm{Aut}_K(F)| = [\mathrm{Aut}_K(E) : 1] = [K' : F'] = [F : K]$ is finite. Therefore, every subgroup $J$ of $\mathrm{Aut}_K(F)$ is finite. Now $1' = F$ and $1'' = F' = \mathrm{Aut}_F(F) = 1$, so 1 is closed. Now by (ii), $J$ is closed and so every subgroup of $\mathrm{Aut}_K(F)$ is closed. □





# Lemma V.2.11

**Lemma V.2.11.** Let $F$ be an extension field of $K$.

(i) If $E$ is a stable intermediate field of the extension, then $E' = \mathrm{Aut}_E(F)$ is a normal subgroup of the Galois group $\mathrm{Aut}_K(F)$;

(ii) if $H$ is a normal subgroup of $\mathrm{Aut}_K(F)$, then the fixed field $H'$ of $H$ is a stable intermediate field of the extension.

**Proof. (i)** If $u \in E$ and $\sigma \in \mathrm{Aut}_K(F)$ then $\sigma(u) \in E$ by the stability of $E$. Hence for $\tau \in E' = \mathrm{Aut}_E(F)$ we have $\tau\sigma(u) = \sigma(u)$. Therefore, for any $\sigma \in \mathrm{Aut}_K(F)$, $\tau \in E' = \mathrm{Aut}_E(F)$, and $u \in E$ we have $\sigma^{-1}\tau\sigma(u) = \sigma^{-1}\sigma(u) = u$. Consequently $\sigma^{-1}\tau\sigma \in E' = \mathrm{Aut}_E(F)$ and hence $E'$ is a normal subgroup of $\mathrm{Aut}_K(F)$ by Theorem I.5.1(iv).

## Lemma V.2.11 (continued)

**Lemma V.2.11.** Let $F$ be an extension field of $K$.

(ii) if $H$ is a normal subgroup of $\mathrm{Aut}_K(F)$, then the fixed field $H'$ of $H$ is a stable intermediate field of the extension.

**Proof. (ii)** If $\sigma \in \mathrm{Aut}_K(F)$ and $\tau \in H$, then $\sigma^{-1}\tau\sigma \in H$ since $H$ is hypothesized to be a normal subgroup of $\mathrm{Aut}_K(F)$ (by Theorem I.5.1(iv)). Therefore, for any $u \in H'$, $\sigma^{-1}\tau\sigma(u) = u$ (since $H'$ denotes the fixed field of $H$), which implies that $\tau\sigma(u) = \sigma(u)$ for all $\tau \in H$. This $\sigma(u) \in H'$ for any $u \in H'$ and for any $\sigma \in \mathrm{Aut}_K(F)$. This means that $H'$ is stable relative to $K$ and $F$. □





## Lemma V.2.12

**Lemma V.2.12.** If $F$ is a Galois extension field of $K$ and $E$ is a stable intermediate field of the extension, then $E$ is Galois over $K$.

**Proof.** If $u \in E \setminus K$ then there exists $\sigma \in \mathrm{Aut}_K(F)$ such that $\sigma(u) \neq u$ since $F$ is Galois over $K$ (meaning $K = (\mathrm{Aut}_K(F))' = K'$, so $u \notin K$ implies that $u$ is not fixed by some $\sigma \in \mathrm{Aut}_K(F)$). Since $E$ is stable then $\sigma$ maps $E$ into itself; that is, $\sigma|_E \in \mathrm{Aut}_K(E)$. So for every $u \in E \setminus K$ there is an element of $\mathrm{Aut}_K(F)$ which does not fix $u$. So the fixed field of $\mathrm{Aut}_K(F)$ is just $K$; $K = (\mathrm{Aut}_K(F))' = K'$. Therefore, $E$ is a Galois extension of $K$. □





## Lemma V.2.13

**Lemma V.2.13.** If $F$ is an extension field of $K$ and $E$ is an intermediate field of the extension such that $E$ is algebraic and Galois over $K$, then $E$ is stable (relative to $F$ and $K$).

**Proof.** If $u \in E$, let $f \in K[x]$ be the irreducible monic polynomial of $u$ and let $u_1, u_2, \ldots, u_r$ be the distinct roots of $f$ that lie in $E$, where $u = u_1$. Then $r \leq n = \deg(f)$ by Theorem III.6.7. If $\tau \in \mathrm{Aut}_K(E)$, then by Theorem V.2.2 we have that $\tau$ permutes roots of $f$; that is, $\tau$ permutes the $u_i$. Therefore the coefficients of the monic polynomial $g(x) = (x - u_1)(x - u_2)\cdots(x - u_r) \in E[x]$ are fixed by every $\tau \in \mathrm{Aut}_K(E)$, since the coefficients are "symmetric" functions of the $u_i$. Since $E$ is Galois over $K$, then $K = (\mathrm{Aut}_K(E))' = K'$ and so the coefficients are all in $K$ and $g \in K[x]$. Now $u = u_1$ is a root of $g$ and hence irreducible $f$ divides $g$ by Theorem V.1.6(ii). Since $g$ is monic and $\deg(g) \leq \deg(f)$ (because $f$ divides $g$) we must have that $f = g$ (or else, $g$ is a divisor of $f$ since $f$ is irreducible). Consequently, all the roots of $f$ are distinct and lie in $E$ (as in the case for $g$).





## Lemma V.2.13 (continued)

**Lemma V.2.13.** If $F$ is an extension field of $K$ and $E$ is an intermediate field of the extension such that $E$ is algebraic and Galois over $K$, then $E$ is stable (relative to $F$ and $K$).

**Proof (continued).** Now if $\sigma \in \mathrm{Aut}_K(F)$, then $\sigma(u)$ is a root of $f$ by Theorem V.2.2, whence $\sigma(u) \in E$. Since $u$ was an arbitrary element of $E$, we have shown that $\sigma \in \mathrm{Aut}_K(F)$ maps $E$ into itself; that is, $E$ is stable relative to $K$ and $F$. □

## Lemma V.2.14

**Lemma V.2.14.** Let $F$ be an extension field of $K$ and let $E$ be a stable intermediate field of the extension. Then the quotient group $\text{Aut}_K(F)/\text{Aut}_E(F)$ is isomorphic to the group of all automorphisms in $\text{Aut}_K(E)$ that are extendible to $F$.

**Proof.** Intermediate field $E$ is stable, so (by the definition of stable) every automorphism $\sigma \in \text{Aut}_K(F)$ maps $E$ into itself, and hence the mapping $\sigma \mapsto \sigma|_E$ defines a group homomorphism from $\text{Aut}_K(F)$ to $\text{Aut}_K(E)$. The image of this homomorphism is "clearly" the subgroup of $\text{Aut}_K(E)$ of all automorphisms that are extendible to $F$ (of course, the extension of $\sigma|_E$ is $\sigma$ itself). Now the kernel of the homomorphism is all elements of $\text{Aut}_K(F)$ which are the identity on $E$; so the kernel is $\text{Aut}_E(F)$. By the First Isomorphism Theorem (Theorem I.5.7) the homomorphism induces an isomorphism between $\text{Aut}_K(F)$ modulo the kernel and the image of the homomorphism. So $\text{Aut}_K(F)/\text{Aut}_E(F)$ is isomorphic to the group of all automorphisms in $\text{Aut}_K(E)$ that are extendible to $F$. □





## Theorem V.2.5. The Fundamental Theorem of Galois Theory

**Theorem V.2.5. The Fundamental Theorem of Galois Theory.** If $F$ is a finite dimensional Galois extension of $K$, then there is a one to one correspondence between the set of all intermediate fields of the extension and the set of all subgroups of the Galois group $\text{Aut}_K(F)$ (given by $E \mapsto E' = \text{Aut}_E(F)$) such that:

(i) the relative dimension of two intermediate fields is equal to the relative index of the corresponding subgroups; in particular, $\text{Aut}_K(F)$ has order $[F : K]$;

(ii) $F$ is Galois over every intermediate field $E$, but $E$ is Galois over $K$ if and only if the corresponding subgroup $E' = \text{Aut}_E(F)$ is normal in $G = \text{Aut}_K(F)$; in the case $G/E'$ is (isomorphic to) the Galois group $\text{Aut}_K(E)$ of $E$ over $K$.





## Theorem V.2.5. The Fundamental Theorem of Galois Theory (i)

**Proof.** Theorem V.2.7 shows that there is a one to one correspondence between the *closed* intermediate fields and *closed* subgroups of the Galois group. By Lemma V.2.10(iii) all intermediate fields are closed and all subgroups of $\text{Aut}_K(F)$ are closed. So the one to one correspondence between closed intermediate fields and closed subgroups is in fact a one to one correspondence between all intermediate fields and all subgroups. This correspondence is given by mapping each group $H$ to its fixed field $H'$ and by mapping each field $M$ to its Galois group $M' = \text{Aut}_M(F)$.

**(i)** For intermediate fields $L$ and $M$ (with $L \subset M$) we have by Lemma V.2.10(i) that the relative dimension of the fields $[M : L]$ equals the relative index of the corresponding subgroups $[L' : M']$; that is, $[M : L] = [L' : M']$. The "in particular" part follows from Lemma V.2.10(iii); that is, $|\text{Aut}_K(F)| = [F : K]$.





## Theorem V.2.5. The Fundamental Theorem of Galois Theory (ii)

(ii) $F$ is Galois over every intermediate field $E$, but $E$ is Galois over $K$ if and only if the corresponding subgroup $E' = \text{Aut}_E(F)$ is normal in $G = \text{Aut}_K(F)$; in the case $G/E'$ is (isomorphic to) the Galois group $\text{Aut}_K(E)$ of $E$ over $K$.

**Proof.** $F$ is Galois over $E$ since $E$ is closed (see the comment after the definition of closed), so $F$ is Galois over every intermediate field. $E$ is finite dimensional over $K$ (since $F$ is; see Theorem V.1.2) and hence, by Theorem V.1.11, $F$ is algebraic over $K$. Consequently if $E$ is Galois over $K$ then $E$ satisfies the hypotheses of Lemma V.2.13 and so $E$ is stable relative to $F$ and $K$. By Lemma V.2.11(i), $E' = \text{Aut}_E(F)$ is normal in $G = \text{Aut}_K(F)$ (this is the first part of the claim of (ii)). Conversely, if $E' = \text{Aut}_E(F)$ is normal in $G = \text{Aut}_K(F)$, then by Lemma V.2.11(ii), $E''$ is a stable intermediate field.

# Theorem V.2.5. The Fundamental Theorem of Galois Theory (ii) (continued)

**Proof (continued).** We establish that all intermediate fields are closed, so $E = E''$ and $E$ is stable. Therefore by Lemma V.2.12, $E$ is Galois over $K$ (this is the second part of the claim of (ii), the converse of the first part).

Now for the "in the case" part. Let $E' = \mathrm{Aut}_E(F)$ be normal in $G = \mathrm{Aut}_K(F)$, or equivalently, let $E$ be Galois over $K$. We have seen at the beginning of the proof that all intermediate fields and subgroups are closed, so $E$ and $E'$ are closed. Since $F$ is Galois over $K$ then $G' = (\mathrm{Aut}_K(F))' = K$. Now the elements of $G/E'$ are cosets of $E'$, so $|G/E'| = [G : E']$. Hence

$$\begin{aligned} |G/E'| &= [G : E'] \\ &= [E'' : G'] \text{ by Lemma V.2.10(ii)} \\ &= [E : K] \text{ since } E = E'' \text{ and } K = G'. \end{aligned}$$





# Theorem V.2.5. The Fundamental Theorem of Galois Theory (ii)

(ii) $F$ is Galois over every intermediate field $E$, but $E$ is Galois over $K$ if and only if the corresponding subgroup $E' = \mathrm{Aut}_E(F)$ is normal in $G = \mathrm{Aut}_K(F)$; in the case $G/E'$ is (isomorphic to) the Galois group $\mathrm{Aut}_K(E)$ of $E$ over $K$.

**Proof.** We saw above that $E''$ is stable and $E = E''$, so $E$ is stable. By Lemma V.2.14, $G/E' = \mathrm{Aut}_K(F)/\mathrm{Aut}_E(F)$ is isomorphic to a subgroup of $\mathrm{Aut}_K(E)$. Since we have just shown that $|G/E'| = [E : K]$, then this subgroup of $\mathrm{Aut}_K(E)$ is of order $[E : K]$. Since $E$ is Galois over $K$ (by hypothesis, here) then part (i) shows that $|\mathrm{Aut}_K(E)| = [E : K]$. Since $G/E'$ is isomorphic to a subgroup of $\mathrm{Aut}_K(E)$ of order $[E : K]$ and $\mathrm{Aut}_K(E)$ itself is of order $[E : K]$, then $G/E' = \mathrm{Aut}_K(F)/\mathrm{Aut}_E(F) \cong \mathrm{Aut}_K(E)$. □





# Theorem V.2.15. Artin

**Theorem V.2.15. (Artin.)**
Let $F$ be a field, $G$ a group of automorphisms of $F$, and $K$ the fixed field of $G$ in $F$. Then $F$ is Galois over $K$. If $G$ is finite, then $F$ is a finite dimensional Galois extension of $K$ with Galois group $G$.

**Proof.** Since $K$ is the fixed field of $G$ in $F$, then for each $u \in F \setminus K$ there must be a $\sigma \in G$ such that $\sigma(u) \neq u$. By the definition of $G$ as a group of automorphisms of $F$ which fixes $K$ elementwise, we have $G < \mathrm{Aut}_K(F)$ (since $\mathrm{Aut}_K(F)$ fixes $K$ elementwise, as well as possibly other things). So each such $\sigma \in G$ is also in $\mathrm{Aut}_K(F)$ and therefore the fixed field of $\mathrm{Aut}_K(F)$ is $K$ itself. Whence (by definition) $F$ is Galois over $K$, establishing the first claim.





# Theorem V.2.15. Artin (continued)

**Proof (continued).** If $G$ is finite, then by Lemma V.2.9 (with $H = 1$ and $J = G$, which gives $|G| = [G : 1]$ is finite) we have

$$\begin{aligned} [F : K] &= [1' : G'] \text{ since } 1' = F \text{ and } G' = K \\ &\qquad \text{(fixed fields of 1 and } G\text{, respectively)} \\ &\leq [G : 1] \text{ by Lemma V.2.9} \\ &= |G|. \end{aligned}$$

Consequently, $F$ is finite dimensional over $K$. So $F$ is a finite dimensional Galois extension of $K$, and so by Lemma V.2.10(iii) all intermediate groups are closed and so $G = G''$. Since the fixed field of $G$ is $G' = K$ (and hence $G'' = K'$) we have that the Galois group of $F$ over $K$ is

$$\begin{aligned} \mathrm{Aut}_K(F) &= K' \text{ by the prime notation} \\ &= G'' \text{ as just observed} \\ &= G \text{ since } G \text{ is closed.} \end{aligned}$$

□