This paragraph gives an exposition of Galois theory. Given any field extension \( E/K \), we associate intermediate fields of \( E/K \) with subgroups of a group, called the Galois group of the extension. Many questions about the intermediate field structure of the extension can be thus reduced to related questions about the subgroup structure of the Galois group. Our exposition closely follows the treatment of I. Kaplansky.

If \( E/K \) is a field extension, then \( E \) is a field and also a \( K \)-vector space. It will be very fruitful to study both the field and the vector space structure of \( E \) at the same time. For this reason, we consider mappings which preserve both of these structures.

Let \( E \) be a field. Let us recall that a field automorphism \( \varphi \) of \( E \) is a one-to-one ring homomorphism from \( E \) onto \( E \). Equivalently, a field automorphism of \( E \) is an automorphism of the additive group \( (E,+) \) which is also a ring isomorphism of \( E \). Clearly the identity mapping on \( E \) is a field automorphism of \( E \), so the set of all field automorphisms of \( E \) is not empty. Besides, if \( \varphi \) and \( \psi \) are any two field automorphisms of \( E \), then \( \varphi \psi \) and \( \varphi^{-1} \) are automorphisms of the additive group \( (E,+) \) which are ring isomorphisms from \( E \) onto \( E \) as well (Lemma 30.16); thus \( \varphi \psi \) and \( \varphi^{-1} \) are field automorphisms of \( E \). Therefore the set of all field automorphisms of \( E \) is a subgroup of the group of all automorphisms of \( E \). The group of all field automorphisms of \( E \) will be denoted by \( \text{Aut}(E) \). Thus we use the same notation for the group of additive group automorphisms of \( E \) and the group of field automorphisms of \( E \). This is not likely to cause confusion. Anyhow, \( \text{Aut}(E) \) will play a minor role in the sequel.

\( \text{Aut}(E) \) is the collection of mappings from \( E \) onto \( E \) that preserve the field structure of \( E \). From these field automorphisms, we select the mappings that preserve the vector space structure of \( E \). We introduce some terminology.
54.1 Definition: Let $E/K$ and $F/K$ be field extensions. A mapping $\varphi: E \to F$ is called a $K$-homomorphism if $\varphi$ is both a field homomorphism and a $K$-vector space homomorphism. A $K$-homomorphism $\varphi: E \to F$ is called a $K$-isomorphism if $\varphi$ is one-to-one and onto. A $K$-isomorphism from $E$ onto $E$ is called a $K$-automorphism of $E$. The set of all $K$-automorphisms of $E$ will be denoted by $\text{Aut}_K E$ or by $G(E/K)$.

If $\varphi: E \to F$ is a $K$-homomorphism, then $(1_E)\varphi = 1_F$ (see the remarks following Definition 48.9) since $\varphi$ is a field homomorphism and, for any $k \in K$, there holds $k\varphi = (k1_E)\varphi = k(1_E)\varphi = k1_F = k$ since $\varphi$ is a $K$-linear transformation. Thus $k\varphi = k$ for all $k \in K$. Conversely, if $\varphi: E \to F$ is a $K$-homomorphism such that $k\varphi = k$ for all $k \in K$, then $(ke)\varphi = k\varphi e\varphi = k(e\varphi)$ for all $k \in K$ and $e \in E$, and thus $\varphi$ is a $K$-linear transformation, too. Therefore a field homomorphism $\varphi: E \to F$ is a $K$-homomorphism if and only if $\varphi$ fixes every element of $K$.

54.2 Lemma: Let $E/K$ be a field extension and let $\text{Aut}_K E$ be the set of all $K$-automorphisms of $E$ over $K$. Then $\text{Aut}_K E$ is a group.

Proof: We have $1_E \in \text{Aut}_K E \subseteq \text{Aut}(E)$ and $\text{Aut}(E)$ is a group. Since the composition two vector space isomorphisms and also the inverse of a vector space isomorphism are vector space isomorphisms (Theorem 41.10), $\text{Aut}_K E$ is closed under composition and forming of inverses. Thus $\text{Aut}_K E$ is a subgroup of $\text{Aut}(E)$. $\square$

54.3 Definition: Let $E/K$ be a field extension. The group $\text{Aut}_K E = G(E/K)$ is called the Galois group of $E$ over $K$.

54.4 Examples: (a) Let $E$ be any field and let $P$ be the prime subfield of $E$. Any field automorphism $\varphi$ of $E$ fixes $1 \in E$. This implies that $\varphi$ fixes each element in $P$. Therefore any field automorphism of $E$ is a $P$-automorphism of $E$ and $\text{Aut}(E) = \text{Aut}_P(E)$:
(b) The familiar complex conjugation mapping \((a + bi \rightarrow a - bi, \text{ where } a, b \in \mathbb{R})\) is an \(\mathbb{R}\)-automorphism of \(\mathbb{C}\).

(c) The mapping \(\phi: \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})\) that maps \(a + b\sqrt{2}\) to \(a - b\sqrt{2}\) (where \(a, b \in \mathbb{Q}\)) is a \(\mathbb{Q}\)-automorphism of \(\mathbb{Q}(\sqrt{2})\).

(d) Let \(K\) be a field and \(x\) an indeterminate over \(K\). Then \(K(x)\) is an extension field of \(K\). If \(a \in K\), then \(ax\) is transcendental over \(K\) and, by Theorem 49.10, the mapping \(\sigma_a: K(x) \rightarrow K(x)\) given by \(f(x)/g(x) \rightarrow f(ax)/g(ax)\) is a field automorphism of \(K(x)\). It is easy to see that \(\sigma_a\) is in fact a \(K\)-automorphism of \(K(x)\). Likewise, for any \(b \in K\), the mapping \(\tau_b: K(x) \rightarrow K(x)\) given by \(f(x)/g(x) \rightarrow f(x + b)/g(x + b)\) is a \(K\)-automorphism of \(K(x)\). As \(x\sigma_a \tau_b = (ax + b)\neq ax + b = (a + b)\sigma_a = x\tau_b \sigma_a\) unless \(a \neq 1\) or \(b \neq 0\), we see that \(Aut_K K(x)\) is a nonabelian group.

We find \(Aut_K K(x)\). In the following, \(y\) and \(z\) are two additional distinct indeterminates over \(K\).

Let \(u\) be an arbitrary element in \(K(x)\), say \(u = p(x)/q(x)\), where \(p(x)\) and \(q(x)\) are relatively prime polynomials in \(K[x]\) and \(q(x) \neq 0\). We claim that \(u\) is transcendental over \(K\) and \(K(x)\) is finite dimensional (hence algebraic) over \(K(u)\).

We prove the first claim, viz. that \(u\) is transcendental over \(K\). If \(u\) were algebraic over \(K\), then \(u\) would have a minimal polynomial
\[H(y) = y^k + c_{k-1}y^{k-1} + \cdots + c_1y + c_0 \in K[y]\]
over \(K\). Then, from \(H(u) = 0\), we would get
\[\begin{align*}
(p(x)/q(x))^k + c_{k-1}(p(x)/q(x))^{k-1} + \cdots + c_1(p(x)/q(x)) + c_0 &= 0, \\
p(x)^k + c_{k-1}p(x)^{k-1}q(x) + \cdots + c_1p(x)q(x)^{k-1} + c_0q(x)^k &= 0,
\end{align*}\]
\(q(x)p(x)^k\) in \(K[x]\) and \((p(x),q(x)) \approx 1\), \(q(x)\) is a unit in \(K[x]\), so \(q(x) \notin K\),
\[u = p(x)/q(x) \notin K[x],\]
\(H(u) = u^k + c_{k-1}u^{k-1} + \cdots + c_1u + c_0\) is a polynomial of degree \(k(deg p(x))\), contrary to \(H(u) = 0\). Thus \(u\) is transcendental over \(K\).

Secondly, we prove that \(|K(x):K(u)|\) is finite. Now \(u = p(x)/q(x)\). Let us put \(p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0\), \(q(x) = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0\), with \(a_n \neq 0 \neq b_m\). We note that \(x\) is a root of the polynomial
\[F(y) = (b_mu)y^m + (b_{m-1}u)y^{m-1} + \cdots + (b_1u)y + b_0,\]
\[-a_ny^n - a_{n-1}y^{n-1} - \cdots - a_1y - a_0\]
\[= 0,\]
\[\text{implying that } x \notin K(u).\]
in \( K(u)[y] \). Thus \( x \) is algebraic over \( K(u) \). We see moreover that \( \text{deg } F(y) = \text{max } (m,n) = \text{max } (\text{deg } p(x), \text{deg } q(x)) \), because \( b_m u - a_n \neq 0 \) as \( u \notin K \). We will show that \( F(y) \) is irreducible over \( K(u) \). This will imply \( cF(y) \) is the minimal polynomial of \( x \) over \( K(u) \), where \( 1/c \) is the leading coefficient of \( F(y) \), and so \( |K(x):K(u)| = \text{deg } cF(y) = \text{deg } F(y) = \text{max } (\text{deg } p(x), \text{deg } q(x)) \).

Now the irreducibility of \( F(y) \) over \( K(u) \). Since \( u \) is transcendental over \( K \), the substitution homomorphism \( z \rightarrow u \) is in fact a field isomorphism from \( K(z) \) onto \( K(u) \subseteq K(x) \) (Theorem 49.10). So \( K(u) \cong K(z) \) and Theorem 33.8 gives \( K(u)[y] \cong K(z)[y] \). Then \( F(y) \in K(u)[y] \) is irreducible in \( K(u)[y] \) if and only if its image \( F(z) \in K(z)[y] \) is irreducible in \( K(z)[y] \). From Theorem 34.5(3) and Lemma 34.11, we conclude \( F(z) \) is irreducible in \( K(z)[y] \) if and only if \( F(z) = q(y)z - p(y) \) is irreducible in \( K[z][y] = K[y][z] \). But \( F(z) = q(y)z - p(y) \) is certainly irreducible in \( K[y][z] \) since \( q(y)z - p(y) \) is of degree one in \( K[y][z] \) and its coefficients \( q(y) \), \(-p(y)\) are relatively prime in \( K[y] \) (for \( p(x) \) and \( q(x) \) are relatively prime polynomials in \( K[x] \) and \( q(x) \neq 0 \).

Thus we get \( |K(x):K(u)| = \text{max } (\text{deg } p(x), \text{deg } q(x)) \) for any \( u = p(x)/q(x) \) in \( K(x) \setminus K \), where \( p(x) \) and \( q(x) \) are relatively prime polynomials in \( K[x] \) and \( q(x) \neq 0 \).

Now let \( \varphi \in \text{Aut}_K K(x) \) and \( x\varphi = u \). Write \( u = p(x)/q(x) \) as above. Since
\[
K(u) = K(x\varphi) = \{ f(x\varphi)/g(x\varphi) : f, g \in K[x], g \neq 0 \}
= \{ f(x)\varphi/g(x)\varphi : f, g \in K[x], g \neq 0 \}
= \{ (f(x)/g(x))\varphi : f, g \in K[x], g \neq 0 \}
= (K(x))\varphi = K(x) \neq K,
\]
we have \( u \notin K(x) \setminus K \) and
\[
1 = |K(x):K(u)| = |K(x):K(u)| = \text{max } (\text{deg } p(x), \text{deg } q(x))
\]
yields \( p(x) = ax + b, q(x) = cx + d \) for some \( a, b, c, d \in K \). Here \( ad - bc \neq 0 \) for \( ad - bc = 0 \) implies the contradiction \( u = p(x)/q(x) = (ax + b)/(cx + d) \in K \).

Thus every automorphism in \( \text{Aut}_K K(x) \) is a substitution homomorphism that sends \( x \) to \( (ax + b)/(cx + d) \) for some \( a, b, c, d \in K \) satisfying \( ad - bc \neq 0 \). Conversely, if \( \varphi \) is a substitution homomorphism of this type, with \( x\varphi = (ax + b)/(cx + d), a, b, c, d \in K \), \( ad - bc \neq 0 \), then \( (ax + b)/(cx + d) = u \) is not in \( K \), so \( u \) is transcendental over \( K \) and \( \varphi \) is a field homomorphism from \( K(x) \) onto \( K(u) \). Since \( ad - bc \neq 0 \), both of \( a \) and \( c \) cannot be 0, so \( |K(x):K(u)| = \text{max } (\text{deg } ax + b, \text{deg } cx + d) = 1 \) and \( K(u) = K(x) \). Hence \( \varphi \) is a field homomorphism from \( K(x) \) onto \( K(x) \). As \( \varphi \) fixes all elements in \( K \), we
infer that \( \varphi \) is in \( \text{Aut}_K K(x) \). Therefore \( \text{Aut}_K K(x) \) consists exactly of the substitution homomorphisms \( x \to (ax + b)/(cx + d) \), where \( a, b, c, d \in K \) and \( ad - bc \neq 0 \).

The next lemma is a generalization of the familiar fact that the complex conjugate of any root of a polynomial with real coefficients is also a root of the same polynomial. In the terminology of §26, if \( E/K \) is a field extension, \( \text{Aut}_K E \) acts on the set of distinct roots of a polynomial \( f(x) \) over \( K \).

**54.5 Lemma:** Let \( E/K \) be a field extension and \( f(x) \in K[x] \). If \( u \in E \) is a root of \( f(x) \), then, for any \( \varphi \in \text{Aut}_K E \), the element \( u\varphi \) of \( E \) is also a root of \( f(x) \).

**Proof:** If \( f(x) = \sum_{i=0}^{m} a_i x^i \), then \( f(u) = 0 \) implies \( 0 = 0\varphi = (f(u))\varphi = (\sum_{i=0}^{m} a_i u^i)\varphi = \sum_{i=0}^{m} (a_i \varphi)(u^i \varphi) = \sum_{i=0}^{m} a_i (u \varphi)^i = f(u \varphi) \). Thus \( u \varphi \) is a root of \( f(x) \). \( \square \)

Let \( E/K \) be a finite dimensional extension and assume that \( \{a_1, a_2, \ldots, a_m\} \) is a \( K \)-basis of \( E \). Then any \( K \)-automorphism of \( E \) is completely determined by its effect on the basis elements, for if \( \varphi \) and \( \psi \) are \( K \)-automorphisms of \( E \) and \( a_i \varphi = a_i \psi \) for \( i = 1, 2, \ldots, m \), then, for any \( a \in E \), which we write in the form \( \sum_{i=0}^{m} k_i a_i \), we have \( a \varphi = (\sum_{i=0}^{m} k_i a_i) \varphi = \sum_{i=0}^{m} k_i a_i \varphi \)

\[
= \sum_{i=0}^{m} k_i (a_i \varphi) = \sum_{i=0}^{m} k_i (a_i \psi) = \sum_{i=0}^{m} k_i \psi a_i \psi = (\sum_{i=0}^{m} k_i a_i) \psi = a \psi.
\]

For this reason, we will describe the \( K \)-automorphisms of \( E \) by describing the images of the basis elements. Thus the conjugation mapping will be denoted by \( i \to -i \), the mapping of Example 54.4(c) by \( \sqrt{2} \to -\sqrt{2} \), etc.

In particular, if \( E/K \) is a simple extension and \( a \) is a primitive element, then \( \{1, a, a^2, \ldots, a^{n-1}\} \) is a \( K \)-basis of \( E = K(a) \), where \( n \) is the degree of the minimal polynomial of \( a \) over \( K \) (Theorem 50.7). Let \( \varphi \in \text{Aut}_K E \). Since \( a^i \varphi \)
= (aφ)i for any i = 0,1,2, . . . , n − 1, the mapping φ is completely determined by its effect on a. Now aφ is a root in K(a) of the minimal polynomial of a over K. Thus |AutkE| ≤ r, where r is the number of distinct roots in K(a) of the minimal polynomial of a over K. We proved the following lemma.

54.6 Lemma: Let K be a field. If a is algebraic over K with the minimal polynomial f over K, and if r is the number of distinct roots of f in K(a) then |AutK(a)| ≤ r ≤ deg f = |K(a):K|.

54.7 Examples: (a) Let 3\sqrt{2} be the positive real cube root of 2. Thus \( \mathbb{Q}(3\sqrt{2}) \subseteq \mathbb{R} \). We find Aut\( \mathbb{Q}(3\sqrt{2}) \). If φ ∈ Aut\( \mathbb{Q}(3\sqrt{2}) \), then 3\sqrt{2}φ ∈ \mathbb{R} is a root of the minimal polynomial \( x^3 - 2 \) of \( 3\sqrt{2} \) over \( \mathbb{Q} \). Since the roots of \( x^3 - 2 \) other than \( 3\sqrt{2} \) are complex, 3\sqrt{2}φ must be \( 3\sqrt{2} \). Thus φ must be the identity mapping on \( \mathbb{Q}(3\sqrt{2}) \) and Aut\( \mathbb{Q}(3\sqrt{2}) = 1 \).

(b) C = \mathbb{R}(i) and the minimal polynomial of i over \mathbb{R} is \( x^2 + 1 \), which has two roots in C. Thus |Aut\( \mathbb{R}(i) \)| ≤ 2. Since the identity mapping and conjugation mapping are \( \mathbb{R} \)-automorphisms of C, |Aut\( \mathbb{R}(i) \)| = 2 and we get Aut\( \mathbb{R}(i) \) ≅ C2. Likewise Aut\( \mathbb{Q}(\sqrt{2}) \) ≅ C2.

(c) We find Aut\( \mathbb{Q}(\sqrt{2}, \sqrt{3}) \). We have \( \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) \). Here \{1, \sqrt{2}\} is a \( \mathbb{Q} \)-basis of \( \mathbb{Q}(\sqrt{2}) \) and \{1, \sqrt{3}\} is a \( \mathbb{Q}(\sqrt{2}) \)-basis of \( \mathbb{Q}(\sqrt{2})(\sqrt{3}) \) (because \( x^2 - 3 \) is irreducible over \( \mathbb{Q}(\sqrt{2}) \)), hence, by Theorem 48.13, \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\} is a \( \mathbb{Q} \)-basis of \( \mathbb{Q}(\sqrt{2}, \sqrt{3}) \). Now any φ ∈ Aut\( \mathbb{Q}(\sqrt{2}, \sqrt{3}) \) maps \( \sqrt{2} \) to \( \sqrt{2} \) or to \( -\sqrt{2} \) and \( \sqrt{3} \) to \( \sqrt{3} \) or to \( -\sqrt{3} \) and there are four possibilities for φ:

\begin{align*}
(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6})\phi_1 &= a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \\
(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6})\phi_2 &= a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6} \\
(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6})\phi_3 &= a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6} \\
(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6})\phi_4 &= a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}
\end{align*}

(\( a,b,c,d \in \mathbb{Q} \)). It is easy to see that \( \phi_1, \phi_2, \phi_3, \phi_4 \) are indeed \( \mathbb{Q} \)-automorphisms of \( \mathbb{Q}(\sqrt{2}, \sqrt{3}) \) so that Aut\( \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{\phi_1, \phi_2, \phi_3, \phi_4\} \). Here \( \phi_1 \) is the
identity mapping on \( \mathbb{Q}(\sqrt{2}, \sqrt{3}) \) and \( \varphi_i \varphi_j = \varphi_k \) when \( \{i,j,k\} = \{1,2,3\} \). Thus \( Aut_\mathbb{Q}(\sqrt{2}, \sqrt{3}) \cong C_2 \times C_2 \cong V_4 \).

We now proceed to establish the correspondence between intermediate fields of an extension \( E/K \) and subgroups of \( Aut_K E \).

**54.8 Lemma:** Let \( E/K \) be a field extension and put \( G = Aut_K E \).

(1) If \( L \) is an intermediate field of \( E/K \), then
\[
L' = \{ \varphi \in G : l\varphi = l \text{ for all } l \in L \}
\]
is a subgroup of \( G \).

(2) If \( H \) is a subgroup of \( G \), then
\[
H' = \{ a \in E : a\varphi = a \text{ for all } \varphi \in H \}
\]
is an intermediate field of \( E/K \).

**Proof:** (1) Clearly \( I_E \in L' \), so \( L' \neq \emptyset \). If \( \varphi, \psi \in L' \), then \( l(\varphi \psi) = (l\varphi)\psi = l\varphi = l \)
for all \( l \in L \), so \( \varphi \psi \in L' \) and \( l\varphi = l \) gives \( l = l\varphi^{-1} \) for all \( l \in L \), so \( \varphi^{-1} \in L' \). Thus \( L' \) is a subgroup of \( Aut_K E \). (In fact \( L' = Aut_L E \).)

(2) Since any \( \varphi \in H' \subseteq Aut_K E \) fixes the elements of \( K \), we have \( K \subseteq H' \). If \( a, b \in H' \), then \( a\varphi = a \) and \( b\varphi = b \) for all \( \varphi \in H \), so
\[
(a + b)\varphi = a\varphi + b\varphi = a + b, \quad a + b \in H',
\]
\[
(-b)\varphi = -(b\varphi) = -b, \quad -b \in H',
\]
\[
(ab)\varphi = a\varphi b\varphi = ab, \quad ab \in H',
\]
\[
(1/b)\varphi = 1/b\varphi = 1/b \quad (\text{provided } b \neq 0) \quad 1/b \in H'.
\]
So \( H' \) is a subfield of \( E \) and therefore \( H' \) is an intermediate field of \( E/K \). \( \square \)

For example, in the notation of Example 54.7(c), we have
\[
\mathbb{Q}(\sqrt{2}, \sqrt{3})' = 1 \leq G = Aut_\mathbb{Q}(\sqrt{2}, \sqrt{3})
\]
\[
\mathbb{Q}(\sqrt{2})' = \{ \varphi_1, \varphi_2 \}, \quad \mathbb{Q}(\sqrt{3}) = \{ \varphi_1, \varphi_3 \}, \quad \mathbb{Q}(\sqrt{6})' = \{ \varphi_1, \varphi_4 \},
\]
\[
\mathbb{Q}' = G
\]
and
\[
1' = \mathbb{Q}(\sqrt{2}, \sqrt{3})
\]
\[
\{ \varphi_1, \varphi_2 \}' = \mathbb{Q}(\sqrt{2}), \quad \{ \varphi_1, \varphi_3 \}' = \mathbb{Q}(\sqrt{3}), \quad \{ \varphi_1, \varphi_4 \}' = \mathbb{Q}(\sqrt{6}),
\]

659
If $E/K$ is a field extension and $H \leq \text{Aut}_K E$, then $H^\prime$ is called the fixed field of $H$. Let us consider the four extreme cases of the priming correspondence in Lemma 54.8.

54.9 Lemma: Let $E/K$ be a field extension and $G = \text{Aut}_K E$. Then

(1) $1^\prime = E$.
(2) $E^\prime = 1$.
(3) $K^\prime = G$.
(4) $G^\prime$ contains $K$, and possibly $K \subseteq G^\prime$.

Proof: (1) $1^\prime = \{ a \in E : a \varphi = a \text{ for all } \varphi \in 1 \} = \{ a \in E : a 1_K = a \} = E$.
(2) $E^\prime = \{ \varphi \in G : a \varphi = a \text{ for all } a \in E \} = \{ 1_E \} = 1$.
(3) $K^\prime = \{ \varphi \in G : a \varphi = a \text{ for all } a \in K \} = G$.
(4) Of course $K \subseteq G^\prime$. From Example 54.7(a), we know that $\text{Aut}_\mathbb{Q}(\sqrt[3]{2}) = 1$ so that, for the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, we have $G = 1$ and $K = \mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) = 1^\prime = G^\prime$. Thus $G^\prime$ is not always equal to $K$.

\[ E \rightarrow \mathbb{Q} \rightarrow K \rightarrow G \rightarrow 1, \quad E \leftarrow 1 \leftarrow K \rightarrow G \]

54.10 Definition: Let $E/K$ be a field extension and put $G = \text{Aut}_K E$. If $G^\prime$ is equal to $K$, then $E/K$ is said to be a Galois extension and $E$ is said to be Galois over $K$.

Equivalently, $E/K$ is Galois if and only if for any element $a$ of $E \setminus K$, there exists a $\varphi \in \text{Aut}_K E$ such that $a \varphi \neq a$. It is easy to verify that $\mathbb{Q}$ is a Galois extension of $\mathbb{R}$ and that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ are Galois extensions of $\mathbb{Q}$.  

660
54.11 Lemma: Let $E/K$ be a field extension and put $G = \text{Aut}_K E$. Let $L, M$ be intermediate fields of $E/K$ and let $H, J$ be subgroups of $G$. If $X$ is an intermediate field of $E/K$ or a subgroup of $G$, we denote $(X')'$ shortly by $X''$. Then the following hold.

(1) If $L \subseteq M$, then $M' \subseteq L'$.
(2) If $H \subseteq J$, then $J' \subseteq H'$.
(3) $L \subseteq L''$ and $H \subseteq H''$.
(4) $L''' = L'$ and $H''' = H'$.

Proof: (1) Suppose $L \subseteq M$. If $\varphi \in M'$, then $a\varphi = a$ for all $a \in M$ and a fortiori $a\varphi = a$ for all $a \in L$, hence $\varphi \in L'$ and consequently $M' \subseteq L'$.

(2) Suppose $H \subseteq J$. If $a \in J'$, then $a\varphi = a$ for all $\varphi \in J$ and a fortiori $a\varphi = a$ for all $\varphi \in H$, hence $a \in H'$ and consequently $J' \subseteq H'$.

(3) If $a \in L$, then $a\varphi = a$ for all $\varphi \in L'$ by the definition of $L'$, so $a$ is fixed by all the $K$-automorphisms in $L'$. Hence $a$ is in the fixed field of $L'$ and $a \in L'''$. This gives $L \subseteq L''$. If $\varphi \in H$, then $a\varphi = a$ for all $a \in H'$ by the definition of $H'$, so $\varphi$ fixes every element in $H'$, so $\varphi \in H''$. This gives $H \subseteq H''$.

(4) By parts (1) and (2), priming reverses inclusion, therefore $L \subseteq L''$ and $H \subseteq H''$ yield $L''' \subseteq L'$ and $H''' \subseteq H'$. Also, using (3) with $L$ replaced by $H$ and $K$ by $L'$, we get $H' \subseteq H'''$ and $L' \subseteq L'''$. So $L''' = L'$ and $H''' = H'$.

In general, $L$ may very well be a proper subset of $L''$ and $H$ a proper subset of $H''$. We introduce a term for the case of equality.

54.12 Definition: Let $E/K$ be a field extension and $G = \text{Aut}_K E$. An intermediate field $L$ of $E/K$ is said to be closed if $L = L''$ and a subgroup $H$ of $G$ is said to be closed if $H = H''$. 

661
So $E$ is Galois over $K$ if and only if $K$ is closed. Lemma 54.11(4) states that any primed object is closed.

**54.13 Theorem:** Let $E/K$ be a field extension and $G = \text{Aut}_K E$. There is a one-to-one correspondence between the set of all closed intermediate fields of $E/K$ and the set of all closed subgroups of $G$, given by $L \rightarrow L'$.

**Proof:** If $L$ is a closed intermediate field of $E/K$, then $L'$ is a subgroup of $G$ by Lemma 54.8(1) and $L'$ is closed by Lemma 54.11(4). Thus priming is a mapping from the set of all closed intermediate fields of the extension into the set of all closed subgroups of $G$. This mapping is one-to-one, for $L' = M'$ implies $(L')'' = (M')''$, whence $L = M$ by Lemma 54.11(4) again. Finally, the priming mapping is onto the set of all closed subgroups of $G$ because, if $H$ is any closed subgroup of $G$, then $H'$ is a closed intermediate field and $(H')' = H$. This completes the proof.

\[\square\]

This theorem is "virtually useless" until we determine which intermediate fields and which subgroups are closed. In the most important case when $E/K$ is a finite dimensional Galois extension, all intermediate fields and all subgroups will turn out to be closed.

Our next goal is to show that an object is closed if it is "bigger than a closed object by a finite amount" (Theorem 54.16). We need two technical lemmas.

If $E/K$ is a field extension and $L,M$ are intermediate fields with $L \subseteq M$, then the dimension $|M:L|$ of $M$ over $L$ will be called the relative dimension of $L$ and $M$. If $G$ is the Galois group of this extension and $H,J$ are subgroups of $G$ with $H \subseteq J$, then the index $|J:H|$ of $H$ in $J$ will be called the relative index of $H$ and $J$.

**54.14 Lemma:** Let $E/K$ be a field extension and $L,M$ intermediate fields with $L \subseteq M$. If the relative dimension $|M:L|$ of $L$ and $M$ is finite,
then the relative index of $M'$ and $L'$ is also finite. In fact, $|L':M'| \leq |M:L|$. In particular, if $E/K$ is a finite dimensional extension, then $|\text{Aut}_k E| \leq |E:K|$.

**Proof:** We make induction on $n = |M:L|$. If $n = 1$, then $M = L$ and $L' = M'$, so $|L':M'| = 1$. Suppose now $n \geq 2$ and that the theorem has been proved for all $i < n$. Since $|M:L| > 1$, we can find an $a \in MN$. Now $|M:L|$ is finite and therefore $M$ is an algebraic extension of $L$ (Theorem 50.10), so $a$ is algebraic over $L$. Let $f(x) \in L[x]$ be the minimal polynomial of $a$ over $L$ and put $k = \deg f(x)$. We have $k > 1$ because $a \notin L$ (Lemma 49.6(1)). From Theorem 50.7, we deduce $|L(a):L| = k$ and Theorem 48.13 gives $|M:L(a)| = n/k$. The situation is depicted below.

\[
\begin{array}{ccc}
M & \rightarrow & M' \\
\downarrow & & \downarrow \\
\begin{array}{c}
\uparrow \\
n/k \\
\end{array} & \uparrow & \begin{array}{c}
\uparrow \\
L(a) \\
\end{array} \\
\begin{array}{c}
\uparrow \\
k \\
\end{array} & \uparrow & \begin{array}{c}
\uparrow \\
L \\
\end{array} \\
\end{array}
\]

In case $k < n$, induction settles everything: from $n/k < n$ and $k < n$, we obtain $|L(a)':M'| \leq |M:L(a)|$ and $|L':L(a)\gamma| \leq |L(a):L|$ and therefore $|L':M'| = |L':L(a)\gamma| = |L(a)':M'| \leq |L(a):L| |M:L(a)| = k(n/k) = n = |M:L|$. The case $k = n$ requires a separate argument.

Suppose now $k = n$ so that $|M:L(a)| = 1$ and $M = L(a)$. In order to prove $|L':M'| \leq n$, we construct a one-to-one mapping from the set $\mathcal{R}$ of all right cosets of $M'$ in $L'$ into the set of all distinct roots of $f(x)$. Since $\mathcal{R}$ has $|L':M'|$ right cosets, this will prove that $|L':M'| \leq r$, where $r$ is the number of distinct roots of $f(x)$ in $M$. As $r \leq \deg f = |L(a):L| = |M:L|$, the theorem will be thereby proved.

What the required mapping should be is suggested by Lemma 54.5. We put \[
\alpha: \mathcal{R} \rightarrow \{b \in M: f(b) = 0\}
\]
for $\varphi \in L'$. Since $a$ is a root of $f(x)$ and $\varphi \in L' \leq G = \text{Aut}_k E$, Lemma 54.5 yields that $a\varphi$ is indeed a root of $f(x)$. The mapping $\alpha$ is well defined, for if $M'\varphi = M'\psi$ ($\varphi, \psi \in L'$), then $\varphi = \mu \psi$ for some $\mu \in M'$, so $\mu$ fixes every element of $M$, so $\mu$ fixes $a$ and $(M'\varphi)\alpha = a\varphi = a(\mu \psi) = (a\mu)\psi = a\psi = (M'\psi)\alpha$. Moreover, $\alpha$ is one-to-one, for if $(M'\varphi)\alpha = (M'\psi)\alpha$, then $a\varphi = a\psi$, so $a\varphi \psi^{-1} = \psi(a) \neq 1$. Therefore $\alpha$ is a one-to-one mapping from $\mathcal{R}$ to $\{b \in M: f(b) = 0\}$.
Let \( E/K \) be a field extension and \( HJ \) are subgroups of \( G = \text{Aut}_k E \) with \( H \leq J \). If the relative index \( |J:H| \) of \( H \) and \( J \) is finite, then the relative dimension of \( J' \) and \( H' \) is also finite. In fact, \( |H':J'| \leq |J:H| \).

**Proof:** Let \( |J:H| = n \) and assume, by way of contradiction, that \( |H':J'| > n \). Then there are \( n + 1 \) elements in \( H' \) that are linearly independent over \( J' \), say \( a_1, a_2, \ldots, a_n, a_{n+1} \). Let \( \bigcup_{i=1}^{n} H\varphi_i \) be the disjoint decomposition of \( J \) as a union of right cosets of \( H \).

We consider the system of \( n \) linear equations in \( n + 1 \) unknowns:

\[
(a_1 \varphi_1)x_1 + (a_2 \varphi_1)x_2 + (a_3 \varphi_1)x_3 + \cdots + (a_{n+1} \varphi_1)x_{n+1} = 0 \\
(a_1 \varphi_2)x_1 + (a_2 \varphi_2)x_2 + (a_3 \varphi_2)x_3 + \cdots + (a_{n+1} \varphi_2)x_{n+1} = 0 \\
\vdots \\
(a_1 \varphi_n)x_1 + (a_2 \varphi_n)x_2 + (a_3 \varphi_n)x_3 + \cdots + (a_{n+1} \varphi_n)x_{n+1} = 0
\]

(b)

where the coefficients \( a_i \varphi_j \) are in the field \( E \). Since the number of unknowns is greater than the number of equations, this system (b) has a nontrivial solution in \( E \) (Theorem 45.1). From the nontrivial solutions of (b), we choose one for which the number of zeroes among \( x_i \) is as small as possible. Let \( x_1 = b_1, x_2 = b_2, x_3 = b_3, \ldots, x_{n+1} = b_{n+1} \) be such a solution. Assume \( r \) of the \( b_j \) are nonzero (\( r \leq n + 1 \)). By the choice of \( b_j \), there is no solution \( x_1 = c_1, x_2 = c_2, x_3 = c_3, \ldots, x_{n+1} = c_{n+1} \) of (b) in which the number of nonzero \( c_j \)'s is less than \( r \).

Eventually after renumbering, we may assume that \( b_1, \ldots, b_r \) are distinct from zero and (in case \( n + 1 > r \)) \( b_{r+1} = \cdots = b_{n+1} = 0 \). Also, we may assume that \( b_1 = 1 \), for otherwise we may take the solution \( b_1/b_1, b_2/b_1, b_3/b_1, \ldots, b_{n+1}/b_1 \) instead of \( b_1, b_2, b_3, \ldots, b_{n+1} \). Of course the number \( r \) of nonzero elements in both solutions are the same.

Let \( \varphi \in J \). We consider the system:

\[
L(a) = M, \quad \varphi \varphi^{-1} \in M' \quad \text{and} \quad M' = M'.
\]

This completes the proof of \( |L':M| \leq |M:L| \).

The assertion \( |\text{Aut}_k E| \leq |E:K| \) follows easily: \( |\text{Aut}_k E| = |\text{Aut}_k E:1| = |K:1| = |K':E| \leq |E:K| \). \( \Box \)
We make two remarks concerning \((s)\). First, since \(x_1 = b_1 = 1\), \(x_2 = b_2\), \(x_3 = b_3\), \ldots, \(x_{n+1} = b_{n+1}\) is a solution of \((b)\) and \(\psi\) is a homomorphism, it is clear that \(x_1 = b_1\psi = 1\), \(x_2 = b_2\psi\), \(x_3 = b_3\psi\), \ldots, \(x_{n+1} = b_{n+1}\psi\) is a solution of \((s)\).

Second, the system \((s)\) is identical with \((b)\), aside from the order of the equations. To prove the last assertion, we note that \(\varphi_1\psi, \varphi_2\psi, \varphi_3\psi, \ldots, \varphi_n\psi\) are elements of distinct right cosets of \(H\) in \(J\), for \(H\varphi_i\psi = H\varphi_j\psi\) implies \((\varphi_i\psi)(\varphi_j\psi)^{-1} \in H\), so \(\varphi_i\psi^{-1} \in H\), so \(H\varphi_i = H\varphi_j\), so \(i = j\). Let us write then

\[
H\varphi_1\psi = H\varphi_1, \quad H\varphi_2\psi = H\varphi_2, \quad H\varphi_3\psi = H\varphi_3, \ldots, H\varphi_n\psi = H\varphi_n,
\]

so that

\[
\varphi_1\psi = \eta_1 \varphi_1, \quad \varphi_2\psi = \eta_2 \varphi_2, \quad \varphi_3\psi = \eta_3 \varphi_3, \ldots, \varphi_n\psi = \eta_n \varphi_n,
\]

for some \(\eta_1, \eta_2, \eta_3, \ldots, \eta_n \in H\) (where \(\{i_1, i_2, i_3, \ldots, i_n\} = \{1, 2, \ldots, n\}\)). Thus each \(\eta_k\) fixes each \(a_m\) in \(H^*\) and the \(i_k\)-th equation

\[
(a_1 \varphi_{i_1}^k)x_1 + (a_2 \varphi_{i_2}^k)x_2 + (a_3 \varphi_{i_3}^k)x_3 + \cdots + (a_{n+1} \varphi_{i_{n+1}}^k)x_{n+1} = 0
\]

in \((b)\) is identical with

\[
(a_1 \eta_k \varphi_{i_1}^k)x_1 + (a_2 \eta_k \varphi_{i_2}^k)x_2 + (a_3 \eta_k \varphi_{i_3}^k)x_3 + \cdots + (a_{n+1} \eta_k \varphi_{i_{n+1}}^k)x_{n+1} = 0
\]

and therefore with the \(k\)-th equation

\[
(a_1 \varphi_k^k)x_1 + (a_2 \varphi_k^k)x_2 + (a_3 \varphi_k^k)x_3 + \cdots + (a_{n+1} \varphi_k^k)x_{n+1} = 0
\]

in \((s)\). This proves that \((b)\) and \((s)\) are identical systems.

Consequently, the solution \(x_1 = 1, x_2 = b_2\psi, x_3 = b_3\psi, \ldots, x_{n+1} = b_{n+1}\psi\) of \((s)\) is also a solution of \((b)\). Now \(x_1 = 1, x_2 = b_2, x_3 = b_3, \ldots, x_{n+1} = b_{n+1}\) is a solution of \((b)\). Hence the difference of these solutions

\[
x_1 = 0, \quad x_2 = b_2 - b_2\psi, \quad x_3 = b_3 - b_3\psi, \ldots, x_{n+1} = b_{n+1} - b_{n+1}\psi
\]

i.e.,

\[
x_1 = 0, \quad x_2 = b_2 - b_2\psi, \quad x_r = b_r - b_r\psi, \quad x_{r+1} = 0, \ldots, x_{n+1} = 0
\]

is a solution of \((b)\).

So far, \(\psi\) was an arbitrary element of \(J\). We now make a judicious choice of \(\psi\). One of the \(\varphi_1, \varphi_2, \varphi_3, \ldots, \varphi_n\) belongs to \(H\), say \(\varphi_1 \in H\), so \(a_m \varphi_1 = a_m\) because \(a_m \in H^*\) for \(m = 1, 2, \ldots, n, n + 1\). Since \(x_1 = b_1, x_2 = b_2, x_3 = b_3, \ldots, x_{n+1} = b_{n+1}\) is a solution of \((b)\), we get

\[
a_1 b_1 + a_2 b_2 + a_3 b_3 + \cdots + a_{n+1} b_{n+1} = 0
\]

665
from the first equation in (b). Here \( \{a_1, a_2, a_3, \ldots, a_{n+1}\} \) is linearly independent over \( J' \) and \( b_1 = 1 \neq 0 \). Thus all of \( b_1, b_2, b_3, \ldots, b_{n+1} \) cannot be in \( J' \): one of them, say \( b_2 \), is not in \( J' \). So there is a \( \psi \in J \) such that \( b_2 \psi \neq b_2 \).

We choose \( \psi \in J \) such that \( b_2 \psi \neq b_2 \). Then the solution (c) of the system (b) is a nontrivial solution in which the number of nonzero elements is less than \( r \), contrary to the meaning of \( r \) as the smallest number of nonzero elements in any solution of (b). This contradiction shows that \( |H' : J'| > n \) is impossible. Hence \( |H' : J'| \leq n = |J:H| \). 

\[ \square \]

**54.16 Theorem:** Let \( E/K \) be a field extension and \( G = \text{Aut}_K E \). Let \( L, M \) be intermediate fields of \( E/K \) with \( L \subseteq M \) and let \( H, J \) be subgroups of \( G \) with \( H \leq J \).

(1) If \( L \) is closed and \( |M:L| \) is finite, then \( M \) is closed and \( |L:M'| = |M:L| \).

(2) If \( H \) is closed and \( |J:H| \) is finite, then \( J \) is closed and \( |H':J'| = |J:H| \).

**Proof:** (1) Here \( M \subseteq M' \) by Lemma 54.11(3) and \( L = L'' \) by hypothesis, so

\[ |M:L| \leq |M':M| \cdot |M:L| = |M':L'| = |M':L'| \cdot |L':M'| \leq |L':M'| \leq |M:L|, \]

the last two inequalities by Lemma 54.15 and Lemma 54.14, respectively. This proves \( |L':M'| = |M:L| \). The proof of (2) is similar and will be omitted.

\[ \square \]

We are now in a position to state and prove the major theorem of this paragraph.

**54.17 Theorem (Fundamental theorem of Galois theory):** Let \( E/K \) be a finite dimensional Galois extension of fields and \( G = \text{Aut}_K E \). Then there is a one-to-one correspondence between the set of all intermediate fields of \( E/K \) and the set of all subgroups of \( G \), given by \( L \rightarrow L' \). In this correspondence, the relative dimension of two intermediate fields is equal to the relative index of the corresponding subgroups. In particular, \( |G| = |\text{Aut}_K E| = |E/K| \).
Proof: By Theorem 54.13, there is a one-to-one correspondence between the set of all closed intermediate fields of $E/K$ and the set of all closed subgroups of $G$, given by $L \rightarrow L'$. Now $K$ is closed ($E/K$ is a Galois extension) by hypothesis and all intermediate fields are closed by Theorem 54.16(1) since they are finite dimensional over $K$. Moreover, if $M$ is any intermediate field, then $|K':M'| = |M:K|$. In particular, $E$ is closed and $|\text{Aut}_K E| = |G| = |G:E'| = |K':E'| = |E:K|$. Hence $G$ is finite. Since 1 is closed, it follows from Theorem 54.16(2) that all subgroups of $G$ are closed, because they are finite subgroups of $G$. Hence the priming mapping is a one-to-one correspondence between the set of all intermediate fields of $E/K$ and the set of all subgroups of $G$. Theorem 54.16 tells that the relative dimension $|M:L|$ of two intermediate fields $L \subseteq M$ is equal to the relative index $|L':M'|$ of the corresponding subgroups of $G$ and that the relative index $|J:H|$ of two subgroups $H \triangleleft J$ of $G$ is equal to the relative dimension $|H':J'|$ of the corresponding intermediate fields. 

54.18 Examples: (a) Let $\sqrt[3]{2}$ be the real cube root of 2 and consider the extension $\mathbb{Q}(\sqrt[3]{2}, \omega)$ over $\mathbb{Q}$. The $\mathbb{Q}$-automorphisms of $\mathbb{Q}(\sqrt[3]{2}, \omega)$ are $\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6$, where

\[
\begin{align*}
\varphi_1: \sqrt[3]{2} &\mapsto \sqrt[3]{2}, & \omega &\mapsto \omega, \\
\varphi_2: \sqrt[3]{2} &\mapsto \sqrt[3]{2}, & \omega &\mapsto \omega^2 = -1 - \omega, \\
\varphi_3: \sqrt[3]{2} &\mapsto \sqrt[3]{2} \omega, & \omega &\mapsto \omega, \\
\varphi_4: \sqrt[3]{2} &\mapsto \sqrt[3]{2} \omega, & \omega &\mapsto \omega^2 = -1 - \omega, \\
\varphi_5: \sqrt[3]{2} &\mapsto \sqrt[3]{2} \omega^2 = \sqrt[3]{2}(-1 - \omega), & \omega &\mapsto \omega, \\
\varphi_6: \sqrt[3]{2} &\mapsto \sqrt[3]{2} \omega^2 = \sqrt[3]{2}(-1 - \omega), & \omega &\mapsto \omega^2 = -1 - \omega.
\end{align*}
\]

Any element $u$ of $\mathbb{Q}(\sqrt[3]{2}, \omega)$ can be written uniquely in the form

\[u = a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\omega + e\sqrt[3]{2}\omega + f\sqrt[3]{4}\omega,\]

where $a, b, c, d, e, f$ are rational numbers. We show that $\mathbb{Q}(\sqrt[3]{2}, \omega)$ is Galois over $\mathbb{Q}$. To this end, we have to show that the fixed field of $G$ is exactly $\mathbb{Q}$. Since

667
\((a + b\sqrt{2} + c\sqrt{4} + d\omega + e\sqrt{2}\omega + f\sqrt{4}\omega)\varphi_2\)

\[= a + b\sqrt{2} + c\sqrt{4} + (d + e\sqrt{2} + f\sqrt{4})\omega^2\]

\[= a + b\sqrt{2} + c\sqrt{4} + (d + e\sqrt{2} + f\sqrt{4})(-1 - \omega)\]

\[= (a - d) + (b - e)\sqrt{2} + (c - f)\sqrt{4} - d\omega - e\sqrt{2}\omega - f\sqrt{4}\omega.\]

we see that an element \(u = a + b\sqrt{2} + c\sqrt{4} + d\omega + e\sqrt{2}\omega + f\sqrt{4}\omega\) of \(\mathbb{Q}(\sqrt{2}, \omega)\) is fixed by \(\varphi_2\) if and only if

\[
\begin{align*}
  a &= a - d, \quad d = -d \\
  b &= b - e, \quad e = -e \\
  c &= c - f, \quad f = -f.
\end{align*}
\]

So an element \(u\) of \(\mathbb{Q}(\sqrt{2}, \omega)\) fixed by \(\varphi_2\) has the form \(a + b\sqrt{2} + c\sqrt{4}\). If \(u\) is fixed also by \(\varphi_3\), then

\[
\begin{align*}
  a + b\sqrt{2} + c\sqrt{4} &= (a + b\sqrt{2} + c\sqrt{4})\varphi \\
  &= a + b\sqrt{2} + c\sqrt{4}^2 \\
  &= a + b\sqrt{2} + c\sqrt{4}(-1 - \omega) \\
  &= a - c\sqrt{4} + b\sqrt{2} - c\sqrt{4}\omega
\end{align*}
\]

yields \(b = 0\), \(c = -c\), \(-c = 0\) and so \(u = a \in \mathbb{Q}\). Since an element \(u\) in the fixed field of \(G\) is necessarily fixed by \(\varphi_2\) and \(\varphi_3\), that \(u\) has to be rational.

Thus the fixed field of \(G\) is \(\mathbb{Q}\). This shows that \(\mathbb{Q}(\sqrt{2}, \omega)\) is Galois over \(\mathbb{Q}\).

The multiplication table of \(G(\mathbb{Q}(\sqrt{2}, \omega)/\mathbb{Q})\) can be constructed easily.

Since \(\sqrt{2}\varphi_2\varphi_3 = \sqrt{2}\varphi_3 = \sqrt{2}\omega\) and \(\omega\varphi_2\varphi_3 = \omega^2\varphi_3 = \omega^2\), we have \(\varphi_2\varphi_3 = \varphi_4\) etc.

and the multiplication table of \(G(\mathbb{Q}(\sqrt{2}, \omega)/\mathbb{Q})\) is

\[
\begin{array}{cccccccc}
\varphi_1 & \varphi_2 & \varphi_3 & \varphi_4 & \varphi_5 & \varphi_6 \\
\varphi_1 & \varphi_1 & \varphi_2 & \varphi_3 & \varphi_4 & \varphi_5 & \varphi_6 \\
\varphi_2 & \varphi_2 & \varphi_1 & \varphi_4 & \varphi_3 & \varphi_6 & \varphi_5 \\
\varphi_3 & \varphi_3 & \varphi_6 & \varphi_1 & \varphi_3 & \varphi_5 & \varphi_2 \\
\varphi_4 & \varphi_4 & \varphi_5 & \varphi_6 & \varphi_1 & \varphi_2 & \varphi_3 \\
\varphi_5 & \varphi_5 & \varphi_4 & \varphi_1 & \varphi_6 & \varphi_3 & \varphi_2 \\
\varphi_6 & \varphi_6 & \varphi_3 & \varphi_2 & \varphi_5 & \varphi_4 & \varphi_1 \\
\end{array}
\]
So $G(\mathbb{Q}(\sqrt{2}, \omega)/\mathbb{Q})$ is a nonabelian group of order 6 and isomorphic to $S_3$, as can be easily seen by comparing the table above with the multiplication table of $S_3$:

<table>
<thead>
<tr>
<th></th>
<th>$t$</th>
<th>$(23)$</th>
<th>$(123)$</th>
<th>$(12)$</th>
<th>$(132)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$t$</td>
<td>$t$</td>
<td>$(23)$</td>
<td>$(123)$</td>
<td>$(12)$</td>
<td>$(132)$</td>
</tr>
<tr>
<td>$(23)$</td>
<td>$(23)$</td>
<td>$t$</td>
<td>$(12)$</td>
<td>$(123)$</td>
<td>$(13)$</td>
</tr>
<tr>
<td>$(132)$</td>
<td>$(123)$</td>
<td>$(13)$</td>
<td>$(132)$</td>
<td>$(23)$</td>
<td></td>
</tr>
<tr>
<td>$(12)$</td>
<td>$(123)$</td>
<td>$(13)$</td>
<td>$(132)$</td>
<td>$t$</td>
<td>$(23)$</td>
</tr>
<tr>
<td>$(123)$</td>
<td>$(132)$</td>
<td>$(12)$</td>
<td>$t$</td>
<td>$(13)$</td>
<td></td>
</tr>
<tr>
<td>$(132)$</td>
<td>$(123)$</td>
<td>$(123)$</td>
<td>$(23)$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$(13)$</td>
<td>$(132)$</td>
<td>$(23)$</td>
<td>$(132)$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$(12)$</td>
<td>$t$</td>
<td>$(123)$</td>
<td>$(132)$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The isomorphism $G(\mathbb{Q}(\sqrt{2}, \omega)/\mathbb{Q}) \cong S_3$ can be found in a better way by observing that any automorphism in $G(\mathbb{Q}(\sqrt{2}, \omega)/\mathbb{Q})$ is completely determined by its effect on the roots of $x^3 - 2$. The roots of $x^3 - 2$ are $u_1 = \sqrt[3]{2}$, $u_2 = \sqrt[3]{2} \omega$, $u_3 = \sqrt[3]{2} \omega^2$. Now $\varphi_2$ maps $u_1$ to $u_1$, $u_2$ to $u_3$ and $u_3$ to $u_2$ and can therefore be represented, in a readily understood extension of the notation for permutations, as $\left( \begin{array}{ccc} u_1 & u_2 & u_3 \\ u_1 & u_3 & u_2 \end{array} \right) = (u_1)(u_2u_3) = (u_2u_3)$. Dropping $u$ and retaining only the indices, we see that $\varphi_2$ can be thought of as the permutation $(23)$ in $S_3$. The other $\varphi_j$ can be thought of as permutations in $S_3$ in a similar way and this gives the isomorphism $G(\mathbb{Q}(\sqrt{2}, \omega)/\mathbb{Q}) \cong S_3$.

In the multiplication tables above, $\varphi_j$ and its image in $S_3$ under this isomorphism occupy corresponding places.

The subgroup structure of $S_3$ is well known. The subgroups of $S_3$ are depicted in the Hasse diagram below ($A \rightarrow B$ means $A \subseteq B$).
\{\lambda(23)\} \quad \{\lambda(13)\} \quad \{\lambda(12)\}

\{\lambda(123),(132)\} = A_3

S_3

So the subgroups of \(G(\mathbb{Q}(\sqrt{2},\omega)/\mathbb{Q})\) are

\{1\}

\{\varphi_1,\varphi_2\} \quad \{\varphi_1,\varphi_5\} \quad \{\varphi_1,\varphi_4\}

\{\varphi_1,\varphi_3,\varphi_5\}

\(G(\mathbb{Q}(\sqrt{2},\omega)/\mathbb{Q})\)

and priming yields

\(\mathbb{Q}(\sqrt{2},\omega)\)

\(\mathbb{Q}(\sqrt{2}) \quad \mathbb{Q}(\sqrt{2}\omega) \quad \mathbb{Q}(\sqrt{2}\omega^2) \quad \mathbb{Q}(\omega) \quad \mathbb{Q}.

670
Let $\sqrt[4]{2}$ be the real fourth root of 2 and consider the extension $\mathbb{Q}(\sqrt[4]{2}, i)$ over $\mathbb{Q}$. The $\mathbb{Q}$-automorphisms of $\mathbb{Q}(\sqrt[4]{2}, i)$ are $\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6, \varphi_7, \varphi_8$ where

- $\varphi_1: \sqrt[4]{2} \rightarrow \sqrt[4]{2}, \quad i \rightarrow i,$
- $\varphi_2: \sqrt[4]{2} \rightarrow \sqrt[4]{2}, \quad i \rightarrow -i,$
- $\varphi_3: \sqrt[4]{2} \rightarrow -\sqrt[4]{2}i, \quad i \rightarrow i,$
- $\varphi_4: \sqrt[4]{2} \rightarrow -\sqrt[4]{2}i, \quad i \rightarrow -i,$
- $\varphi_5: \sqrt[4]{2} \rightarrow -\sqrt[4]{2}, \quad i \rightarrow i,$
- $\varphi_6: \sqrt[4]{2} \rightarrow -\sqrt[4]{2}, \quad i \rightarrow -i,$
- $\varphi_7: \sqrt[4]{2} \rightarrow \sqrt[4]{2}, \quad i \rightarrow i,$
- $\varphi_8: \sqrt[4]{2} \rightarrow -\sqrt[4]{2}i, \quad i \rightarrow -i.$

We put $\phi_2 = \tau$ and $\phi_3 = \sigma$. Then $o(\tau) = 2$, $o(\sigma) = 4$ and $\sigma^f = \sigma^{-1}$. Thus $G(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ is a dihedral group of order 8. Since any automorphism in $G(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ is completely determined by its effect on the four roots $u_1 = \sqrt[4]{2}, u_2 = \sqrt[4]{2}i, u_3 = -\sqrt[4]{2}, u_4 = -\sqrt[4]{2}i$ of $x^4 - 2$, the group $G(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ is isomorphic to a subgroup of $S_4$. We see $\sigma = \left(\begin{array}{cccc}u_1 & u_2 & u_3 & u_4 \\ u_2 & u_3 & u_4 & u_1\end{array}\right) = (u_1 u_2 u_3 u_4)$ and $\tau = \left(\begin{array}{cccc}u_1 & u_2 & u_3 & u_4 \\ u_1 & u_4 & u_3 & u_2\end{array}\right) = (u_2 u_4)$. So $G(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}) \cong \langle(24),(1234)\rangle = \{1, (13),(24),(12)(34),(13)(24),(14),(23),(1234),(1432)\} \leq S_4$ by an isomorphism $\varphi_2 = \tau \rightarrow (24), \varphi_3 = \sigma \rightarrow (1234)$. The subgroups of $G(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ are

- $\{1, \tau\}$
- $\{1, \sigma^2 \tau\}$
- $\{1, \sigma^3 \tau\}$
- $\{1, \sigma^2\}$
- $\{1, \sigma \tau\}$

We see $\sigma = \left(\begin{array}{cccc}u_1 & u_2 & u_3 & u_4 \\ u_2 & u_3 & u_4 & u_1\end{array}\right) = (u_1 u_2 u_3 u_4)$ and $\tau = \left(\begin{array}{cccc}u_1 & u_2 & u_3 & u_4 \\ u_1 & u_4 & u_3 & u_2\end{array}\right) = (u_2 u_4)$. So $G(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}) \cong \langle(24),(1234)\rangle = \{1, (13),(24),(12)(34),(13)(24),(14),(23),(1234),(1432)\} \leq S_4$ by an isomorphism $\varphi_2 = \tau \rightarrow (24), \varphi_3 = \sigma \rightarrow (1234)$. The subgroups of $G(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ are

- $\{1, \tau\}$
- $\{1, \sigma^2 \tau\}$
- $\{1, \sigma^3 \tau\}$
- $\{1, \sigma^2\}$
- $\{1, \sigma \tau\}$

We see $\sigma = \left(\begin{array}{cccc}u_1 & u_2 & u_3 & u_4 \\ u_2 & u_3 & u_4 & u_1\end{array}\right) = (u_1 u_2 u_3 u_4)$ and $\tau = \left(\begin{array}{cccc}u_1 & u_2 & u_3 & u_4 \\ u_1 & u_4 & u_3 & u_2\end{array}\right) = (u_2 u_4)$. So $G(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}) \cong \langle(24),(1234)\rangle = \{1, (13),(24),(12)(34),(13)(24),(14),(23),(1234),(1432)\} \leq S_4$ by an isomorphism $\varphi_2 = \tau \rightarrow (24), \varphi_3 = \sigma \rightarrow (1234)$. The subgroups of $G(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ are

- $\{1, \tau\}$
- $\{1, \sigma^2 \tau\}$
- $\{1, \sigma^3 \tau\}$
- $\{1, \sigma^2\}$
- $\{1, \sigma \tau\}$
Let us find the intermediate field of \( \mathbb{Q}(\sqrt{2}, i) / \mathbb{Q} \) corresponding to \( \{1, \sigma^{2}\tau\} \).

We write \( u = \sqrt{2} \) for brevity. We have \((u)\sigma^{2}\tau = (u\sigma)\sigma\tau = (u\sigma)i\sigma\tau = (ui\cdot i)\tau = -(ut) = -u\) and \((i)\sigma^{2}\tau = (i\sigma)\sigma\tau = (i\sigma)i = it = -i\). Now let \( a, b, c, d, e, f, g, h \in \mathbb{Q} \) and \( s = a + bu + cu^{2} + du^{3} + ei + fui + gu^{2}i + hu^{3}i \). Then \( s\sigma^{2}\tau = (a + bu + cu^{2} + du^{3} + ei + fui + gu^{2}i + hu^{3}i)\tau \)
\[ = a + b(-u) + c(-u)^{2} + d(-u)^{3} + e(-i) + f(-u)(-i) + g(-u)(-i) + h(-u)^{3}(-i) \]
\[ = a - bu + cu^{2} - du^{3} - ei + fui - gu^{2}i + hu^{3}i \]

and so \( s \) is fixed under \( \sigma^{2}\tau \) if and only if
\[ a = a, \quad b = -b, \quad c = c, \quad d = -d, \quad e = -e, \quad f = f, \quad g = -g, \quad h = h, \]
so if and only if \( b = d = e = g = 0 \), so if and only if \( s = a + cu^{2} + fui + hu^{3}i = a + f(ui) - c(ui)^{2} - h(ui)^{3} \)
so if and only if \( s \in \mathbb{Q}(ui) \).

Thus the intermediate field of \( \mathbb{Q}(\sqrt{2}, i) / \mathbb{Q} \) corresponding to \( \{1, \sigma^{2}\tau\} \) is \( \mathbb{Q}(ui) = \mathbb{Q}(\sqrt{2}i) \). Similar computations yield that the Galois correspondence is as in the diagram below, where intermediate fields occupy the same relative position as the corresponding subgroups.
Let \( p \) be a prime number and \( n \in \mathbb{N} \). We consider the extension \( \mathbb{F}_{p^n}/\mathbb{F}_p \). The mapping \( \sigma: \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, a \to a^p \) is a field homomorphism (Lemma 52.2) and fixes every element in \( \mathbb{F}_p \) (Theorem 12.7 or Theorem 52.8). Thus \( \sigma \) is \( \mathbb{F}_p \)-linear and, since \( |\mathbb{F}_{p^n}:\mathbb{F}_p| \) is finite, \( \sigma \) is onto \( \mathbb{F}_{p^n} \) (Theorem 42.22). So \( \sigma \) is an \( \mathbb{F}_p \)-automorphism of \( \mathbb{F}_{p^n} \).

We put \( G = \text{Aut}_{\mathbb{F}_p} \mathbb{F}_{p^n} \). We want to show \( G = \langle \sigma \rangle \). First we prove \( o(\sigma) = n \). From \( a\sigma^n = a^p = a \) for all \( a \in \mathbb{F}_{p^n} \) (Lemma 52.4(2) or Theorem 52.8), we get \( \sigma^n = 1 \), so \( o(\sigma) | n \). On the other hand, if \( m \) is a positive proper divisor of \( n \), then \( \mathbb{F}_{p^n} \) has a proper subfield \( \mathbb{F}_{p^m} \) with \( p^m \) elements (Theorem 52.8) and there is a \( b \in \mathbb{F}_{p^n} \setminus \mathbb{F}_{p^m} \) with \( b\sigma^m = \sigma^m \neq b \), so \( \sigma^m \neq 1 \). So we conclude \( o(\sigma) = n \). Since \( |\mathbb{F}_{p^n}:\mathbb{F}_p| \) is finite, we get
\[
n = o(\sigma) = |\langle \sigma \rangle| \leq |G| = |G:1| = (|\mathbb{F}_p|:|\mathbb{F}_{p^n}|) | \leq |\mathbb{F}_{p^n}:\mathbb{F}_p| = n
\]
from Lemma 54.14, so \( |\langle \sigma \rangle| = |G| = n \) and \( G = \langle \sigma \rangle \).

It is now easy to show that \( \mathbb{F}_{p^n} \) is Galois over \( \mathbb{F}_p \). We have
\[
G' = \langle \sigma \rangle = \{ a \in \mathbb{F}_{p^n} : a\sigma = a \} = \mathbb{F}_p
\]
by Theorem 52.8 and thus \( \mathbb{F}_{p^n} \) is Galois over \( \mathbb{F}_p \).

The Galois correspondence is easy to describe. The subgroups of \( \langle \sigma \rangle \) are in one-to-one correspondence with the positive divisors of \( n \) and any subgroup \( H \) of \( G \) is of the form \( H = \langle \sigma^m \rangle \) (Theorem 11.8). The subfield of \( \mathbb{F}_{p^n} \) corresponding to \( H = \langle \sigma^m \rangle \) is
\[
H' = \langle \sigma^m \rangle = \{ a \in \mathbb{F}_{p^n} : a\sigma^m = a \} = \{ a \in \mathbb{F}_{p^n} : a^{p^m} = a \} = \mathbb{F}_{p^m},
\]
the unique subfield of \( \mathbb{F}_{p^n} \) with \( p^m \) elements.

<table>
<thead>
<tr>
<th>( \mathbb{F}_{p^n} )</th>
<th>( \mathbb{F}_p )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( n/m )</td>
<td>( n/m )</td>
</tr>
<tr>
<td>( \mathbb{F}_{p^m} )</td>
<td>( \langle \sigma^m \rangle )</td>
</tr>
<tr>
<td>( m )</td>
<td>( m )</td>
</tr>
<tr>
<td>( \mathbb{F}_p )</td>
<td>( G = \langle \sigma \rangle )</td>
</tr>
</tbody>
</table>

In all these examples, we first determined the subgroups of the Galois group and then found the intermediate fields corresponding to them. One can of course reverse this, i.e., one can determine the intermediate fields in the first place and then find the subgroups corresponding to
them. However, it is in general more difficult to find all intermediate fields of an extension, for it is likely that one overlooks some of them. Also, it is more difficult to avoid duplications. For instance, in Example 54.18(c), it is not immediately clear where \( \mathbb{Q}(\sqrt{2}(1+i)) \) and \( \mathbb{Q}(\sqrt{2}(1-i)) \) are, nor whether \( \mathbb{Q}(\sqrt{2}(1+i)) = \mathbb{Q}(\sqrt{2}(1-i)) \). It is far easier to list the subgroups than to list the intermediate fields.

It is natural to ask which intermediate fields correspond to the normal subgroups of the Galois group of an extension. Also, what can be said about the factor groups of the Galois group? We proceed to answer these questions. We need a definition.

**54.19 Definition:** Let \( E/K \) be a field extension and let \( G = \text{Aut}_K E \) be its Galois group. An intermediate field \( L \) of this extension is said to be **stable relative to** \( K \) and \( E \), or to be \( (K,E) \)-stable if every \( K \)-automorphism \( \varphi \in \text{Aut}_K E \) of \( E \) maps \( L \) into \( L \).

In the situation of Definition 54.19, if \( L \) is a \( (K,E) \)-stable intermediate field, then the inverse \( \varphi^{-1} \) of any \( K \)-automorphism \( \varphi \) of \( E \) also maps \( L \) into \( L \). Thus the restriction \( \varphi|_L \) to \( L \) of any \( K \)-automorphism of \( E \) is a \( K \)-automorphism of \( L \). Thus we have a "restriction" mapping

\[
\text{res} : \text{Aut}_K E \to \text{Aut}_K L \\
\varphi \quad \mapsto \quad \varphi|_L
\]

A \( K \)-automorphism \( \lambda \) of \( L \) is said to be **extendible to** \( E \) if there is a \( K \)-automorphism \( \varphi \) of \( E \) such that \( \lambda = \varphi|_L \). Therefore \( \text{res} \) is a mapping onto the set of all extendible \( K \)-automorphisms of \( L \).

**54.20 Theorem:** Let \( E/K \) be a field extension.

1. If \( L \) is a \( (K,E) \)-stable intermediate field, then \( L' \) is a normal subgroup of the Galois group \( \text{Aut}_K E \).
2. If \( H \) is a normal subgroup of \( \text{Aut}_K E \), then \( H' \) is a \( (K,E) \)-stable intermediate field of the extension.
**Proof:** (1) We are to prove that \( \varphi^{-1} \lambda \varphi \in L \) for all \( \lambda \in L' \) and \( \varphi \in \text{Aut}_K E \). Thus we must show that \( a(\varphi^{-1} \lambda \varphi) = a \) for all \( a \in L \). Indeed, if \( a \in L, \lambda \in L' \) and \( \varphi \in \text{Aut}_K E \), then \( a \varphi^{-1} \in L \) since \( L \) is \((K,E)\)-stable, so \( (a \varphi^{-1}) \lambda = a \varphi^{-1} \), so \( a(\varphi^{-1} \lambda \varphi) = (a \varphi^{-1} \lambda) \varphi = (a \varphi^{-1}) \varphi = a \). Hence \( L' \subseteq \text{Aut}_K E \).

(2) We are to prove that \( a \varphi \in H' \) for all \( a \in H' \) and \( \varphi \in \text{Aut}_K E \). Thus we must show that \( (a \varphi) \eta = a \varphi \) for all \( \eta \in H \). Indeed, if \( a \in H', \eta \in H \) and \( \varphi \in \text{Aut}_K E \), then \( \varphi \eta \varphi^{-1} \in H \) since \( H \subseteq \text{Aut}_K E \), so \( a(\varphi \eta \varphi^{-1}) = a \), so \( a(\varphi \eta) \varphi^{-1} = a \), so \( a(\varphi \eta) = a \varphi \). Hence \( H' \) is \((K,E)\)-stable. \(\square\)

**54.21 Theorem:** Let \( E/K \) be a Galois extension and \( L \) an intermediate field. If \( L \) is \((K,E)\)-stable, then \( L \) is Galois over \( K \).

**Proof:** For any \( a \in L \cap K \), we must find a \( \lambda \in \text{Aut}_K L \) such that \( a \lambda \neq a \). Since \( E \) is Galois over \( K \), there is a \( \varphi \in \text{Aut}_K E \) such that \( a \varphi \neq a \). Then \( \varphi|_L \in \text{Aut}_K L \) by stability of \( L \) relative to \( K \) and \( E \). Thus \( \varphi|_L \) can be taken as \( \lambda \). \(\square\)

**54.22 Theorem:** Let \( E/K \) be a Galois extension and \( f(x) \in K[x] \) be irreducible in \( K[x] \). If \( f(x) \) has a root in \( E \), then \( f(x) \) splits in \( E \) and the roots of \( f(x) \) are all simple.

**Proof:** Let \( a_1 \) be a root of \( f(x) \) in \( E \). We put \( \text{deg} f(x) = n \). We want to show that \( f(x) = c(x - a_1)(x - a_2)\ldots(x - a_n) \) for some elements \( c,a_1,a_2,\ldots,a_n \) in \( E \).

For this purpose, we put \( g(x) = (x - a_1)(x - a_2)\ldots(x - a_m) \in E[x] \), where \( a_1,a_2,\ldots,a_m \) are all the distinct roots of \( f(x) \) in \( E \). We know \( m \leq n \) from Theorem 35.7.

Any \( K \)-automorphism of \( E \) maps a root of \( f(x) \) to a root of \( f(x) \) (Lemma 54.5). Thus the coefficients of \( g(x) \), which are symmetric in the roots \( a_1,a_2,\ldots,a_m \) of \( g(x) \), are fixed by any \( K \)-automorphism of \( E \). This shows that the coefficients of \( g(x) \) are in \( E' = K \). Hence \( g(x) \in K[x] \). Then \( f(x) \) and \( g(x) \) are two polynomials in \( K[x] \) with a common root \( a_1 \) and \( f(x) \) is irreducible over \( K \). Theorem 35.18(1),(3) gives then \( f(x)|g(x) \) and consequently \( n = \text{deg} f(x) \leq \text{deg} g(x) = m \). We have \( m \leq n \) also, thus \( n = m \).

From \( f(x)|g(x) \) we get then \( f(x) \cong g(x) \). So \( f(x) = c(x - a_1)(x - a_2)\ldots(x - a_n) \) for some \( c \in K^\times \) and the roots \( a_1,a_2,\ldots,a_n \in E \) of are all distinct, i.e., all roots of \( f(x) \) are simple. \(\square\)
The next theorem is a kind of converse to Theorem 54.21. The result is not necessarily true without the hypothesis that \( L \) is algebraic (cf. Ex. 8).

54.23 Theorem: Let \( E/K \) be a field extension and \( L \) an intermediate field. If \( L \) is algebraic and Galois over \( K \), then \( L \) is \((K,E)\)-stable.

Proof: We want to show that \( a \varphi \in L \) for any \( a \in L \) and any \( \varphi \in \text{Aut}_K E \). If \( a \in L \), then \( a \) is algebraic over \( K \) since \( L \) is algebraic over \( K \). Let \( f(x) \) be the minimal polynomial of \( a \) over \( K \). Then \( f(x) \) is a product of \( n \) distinct polynomials of degree one in \( L[x] \) because \( L \) is Galois over \( K \) (Theorem 54.22). Thus all roots of \( f(x) \) are in \( L \). Now if \( \varphi \in \text{Aut}_K E \), then \( a \varphi \) is a root of \( f(x) \), hence \( a \varphi \in L \), as was to be proved. \( \square \)

Let \( E/K \) be a field extension and let \( L \) be a \((K,E)\)-stable intermediate field of \( E/K \). Let us consider the restriction mapping

\[
res : \text{Aut}_K E \to \text{Aut}_K L \\
\varphi \to \varphi|_L
\]

Since \((\varphi\psi)_L = \varphi_L \psi_L\) for any two \( K \)-automorphisms \( \varphi, \psi \) of \( E \), we see that \( res \) is a homomorphism. Therefore \((\text{Aut}_K E)/\text{Ker } res = \text{Im } res \). Now \( \text{Im } res \) is the set of all \( K \)-automorphisms of \( L \) that are extendible to \( E \) (hence the set of all \( K \)-automorphisms of \( L \) that are extendible to \( E \) is a subgroup of \( \text{Aut}_K E \)) and \( \text{Ker } res = \{ \varphi \in \text{Aut}_K E : \varphi|_L = \text{id}_L \} = \{ \varphi \in \text{Aut}_K E : a \varphi = a \text{ for all } a \in L \} = L' = \text{Aut}_L E \). Hence \((\text{Aut}_K E)/(\text{Aut}_L E)\) is isomorphic to the group of all \( K \)-automorphisms of \( L \) that are extendible to \( E \). We proved the

54.24 Theorem: Let \( E/K \) be a field extension and \( L \) an intermediate field. If \( L \) is \((K,E)\)-stable, then \((L' = \text{Aut}_L E) \) is normal in \( \text{Aut}_K E \) and the quotient group \( G(E/K)/G(E/L) = (\text{Aut}_K E)/(\text{Aut}_L E) \) is isomorphic to the subgroup of \( \text{Aut}_K L \) consisting exactly of the \( K \)-automorphisms of \( L \) that are extendible to \( E \). \( \square \)

We can now supplement the fundamental theorem by describing the situation with respect to an intermediate field.
54.25 Theorem: Let $E/K$ be a finite dimensional Galois extension of fields and $G = \text{Aut}_K E$. Let $L$ be an intermediate field of $E/K$.

(1) $E$ is Galois over $L$.

(2) $L$ is Galois over $K$ if and only if $L' = \text{Aut}_L E$ is normal in $G = \text{Aut}_K E$. In this case, $G/L' = (\text{Aut}_K E)/\text{(Aut}_L E)$ is isomorphic to the Galois group $\text{Aut}_K L$ of $L$ over $K$. Thus $G(E/K)/G(E/L) \cong G(L/K)$.

Proof: Here the hypotheses of the fundamental theorem are satisfied. The fundamental theorem states that any intermediate field of $E/K$ and any subgroup of $G$ is closed.

(1) In order to show that $E$ is Galois over $L$, we must prove that $L = L''$, that is, that $L$ is closed. This follows from the fundamental theorem.

(2) $E/K$ is a finite dimensional extension by hypothesis and so $L/K$ is also a finite dimensional extension. Thus $L$ is algebraic over $K$ (Theorem 50.10) If $L$ is Galois over $K$, then $L$ is $(K,E)$-stable by Theorem 54.24 and so $L'$ is normal in $\text{Aut}_K E$ by Theorem 54.20(1). Conversely, if $L'$ is normal in $\text{Aut}_K E$, then $L''$ is a $(K,E)$-stable intermediate field by Theorem 54.20(2). Here $L = L''$ because all intermediate fields are closed. Thus $L$ is $(K,E)$-stable. Theorem 54.21 tells then that $L$ is Galois over $K$. So $L$ is Galois over $K$ if and only if $L'$ is normal in $G = \text{Aut}_K E$.

Suppose now $L$ is Galois over $K$ and $L' \subseteq G = \text{Aut}_K E$. Then $|\text{Aut}_K L| = |L:K|$ by the fundamental theorem (with $L$ in place of $E$). Theorem 54.23 states that $G/L' = (\text{Aut}_K E)/\text{(Aut}_L E)$ is isomorphic to a subgroup of $\text{Aut}_K L$. Using $L = L''$ (i.e., $L$ is closed) and $G' = K$ (i.e., $L$ is Galois over $K$), we see $|G/L'| = |G:L'| = |L'':G| = |L:K| = |\text{Aut}_K L|$ by the fundamental theorem. Thus $G/L'$, which is isomorphic to a subgroup of $\text{Aut}_K L$, has the same order as $\text{Aut}_K L$. Since $|\text{Aut}_K L| = |L:K|$ is finite, this implies that $G/L'$ is actually isomorphic to $\text{Aut}_K L$ itself, as was to be shown.

We end this paragraph with an important illustration of Theorem 54.25.
54.26 Theorem: Let \( \mathbb{F}_q \) be a field of \( q \) elements and \( E \) a finite dimensional extension of \( \mathbb{F}_q \). Then \( E \) is Galois over \( \mathbb{F}_q \) and \( \text{Aut}_{\mathbb{F}_q} E \) is cyclic, generated by the automorphism \( \varphi \), where \( \varphi: a \rightarrow a^q \) for all \( a \in E \).

Proof: Let \( |E: \mathbb{F}_q| = r \) and \( \text{char} \mathbb{F}_q = p \), so that \( \mathbb{F}_p \) is the prime subfield of \( \mathbb{F}_q \) (and of \( E \)). We have \( q = p^m \), where \( m = |\mathbb{F}_q: \mathbb{F}_p| \). We consider the extension \( E/\mathbb{F}_p \). Since \( E \) is an \( r \)-dimensional vector space over \( \mathbb{F}_q \) and \( \mathbb{F}_q \) is an \( m \)-dimensional vector space over \( \mathbb{F}_p \), Theorem 48.13 says \( E \) is an \( rm \)-dimensional vector space over \( \mathbb{F}_p \) and so \( |E| = p^{rm} \). Thus \( E \) is a finite field and \( E \) is Galois over \( \mathbb{F}_p \) (Example 54.18(c)). Then \( E \) is Galois over any intermediate field of \( E/\mathbb{F}_p \) (Theorem 54.25(1)); in particular, \( E \) is Galois over \( \mathbb{F}_q \). Furthermore, we know from Example 54.18(c) that \( \text{Aut}_{\mathbb{F}_p} E = \langle \sigma \rangle \), where \( \sigma \) is the field isomorphism \( a \rightarrow a^p \) for all \( a \in E \) and that the group \( (\mathbb{F}_q)´ \) corresponding to the intermediate field \( \mathbb{F}_q \) with \( p^m \) elements is \( \langle \sigma^m \rangle \). Thus \( \text{Aut}_{\mathbb{F}_q} E = (\mathbb{F}_q)´ = \langle \varphi \rangle \), where \( \varphi = \sigma^m \) is the mapping \( a \rightarrow a^{p^m} = a^q \) for all \( a \in E \). \[\square\]

Exercises

1. Find the Galois group \( \text{Aut}_k E \) and all its subgroups and describe the Galois correspondence between the subgroups of \( \text{Aut}_k E \) and the intermediate fields of \( E/K \) when

   (a) \( E = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \) and \( K = \mathbb{Q} \);

   (b) \( E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}) \) and \( K = \mathbb{Q}, K = \mathbb{Q}(\sqrt[3]{2}) \);

   (c) \( E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3}, i) \) and \( K = \mathbb{Q}(i), K = \mathbb{Q}(i, \sqrt[4]{3}) \);

   (d) \( E = \mathbb{Q}(\sqrt{2}, i) \) and \( K = \mathbb{Q}(i) \);

   (e) \( E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{5}) \) and \( K = \mathbb{Q}, \mathbb{Q}(\sqrt[3]{2}) \).

2. Let \( E/K \) be a field extension. Prove that if \( L \) is a \( (K,E) \)-stable intermediate field, so is \( L¨ \) and that if \( H \) is a normal subgroup of \( \text{Aut}_K E \), so is \( H¨ \).
3. Let $E/K$ be a field extension and $G = \text{Aut}_K E$. Let $L, M$ be intermediate fields of $E/K$ and let $H, J$ be subgroups of $G$. Prove that $\langle H \cup J \rangle = H' \cap J'$ and $(LM)' = L' \cap M'$.

If, in addition, $L$ is finite dimensional and Galois over $K$, then $LM$ is finite dimensional and Galois over $M$ and $\text{Aut}_{L \cap M} L \cong \text{Aut}_M LM$.

4. Let $K$ be a field and $x$ an indeterminate over $K$. Show that, if $L$ is an intermediate field of $K(x)/K$ and $L \neq K$, then $|K(x):L|$ is finite.

5. Prove that $K(x)$ is Galois over $K$ if and only if $K$ is infinite.

6. Let $K$ be an infinite field. Prove that a proper subgroup of $\text{Aut}_K K(x)$ is closed if and only if it is a finite subgroup of $\text{Aut}_K K(x)$.

7. Consider the extension $\mathbb{Q}(x)/\mathbb{Q}$. Prove that the intermediate field $\mathbb{Q}(x^2)$ is closed and the intermediate field $\mathbb{Q}(x^3)$ is not closed.

8. Let $K$ be an infinite field and $x, y$ two distinct indeterminates over $K$. Show that the intermediate field $K(x)$ of the extension $K(x,y)/K$ is Galois over $K$ but $K(x)$ is not stable relative to $K$ and $K(x,y)$.