In this paragraph, we give some applications of Galois theory to the theory of equations. We shall introduce resultants and discriminants, and then discuss polynomial equations $f(x) = 0$, where $f(x)$ is of degree 2,3,4.

56.1 Lemma: Let $K$ be a field and $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, $g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$ be nonzero polynomials in $K[x] \setminus \{0\}$. Assume that at least one of $a_n, b_m$ is distinct from 0. Then $f(x), g(x)$ have a nonunit greatest common divisor in $K[x]$ if and only if there are nonzero polynomials $g_1(x), f_1(x) \in K[x]$ such that

$$f(x)g_1(x) = g(x)f_1(x) \quad \text{and} \quad \deg f_1(x) < n, \deg g_1(x) < m.$$ 

Proof: One direction is clear. If $f(x)$ and $g(x)$ have a nonunit greatest common divisor $h(x)$ in $K[x]$, then $f(x) = h(x)f_1(x)$, $g(x) = h(x)g_1(x)$ with some suitable $f_1(x), g_1(x)$ in $K[x]$ and

$$\deg f_1(x) = \deg f(x) - \deg h(x) \leq n - \deg h(x) < n$$

since $\deg h(x)$ is greater than zero. Likewise $\deg g_1(x) < m$. We have of course $f(x)g_1(x) = f_1(x)h(x)g_1(x) = f_1(x)g(x)$.

Conversely, assume $f(x)g_1(x) = g(x)f_1(x)$ for some nonzero polynomials $f_1(x), g_1(x)$ in $K[x]$ satisfying $\deg f_1(x) < n$ and $\deg g_1(x) < m$. We put $h(x) = (f(x), g(x))$. We want to prove $\deg h(x) > 0$. Write $f(x) = h(x)F(x)$, $g(x) = h(x)G(x)$. Then $(F(x), G(x)) \sim 1$ and $f(x)g_1(x) = g(x)f_1(x)$ gives $F(x)g_1(x) = G(x)f_1(x)$. Suppose, without loss of generality, $a_n \neq 0$, so that $\deg f(x) = n$. Now $F(x)$ divides $G(x)f_1(x)$ and, as $(F(x), G(x)) \sim 1$, $F(x)$ divides $f_1(x)$; thus $\deg F(x) \leq \deg f_1(x) < n = \deg f(x) = \deg F(x) + \deg h(x)$ and we get $\deg h(x) > 0$. This completes the proof.

Let $K$ be a field and

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$$
two polynomials in \( K[x] \), where \( a_n \neq 0 \) or \( b_n \neq 0 \), so that \( \deg f(x) = n \) or \( \deg g(x) = m \). From Lemma 56.1, we know that \( f(x) \) and \( g(x) \) have a nonunit greatest common divisor in \( K[x] \) if and only if there are elements \( c_{m-1}c_{m-2} \cdots c_1c_0, d_{n-1}d_{n-2} \cdots d_1d_0 \), where at least one \( c_i \neq 0 \) and at least one \( d_j \neq 0 \), such that

\[
(a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0)(c_{m-1}x^{m-1} + c_{m-2}x^{m-2} + \cdots + c_1x + c_0) = (b_mx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0)(d_{n-1}x^{n-1} + d_{n-2}x^{n-2} + \cdots + d_1x + d_0). \quad (*)
\]

This polynomial equation is equivalent to the system of equations:

\[
\begin{align*}
    a_n c_{m-1} &= b_m d_{n-1} \\
    a_n c_{m-2} + a_{n-1} c_{m-1} &= b_m d_{n-2} + b_{m-1} d_{n-1} \\
    a_n c_{m-3} + a_{n-1} c_{m-2} + a_{n-2} c_{m-1} &= b_m d_{n-3} + b_{m-1} d_{n-2} + b_{m-2} d_{n-1} \\
    &\vdots \\
    a_1 c_0 + a_0 c_1 &= b_1 d_0 + b_0 d_1 \\
    a_0 c_0 &= b_0 d_0.
\end{align*}
\]

This system can be written as

\[
\begin{align*}
    a_n c_{m-1} &= -b_m d_{n-1} = 0 \\
    a_n c_{m-2} + a_{n-1} c_{m-1} &= -b_m d_{n-2} - b_{m-1} d_{n-1} = 0 \\
    a_n c_{m-3} + a_{n-1} c_{m-2} + a_{n-2} c_{m-1} &= -b_m d_{n-3} - b_{m-1} d_{n-2} - b_{m-2} d_{n-1} = 0 \\
    &\vdots \\
    a_1 c_0 + a_0 c_1 &= -b_1 d_0 - b_0 d_1 = 0 \\
    a_0 c_0 &= -b_0 d_0 = 0
\end{align*}
\]

or as

\[
\begin{align*}
    a_n c_{m-1} &= -b_m d_{n-1} = 0 \\
    a_n c_{m-2} + a_{n-1} c_{m-2} &= -b_{m-1} d_{n-1} - b_m d_{n-2} = 0 \\
    a_n c_{m-3} + a_{n-1} c_{m-2} + a_{n-2} c_{m-3} &= -b_{m-2} d_{n-1} - b_{m-1} d_{n-2} - b_m d_{n-3} = 0 \\
    &\vdots \\
    a_1 c_0 + a_0 c_2 + a_2 c_3 &= 0 \\
    a_0 c_1 + a_1 c_2 + a_2 c_3 &= 0 \\
    a_0 c_0 &= 0
\end{align*}
\]

\[
\begin{align*}
    a_1 c_0 + a_0 c_1 &= -b_1 d_0 - b_0 d_1 = 0 \\
    a_0 c_0 &= -b_0 d_0 = 0
\end{align*}
\]

701
We write this system in matrix form:

\[
\begin{array}{cccccccc}
  a_n & 0 & 0 & \ldots & 0 & b_m & 0 & 0 & \ldots & 0 & c_{m-1} = 0 \\
  a_{n-1} & a_n & 0 & \ldots & 0 & b_{m-1} & b_m & 0 & \ldots & 0 & c_{m-2} = 0 \\
  a_{n-2} & a_{n-1} & a_n & \ldots & 0 & b_{m-2} & b_{m-1} & b_m & \ldots & 0 & c_{m-3} = 0 \\
  \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
  0 & 0 & 0 & \ldots & a_0 & 0 & 0 & 0 & \ldots & b_0 & -d_0 = 0
\end{array}
\]

Let \( A \) denote the matrix of this system. Then the polynomials \( f(x), g(x) \) have a nonunit greatest common divisor if and only if the matrix equation \( AX = 0 \) has a solution

\[
X = (c_{m-1}, c_{m-2}, c_{m-3}, \ldots, c_1, c_0, -d_{n-1}, -d_{n-2}, -d_{n-3}, \ldots, -d_1, -d_0)^t
\]

in which at least one \( c_i \neq 0 \) and at least one \( d_j \neq 0 \). From the equation (*) and the fact that \( K[x] \) has no zero divisors, we deduce that, in a solution \( X = (c_{m-1}, \ldots, -d_0)^t \) of \( AX = 0 \), there is at least one \( c_i \neq 0 \) if and only if there is at least one \( d_j \neq 0 \). Thus the polynomials \( f(x), g(x) \) have a nonunit greatest common divisor if and only if the matrix equation \( AX = 0 \) has a nontrivial solution. This is the case if and only if \( \text{det} \ A = 0 \) (Theorem 45.3). Since \( \text{det} \ A = \text{det} \ A^t \), we get that \( f(x), g(x) \) have a nonunit greatest common divisor if and only if \( \text{det} \ A^t = 0 \). We proved the

56.2 Theorem: Let \( K \) be a field and \( f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \),
\( g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0 \) be polynomials in \( K[x] \setminus K \), where at least one of \( a_n b_m \) is distinct from 0. Then \( f(x) \) and \( g(x) \) have a nonunit greatest common divisor in \( K[x] \) if and only if the determinant

\[
\begin{array}{cccccccc}
  a_n & a_{n-1} & \cdots & a_1 & a_0 & 0 & 0 & 0 & 0 \\
  0 & a_n & a_{n-1} & \cdots & a_1 & a_0 & 0 & 0 & 0 \\
  0 & 0 & a_n & a_{n-1} & \cdots & a_1 & a_0 & 0 & 0 \\
  \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
  0 & 0 & 0 & \cdots & a_n & a_{n-1} & \cdots & a_1 & a_0 \\
  b_m & b_{m-1} & \cdots & b_1 & b_0 & 0 & 0 & 0 & 0 \\
  0 & b_m & b_{m-1} & \cdots & b_1 & b_0 & 0 & 0 & 0 \\
\end{array}
\]
\[
\begin{pmatrix}
0 & 0 & b_m & b_{m-1} & \ldots & b_1 & b_0 & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \ldots & b_m & b_{m-1} & \ldots & b_1 & b_0
\end{pmatrix}
\]

is equal to zero.

56.3 Definition: Let \( K \) be a field and \( f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \), \( g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0 \) polynomials in \( K[x] \). The determinant

\[
\begin{vmatrix}
a_n & a_{n-1} & \cdots & a_1 & a_0 \\
a_n & a_{n-1} & \cdots & a_1 & a_0 \\
a_n & a_{n-1} & \cdots & a_1 & a_0 \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
b_m & b_{m-1} & \cdots & b_1 & b_0 \\
b_m & b_{m-1} & \cdots & b_1 & b_0 \\
b_m & b_{m-1} & \cdots & b_1 & b_0 \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
b_m & b_{m-1} & \cdots & b_1 & b_0
\end{vmatrix}
\]

(empty places are to be filled with zeroes) is called the resultant of \( f(x) \) and \( g(x) \), and is denoted by \( R(f,g) \) or by \( R(f(x),g(x)) \).

56.4 Remark: Notice that \( a_n \) and \( b_m \) can be zero in Definition 56.3. There is ambiguity in this definition and notation: the resultant depends not only on \( f(x) \) and \( g(x) \), but also on the number of apparent coefficients, a point neglected in almost every book. For example, let \( f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \) and \( g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0 \) again, and let \( b_{m+1} = 0 \), \( h(x) = b_{m+1} x^{m+1} + b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0 \). Then of course \( g(x) = h(x) \) but \( R(f,h) \) has one more column than \( R(f,g) \) and the expansion of \( R(f,h) \) along the first column gives \( R(f,h) = a_n R(f,g) \), so \( R(f,h) \neq R(f,g) \) (unless \( a_n = 1 \) or \( R(f,g) = 0 \)). Thus adding an initial term to \( g(x) \) with coefficient 0 changes \( R(f,g) \) to \( a_n R(f,g) \). Consequently, if

\[
f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \\
g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0 \quad \text{and} \quad b_m = b_{m-1} = \cdots = b_{k+1} = 0, \quad b_k \neq 0, \\
G(x) = b_k x^k + b_{k-1} x^{k-1} + \cdots + b_1 x + b_0,
\]

703
then \( g(x) \) is obtained from \( G(x) \) by adding \( m - k \) initial terms \( b_m x^m, b_{m-1} x^{m-1}, \ldots, b_{k+1} x^k \) with coefficient 0 and so \( R(f,g) = a_n^{m-k} R(f,G) \).

Definition 56.3 gives a new formulation of Theorem 56.2

**56.2 Theorem:** Let \( K \) be a field and \( f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \), \( g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0 \) be polynomials in \( K[x] \), where at least one of \( a_n, b_m \) is distinct from 0. Then \( f(x) \) and \( g(x) \) have a nonunit greatest common divisor in \( K[x] \) if and only if \( R(f,g) = 0 \).

We give some product formulas for the resultant of two polynomials. These formulas make it evident that the resultant is 0 if and only if the polynomials have a nontrivial common factor.

**56.5 Theorem:** Let \( K \) be a field and \( u_1, u_2, \ldots, u_n, y_1, y_2, \ldots, y_m \) indeterminates over \( K \). Let \( a_n, b_m \) be nonzero elements of \( K \) and let \( x \) be an indeterminate over \( K \) distinct from all of \( u_1, u_2, \ldots, u_n, y_1, y_2, \ldots, y_m \). Let \( f(x) \) and \( g(x) \) be polynomials in \( K(u_1, u_2, \ldots, u_n, y_1, y_2, \ldots, y_m)[x] \) defined by
\[
\begin{align*}
f(x) &= a_n (x - u_1)(x - u_2)\cdots(x - u_n) \\
g(x) &= b_m (x - y_1)(x - y_2)\cdots(x - y_m).
\end{align*}
\]
Then the following hold.

1. \( R(f,g) \) is in \( P[a_n, u_1, u_2, \ldots, u_n, b_m, y_1, y_2, \ldots, y_m] \), where \( P \) is the prime subfield of \( K \).

2. \( R(f,g) = a_n b_m \prod_{i=1}^{n} \prod_{j=1}^{m} (u_i - y_j) \).

3. \( R(f,g) = a_n \prod_{i=1}^{n} g(u_i) \).

4. \( R(f,g) = (-1)^{mn} b_m \prod_{j=1}^{m} f(y_j) \).

**Proof:** We put
\[
f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,
\]
\[ g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0, \]

where \( a_i, b_j \in K(u_1, u_2, \ldots, u_n, y_1, y_2, \ldots, y_m). \) Thus \( R(f, g) \) is a determinant of a matrix whose entries are \( a_0 a_1 a_2, \ldots, a_n b_0 b_1 b_2, \ldots, b_m \) and 0. Hence the entries of the matrix are in \( P[a_0 a_1 a_2, \ldots, a_n b_0 b_1 b_2, \ldots, b_m] \) and the determinant \( R(f, g) \) itself is also in \( P[a_0 a_1 a_2, \ldots, a_n b_0 b_1 b_2, \ldots, b_m] \) (Remark 44.2(2)). Since each \( a_i / a_n \), aside from a sign, is an elementary symmetric polynomial in \( u_1, u_2, \ldots, u_n \), and since the coefficients of elementary symmetric polynomials are in the prime subfield \( P \), we get

\[ a_i / a_n \in P[u_1, u_2, \ldots, u_n] \text{ for all } i = 1, 2, \ldots, n. \]

So each \( a_i \) is in \( P[a_n u_1 u_2, \ldots, u_n] \subseteq P[a_n u_1 u_2, \ldots, u_n, b_m y_1 y_2, \ldots, y_m] \). Likewise each \( b_j \) is in \( P[a_n u_1 u_2, \ldots, u_n, b_m y_1 y_2, \ldots, y_m]. \) Consequently \( R(f, g) \in P[a_0 a_1 a_2, \ldots, a_n b_0 b_1 b_2, \ldots, b_m] \subseteq P[a_n u_1 u_2, \ldots, u_n, b_m y_1 y_2, \ldots, y_m] \).

This proves (1). Now let \( L = P[a_n u_1 u_2, \ldots, u_n, b_m y_1 y_2, \ldots, y_m] \). We put

\[ S = a_n m m \prod_{i=1}^{n} \prod_{j=1}^{m} (u_i - y_j) \in L. \]

We have

\[ g(x) = b_m \prod_{j=1}^{m} (x - y_j), \]

\[ g(u_i) = b_m \prod_{j=1}^{m} (u_j - y), \]

\[ \prod_{i=1}^{n} g(u_i) = b_m n \prod_{i=1}^{n} \prod_{j=1}^{m} (u_i - y_j). \]

and thus

\[ S = a_n m \prod_{i=1}^{n} g(u_i). \] (i)

In like manner, from \( f(x) = a_n \prod_{i=1}^{n} (x - u_i) = (-1)^n a_n \prod_{i=1}^{n} (u_i - x) \), we get

\[ f(y_j) = (-1)^n a_n \prod_{i=1}^{n} (u_i - y_j), \]

\[ \prod_{j=1}^{m} f(y_j) = \prod_{j=1}^{m} (-1)^n a_n \prod_{i=1}^{n} (u_i - y_j), \]

\[ \prod_{j=1}^{m} f(y_j) = (-1)^{mn} a_n m \prod_{i=1}^{n} \prod_{j=1}^{m} (u_i - y_j). \]
\[ S = (-1)^{nm} \prod_{m} f(y_j). \] (ii)

Now let \( f_0(x) \) be the polynomial obtained by substituting \( y_j \) for \( u_i \) in \( f(x) \). Thus
\[ f_0(x) = a_n(x - u_1) \ldots (x - u_{i-1})(x - y_j)(x - u_{i+1}) \ldots (x - u_n) \]
\[ \in P(a_n, \ldots, u_{i-1}, u_{i+1}, \ldots, u_n, b_m y_1, y_2, \ldots, y_m)[x]. \]

Then the polynomials \( f_0(x) \) and \( g(x) \) in
\[ P(a_n u_1, \ldots, u_{i-1} u_{i+1}, \ldots, u_n b_m y_1, y_2, \ldots, y_m)[x] \]
have a common factor \( x - y_j \) and therefore \( R(f_0 g) = 0 \).

Thus \( R(fg) \in L \), regarded as a polynomial in
\[ P[a_n u_1, \ldots, u_{i-1} u_{i+1}, \ldots, u_n b_m y_1, y_2, \ldots, y_m][u_i] \]
has the value \( R(f_0 g) = 0 \) when \( y_j \) is substituted \( u_i \). So \( R(fg) \) has the root \( y_j \). So \( u_i - y_j \) divides \( R(fg) \) in
\[ P[a_n u_1, \ldots, u_{i-1} u_{i+1}, \ldots, u_n b_m y_1, y_2, \ldots, y_m][u_i] = L. \]

This is true for all \( i = 1, 2, \ldots, n \) and for all \( j = 1, 2, \ldots, m \). Since any \( u_i - y_j \) is irreducible in \( L \), and \( u_i - y_j \) is distinct from \( u_i - y_j \) whenever \( (i,j) \neq (i',j') \), the polynomials \( u_i - y_j \) are pairwise relatively prime. Thus \( R(fg) \) is divisible, in \( L \), by their product
\[ \prod_{i=1}^{n} \prod_{j=1}^{m} (u_i - y_j). \]

It follows that \( R(fg) \) is divisible by
\[ S = a_n^m b_m^m \prod_{i=1}^{n} \prod_{j=1}^{m} (u_i - y_j) \]
in \( M[u_1, u_2, \ldots, u_n, y_1, y_2, \ldots, y_m] \), where we put \( M = P(a_n, b_m). \)

Let us write \( H = R(fg)/S. \) Basically, we will argue that \( R(fg) \) and \( S \) are both homogeneous (§35, Ex. 4) of the same degree and conclude that \( H \) is a constant. Comparison of a monomial appearing in these polynomials will yield that this constant must be equal to 1, whence \( R(fg) = S. \) The details are rather tedious.
From (i), we see that \( S/\alpha_n^m = \prod_{i=1} \gamma_i \)

\( = (b_1 a_1^m + \cdots)(b_2 a_2^m + \cdots)\ldots(b_n a_n^m + \cdots) \)

\( = b_n^m a_1^m \ldots a_n^m \in P[b_m, y_1, y_2, \ldots, y_m][a_1, a_2, \ldots, a_n] \)

is a symmetric polynomial in \( a_1, a_2, \ldots, a_n \) over \( P[b_m, y_1, y_2, \ldots, y_m] \) and hence there is a unique polynomial \( h_1 \) in \( n \) indeterminates over the integral domain \( P[b_m, y_1, y_2, \ldots, y_m] \) such that

\( S/\alpha_n^m = h_1 (-a_{n-1}/a_n, a_{n-2}/a_n, \ldots, z a_1/a_n, z a_0/a_n). \)

Let us recall that \( h_1 \) is obtained from \( S/\alpha_n^m \) by subtracting symmetric polynomials of the form

\( y_{\sigma_1}^{k_1} y_{\sigma_2}^{k_2} \cdots y_{\sigma_n}^{k_n}, \quad y \in P[b_m, y_1, y_2, \ldots, y_m] \)

where \( y u_1^{k_1} u_2^{k_2} \cdots u_{n-1}^{k_{n-1}} u_n^{k_n} \) are certain monomials appearing in \( S/\alpha_n^m \).

We have \( m \geq k_1 \) by Lemma 38.8(2) since the leading monomial of \( S/\alpha_n^m \) is \( b_n^m a_1^m \ldots a_n^m \). A symmetric polynomial of the form above gives rise to a term

\( y(-a_{n-1}/a_n)^{k_1} (a_{n-2}/a_n)^{k_2} \cdots (z a_1/a_n)^{k_{n-1}} (z a_0/a_n)^{k_n}, \)

which is \( (1/a_n)^{k_1} \) times a polynomial in \( P[b_m, y_1, y_2, \ldots, y_m][a_0, a_1, \ldots, a_{n-1}] \). As \( m \geq k_1 \) for each of the terms in \( h_1 \), we see \( \alpha_n^m h_1 \) is a polynomial in \( P[b_m, y_1, y_2, \ldots, y_m][a_0, a_1, \ldots, a_{n-1}, a_n] \). Thus

\( S = (\alpha_n^m)(S/\alpha_n^m) = \alpha_n^m h_1 (-a_{n-1}/a_n, a_{n-2}/a_n, \ldots, z a_1/a_n, z a_0/a_n), \)

\[ S \in P[b_m, y_1, y_2, \ldots, y_m][a_0, a_1, \ldots, a_{n-1}, a_n] \]

and \( S = h(a_0, a_1, \ldots, a_{n-1}, a_n) \), where \( h \) is a polynomial in \( n + 1 \) indeterminates over \( P[b_m, y_1, y_2, y_m] \) (Lemma 49.5(1)).

Also

\( R(f, g) \in P[b_0, b_1, b_2, \ldots, b_n][a_0, a_1, a_2, \ldots, a_n] \)

\( \subseteq P[b_m, y_1, y_2, \ldots, y_m][a_0, a_1, \ldots, a_{n-1}, a_n] \)

and, together with (iii), we obtain

\( H = R(f, g)/S \in P[b_m, y_1, y_2, \ldots, y_m][a_0, a_1, \ldots, a_{n-1}, a_n] \).

707
Thus \( H \in M[y_1, y_2, \ldots, y_m][u_1, u_2, \ldots, u_n] \) is symmetric in \( u_1, u_2, \ldots, u_n \) and therefore
\[
H = k(-a_{n-1}/a_n, a_{n-2}/a_n, \ldots, a_1/a_n, a_0/a_n)
\]
for some polynomial \( k \) in \( n \) indeterminates over \( M[b_m, y_1, y_2, \ldots, y_m] \), which gives \( H \in M[b_m, y_1, y_2, \ldots, y_m][a_0, a_1, \ldots, a_{n-1}, a_n] \) (Lemma 49.5(1)).

Now \( H = R(f, g)/S = R(f, g)/h(a_0, a_1, \ldots, a_{n-1}, a_n) \). Note that multiplying the coefficients \( a_n a_{n-1}, \ldots, a_1 a_0 \) of \( f(x) \) by an indeterminate \( t \) does not change the roots \( u_1, u_2, \ldots, u_n \) of \( f(x) \), but, in view of (i), changes \( S \) to \( t^m S \), so that
\[
h(ta_n, ta_{n-1}, \ldots, ta_1, ta_0) = t^m h(a_n, a_{n-1}, \ldots, a_1, a_0).
\]

Likewise multiplying the coefficients \( a_n, a_{n-1}, \ldots, a_1, a_0 \) of \( f(x) \) by an indeterminate \( t \) changes \( R(f, g) \) to \( t^m R(f, g) \), as the determinant \( R(f, g) \) has \( m \) rows consisting of zeroes and the coefficients of \( f \). Thus \( H \) does not change when the coefficients of \( f \) are multiplied by \( t \). But any monomial
\[
y^{a_0}k_0 a_1 k_1 \cdots a_n k_n \quad (y \in M[b_m, y_1, y_2, \ldots, y_m])
\]
changes then to \( y(ta_0)^{k_0}(ta_1)^{k_1} \cdots (ta_n)^{k_n} = t^{k_0 + k_1 + \cdots + k_n} y^{a_0 k_0 a_1 k_1 \cdots a_n k_n} \). Thus the exponent system of any monomial \( y^{a_0 k_0 a_1 k_1 \cdots a_n k_n} \) appearing in \( H \) is such that \( k_0 + k_1 + \cdots + k_n = 0 \). This means \( k_0 = k_1 = \cdots = k_n = 0 \) for all monomials \( y^{a_0 k_0 a_1 k_1 \cdots a_n k_n} \) appearing in \( H \) and \( H \) is a "constant", i.e., \( H \) is in \( M[b_m, y_1, y_2, \ldots, y_m] \).

Repeating the same argument with \( S/B_m^n \) in place of \( S/a_n^m \), we get that \( H \) is in \( M[a_n, u_1, u_2, \ldots, u_n] \). So \( H \in M = P(a_n, b_m) \subseteq K \).

Thus \( R(f, g) = HS \) for some \( H \in K \). The constant term in \( S = a_n^m \prod_{i=1}^m g(u_i) \) is equal to \( a_n^m B_0^m \). So \( R(f, g) \) must have a term \( H a_n^m B_0^m \). Now \( R(f, g) \) has the term \( a_n^m B_0^m \), the product of the entries in the principal diagonal. Hence \( H = 1 \) and \( R(f, g) = S \). This proves (2). From (i) and (ii), we get the equations in (3) and (4). \( \square \)

56.6 Lemma: Let \( K \) be a field and \( f(x), g(x) \) polynomials of positive degree in \( K[x] \), say \( \deg f(x) = n \) and \( \deg g(x) = m \). Let \( a_n \) be the leading
Let $r_1, r_2, \ldots, r_n$ be roots of $f(x)$ and $s_1, s_2, \ldots, s_m$ roots of $g(x)$ in a splitting field of $f(x)g(x)$ over $K$. Then

$$R(f, g) = a_n^m b_m^n \prod_{i=1}^n \prod_{j=1}^m (r_i - s_j) = a_n^m \prod_{i=1}^n g(r_i) = (-1)^m b_m^n \prod_{j=1}^m f(s_j).$$

**Proof:** In a splitting field of $f(x)g(x)$ over $K$, we have the factorizations

$$f(x) = a_n(x - r_1)(x - r_2)\ldots(x - r_n),$$

$$g(x) = b_m(x - s_1)(x - s_2)\ldots(x - s_m).$$

Thus $f(x)$ and $g(x)$ are obtained from

$$F(x) = a_n(x - u_1)(x - u_2)\ldots(x - u_n),$$

$$G(x) = b_m(x - y_1)(x - y_2)\ldots(x - y_m),$$

where $u_1, u_2, \ldots, u_n, y_1, y_2, \ldots, y_m$ are indeterminates over $K$, by substituting $r_i$ for $u_i$ and $s_j$ for $y_j$. Since

$$R(F, G) = a_n^m b_m^n \prod_{i=1}^n \prod_{j=1}^m (u_i - y_j) = a_n^m \prod_{i=1}^n g(u_i) = (-1)^m b_m^n \prod_{j=1}^m f(y_j)$$

by Theorem 56.5, this substitution gives

$$R(f, g) = a_n^m b_m^n \prod_{i=1}^n \prod_{j=1}^m (r_i - s_j) = a_n^m \prod_{i=1}^n g(r_i) = (-1)^m b_m^n \prod_{j=1}^m f(s_j).$$


**56.7 Lemma:** Let $K$ be a field. Let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

be a polynomial of degree $n$ in $K[x]\setminus K$ and

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$$

a polynomial in $K[x]\setminus K$, possibly $b_m = 0$. Let $r_1, r_2, \ldots, r_n$ be the roots of $f(x)$ in some splitting field of $f(x)$ over $K$. Then

$$R(f, g) = a_n^m \prod_{i=1}^n g(r_i).$$

**Proof:** Assume first $b_m \neq 0$. Let $F$ be a splitting field of $f(x)$ over $K$ in which $r_1, r_2, \ldots, r_n$ lie and let $E$ be a splitting field of $g(x)$ over $F$ so that both $f(x)$ and $g(x)$ split completely in $E$. Then $R(f, g) = a_n^m \prod_{i=1}^n g(r_i)$ by Lemma 56.6.

Assume now $b_m = 0$ and let $k$ be the largest index for which $b_k \neq 0$. Thus

$$b_m = b_{m-1} = \cdots = b_{k+1} = 0$$

and $b_k \neq 0$. We put $G(x) = b_k x^k + b_{k-1} x^{k-1} + \cdots +
We get \( R(f,g) = a_n^{m-k}R(f,G) \) from Remark 56.4 and we have \( R(f,G) = a_n^k \prod_i G(r_i) \) by what we have just proved. Since \( G(r_i) = g(r_i) \) for any \( i = 1,2, \ldots , n \), we obtain
\[
R(f,g) = a_n^{m-k}R(f,G) = a_n^k \prod_i G(r_i) = a_n^m \prod_i g(r_i).
\]
This completes the proof. \( \square \)

56.8 Definition: Let \( K \) be a field and \( f(x) \) a nonzero polynomial in \( K[x] \) of positive degree \( n \). Let \( a_n \) be the leading coefficient of \( f(x) \) and let \( r_1, r_2, \ldots , r_n \) be the roots of \( f(x) \) in some splitting field \( E \) of \( f(x) \) over \( K \). Then
\[
a_n^{2n-2} \prod_{i \neq j} (r_i - r_j)^2 \in E
\]
is called the discriminant of \( f(x) \) and is denoted by \( D(f) \).

It seems as though the discriminant of \( f(x) \) depended on the splitting field \( E \) we choose and we had to call it actually the discriminant of \( f(x) \) in \( E \) and denoted by \( D_E(f) \). However, there is no need to refer to the splitting field since the discriminant is in fact an element of the field \( K \). This we prove in the next theorem.

In the next theorem, if \( f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \) and \( f'(x) = na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1 \), then \( R(f,f') \) is understood to be the determinant with \( n + (n-1) \) rows, the first \( n-1 \) rows being
\[
a_n a_{n-1} \cdots a_1 a_0
\]
surrounded with zeroes and the last \( n \) being
\[
na_n (n-1)a_{n-1} \cdots a_1
\]
surrounded with zeroes, even if \( na_n = 0, (n-1)a_{n-1} = 0 \), etc. (this happens when \( \text{char } K = p \neq 0 \) and \( p|n, a_{n-1} = 0, \text{ etc.} \)). In other words, we define \( R(f,f') \) as if \( f' \) is of degree \( n - 1 \), although the degree of \( f' \) may be less than \( n - 1 \) (cf. Remark 56.4).
56.9 Theorem: Let $K$ be a field and $f(x)$ a polynomial of positive degree $n$ and let $a_n$ be the leading coefficient of $f(x)$. Then the discriminant $D(f)$ of $f(x)$ is in $K$. In fact, $R(f, f^r) = (-1)^{n(n-1)/2}a_nD(f)$.

Proof: Let $E$ be a splitting field of $f(x)$ over $K$ and let $r_1, r_2, \ldots, r_n$ be the roots of $f(x)$ in $E$. We evaluate $R(f, f^r)$. We have $R(f, f^r) = a_n^{n-1}\prod_{i=1}^{n} f^r(r_i)$ by Lemma 56.7. We must find $f^r(r_i)$. From $f(x) = a_n(x - r_1)(x - r_2)\ldots(x - r_n)$, we get

$$f^r(x) = \sum_{j=1}^{n} a_n (x - r_1)\ldots(x - r_{j-1})(x - r_{j+1})\ldots(x - r_n)$$

so

$$f^r(r_i) = a_n (r_i - r_1)\ldots(r_i - r_{i-1})(r_i - r_{i+1})\ldots(r_i - r_n) = a_n \prod_{j=1 \atop j \neq i}^{n} (r_i - r_j).$$

Thus $R(f, f^r) = a_n^{n-1}\prod_{i=1}^{n} f^r(r_i) = a_n^{n-1}\prod_{i=1}^{n} (a_n \prod_{j=1 \atop j \neq i}^{n} (r_i - r_j)) = a_n^{2n-1} \prod_{i \neq j}^{n} (r_i - r_j)$

$$= a_n a_n^{2n-2} \prod_{i \neq j} (r_i - r_j) = a_n a_n^{2n-2} \prod_{i < j} (r_i - r_j) \prod_{j < i} (r_i - r_j)$$

$$= a_n a_n^{2n-2} \prod_{i < j} (r_i - r_j) \prod_{i < j} (-1)(r_j - r_i)$$

$$= a_n a_n^{2n-2} \prod_{i < j} (r_i - r_j) \prod_{i < j} (-1)(r_i - r_j)$$

$$= (-1)^{n(n-1)/2}a_n a_n^{2n-2} \prod_{i < j} (r_i - r_j)^2 = (-1)^{n(n-1)/2}a_nD(f).$$

\[\Box\]

56.10 Examples: (a) Let $K$ be a field and $ax^2 + bx + c \in K[x]$, with $a \neq 0$. The discriminant of $f(x)$ is $(-1)a^{-1}$ times the resultant

\[
\begin{vmatrix}
a & b & c \\
2a & b & 0 \\
0 & 2a & b \\
\end{vmatrix}
\begin{vmatrix}
a & b & c \\
0 & -b & -2c \\
0 & 2a & b \\
\end{vmatrix}
= \begin{vmatrix}
a & -b & -2c \\
0 & 2 & b \\
\end{vmatrix}
= a\begin{vmatrix}
-b & 2 \\
0 & b \\
\end{vmatrix}
= a(-b^2 + 4ac) = -a(b^2 - 4ac),
\]

711
hence the discriminant of \( f(x) \) is \( b^2 - 4ac \).

(b) Let \( K \) be a field and \( x^3 + px + q \in K[x] \). The discriminant of \( f(x) \) is 
\[ (-1)^{3/2} \frac{1}{1^1} \times \text{the resultant} \]

\[
\begin{vmatrix}
1 & 0 & p & q & 0 \\
0 & 1 & 0 & p & q \\
3 & 0 & p & 0 & 0 \\
0 & 3 & 0 & p & 0 \\
0 & 0 & 3 & 0 & p \\
\end{vmatrix} = \begin{vmatrix}
1 & 0 & p & q \\
0 & 1 & 0 & p & q \\
0 & 0 & -2p & -3q & 0 \\
0 & 3 & 0 & p & 0 \\
0 & 0 & 3 & 0 & p \\
\end{vmatrix} = \begin{vmatrix}
1 & 0 & p & q \\
0 & -2p & -3q & 0 \\
0 & 3 & 0 & p \\
0 & 0 & 3 & 0 & p \\
\end{vmatrix} = 4p^3 + 27q^2.
\]

So the discriminant of \( f(x) \) is equal to \(-4p^3 - 27q^2\).

We now turn our attention to polynomial equations.

56.11 Lemma: (1) Let \( E/K, E_1/K_1 \) be field extensions. Assume that there are field isomorphisms \( \varphi: K \to K_1 \) and \( \psi: E \to E_1 \) and that \( \psi \) is an extension of \( \varphi \). Then \( \text{Aut}_K E \cong \text{Aut}_{K_1} E_1 \).

(2) Let \( K \) be a field and \( f(x) \) a polynomial in \( K[x]\). Let \( E \) and \( F \) be two splitting fields of \( f(x) \) over \( K \). Then \( \text{Aut}_K E \cong \text{Aut}_K F \).

Proof: (1) For any \( \sigma \in \text{Aut}_K E \), consider the mapping \( \psi^{-1} \sigma \psi : E_1 \to E_1 \). Clearly \( \psi^{-1} \sigma \psi \) is a field isomorphism (Lemma 48.10). Moreover, for any \( a_1 \in K_1 \), there is a unique \( a \in K \) with \( a \psi = a \varphi = a_1 \), i.e., \( a \psi^{-1} = a_1 \psi^{-1} = a \) and \( a \psi^{-1} \sigma \psi = (a_1 \psi^{-1}) \sigma \psi = (a) \sigma \psi = (a_\sigma) \psi = a \psi = a_1 \), so \( \psi^{-1} \sigma \psi \) is in fact a \( K_1 \)-automorphism of \( E_1 \). Thus we have a mapping

\[
A: \text{Aut}_K E \to \text{Aut}_{K_1} E_1 \\
\sigma \mapsto \psi^{-1} \sigma \psi
\]

Now \( (\sigma \tau) A = \psi^{-1} (\sigma \tau) \psi = (\psi^{-1} \sigma \psi)(\psi^{-1} \tau \psi) = \sigma A \tau A \) for any \( \sigma, \tau \in \text{Aut}_K E \), so \( A \) is a group homomorphism. Repeating the same argument with \( K, E, \varphi, \psi \) and \( K_1, E_1, \psi^{-1}, \psi^{-1} \) interchanged, we conclude that the mapping
$B: \text{Aut}_{K_1} E_1 \rightarrow \text{Aut}_K E$

$\theta \rightarrow \psi \theta \psi^{-1}$

is an inverse of A, so A is one-to-one and onto $\text{Aut}_{K_1} E_1$. Thus A is an isomorphism and we get $\text{Aut}_K E \cong \text{Aut}_{K_1} E_1$.

(2) The fields $E$ and $F$ are $K$-isomorphic by Theorem 53.8, so the claim follows immediately from part (1).

Thus Galois groups of any two splitting fields (over $K$) of $f(x)$ are isomorphic. This justifies the definite article in the next definition.

56.12 Definition: Let $K$ be a field and $f(x)$ a polynomial in $K[x]\setminus K$. The Galois group $\text{Aut}_K E$ of a splitting field $E$ of $f(x)$ over $K$ is called the Galois group of $f(x) \in K[x]$.

56.13 Examples: (a) $\mathbb{Q}(i)$ is a splitting field of $x^2 + 1 \in \mathbb{Q}[x]$ over $\mathbb{Q}$ and hence the Galois group of $x^2 + 1 \in \mathbb{Q}[x]$ is $\text{Aut}_{\mathbb{Q}} \mathbb{Q}(i) \cong C_2$.

(b) The Galois group of $x^3 - 2$ is $\{\phi_1, \phi_2, \phi_3, \phi_4, \phi_5, \phi_6\} \cong S_3$. Here we used the notation of Example 54.18(a).

(c) The Galois group of $x^4 - 2$ is $\{\phi_1, \phi_2, \phi_3, \phi_4, \phi_5, \phi_6, \phi_7, \phi_8\} = <\sigma, \tau> \cong D_8$. Here we used the notation of Example 54.18(b). We know that $D_8 \cong \{1, (13), (24), (12)(34), (13)(24), (14)(23), (1234), (1432)\} \leq S_4$.

(d) Let $p$ be a prime number. The field $\mathbb{F}_p^x$ is a splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$ (Example 53.5(f)). Hence the Galois group of $x^{p^n} - x \in \mathbb{F}_p[x]$ is $\text{Aut}_{\mathbb{F}_p^x} \mathbb{F}_p[x] = <\sigma>$, where $\sigma$ is the homomorphism $a \rightarrow a^p$ (Example 54.18(c)).

56.14 Theorem: Let $K$ be a field, $f(x)$ a polynomial in $K[x]\setminus K$ and let $G$ be the Galois group of $f(x)$. Then $G$ is isomorphic to a subgroup of a symmetric group $S_n$. 713
**Proof:** Let $E$ be a splitting field of $f(x)$ over $K$ and let $a_1, a_2, \ldots, a_n$ be the distinct roots of $f(x)$ in $E$ ($1 \leq n \leq \deg f(x)$). Any $\varphi \in G = Aut_K E$ maps any $a_i$ to a $a_j$ and thus gives rise to a permutation $\sigma_\varphi \in S_n$, namely $i \rightarrow j$. Thus $\sigma_\varphi$ is given by $a_i \varphi \rightarrow a_i \sigma_\varphi$.

Now the mapping $\sigma: G \rightarrow S_n$ is a homomorphism of groups since, for any $\varphi, \psi \in G$, we have

$$a_{i \sigma_\varphi \psi} = a_{i(\varphi \psi)} = (a_i \varphi) \psi = a_i \psi \psi = a_i \varphi = a_{i \sigma_\psi} \psi \sigma_\psi = a_{i \sigma_\psi} \sigma_\psi$$

for $i = 1, 2, \ldots, n$ and so $\sigma_\varphi \sigma_\psi = \sigma_\varphi \sigma_\psi$. Here $\varphi \in Ker \sigma$ if and only if $a_i \varphi = a_i$ for all $i = 1, 2, \ldots, n$. Thus an automorphism in $Ker \sigma$ fixes each element of $K$ and fixes each $a_i$. Since $E$ is generated by $a_i$ over $K$ (Example 53.5(d)), we deduce that an automorphism in $Ker \sigma$ fixes all elements of $E$. Thus $Ker \sigma = \{1_E\}$. So $\sigma$ is one-to-one and $G$ is isomorphic to $Im \sigma \subseteq S_n$. \qed

The preceding proof is quite simple. $G$ acts on the set of distinct roots of $f(x)$, and the permutation representation $\sigma$ is one-to-one; thus $G$ is isomorphic to a subgroup of $S_U$, and $S_U$ itself is isomorphic to $S_n$. We will often identify the Galois group of a polynomial with its isomorphic images in $S_U$ and in $S_n$.

The Galois group of a polynomial reflects many important properties of that polynomial. We describe how irreducibility is reflected in the Galois group. It turns out that the decomposition of $f(x)$ into irreducible polynomials is intimately connected with the partitioning of its roots into disjoint orbits. Let us recall that a group $G$ is said to act transitively on a set $X$ provided, for any $x, y \in X$, there is a $g \in G$ such that $xg = y$ (Definition 25.11). If $G \subseteq S_n$ acts transitively on $\{1, 2, \ldots, n\}$, then we shall call $G$ a transitive subgroup of $S_n$. Thus $G \subseteq S_n$ is transitive if and only if, for any $i, j \in \{1, 2, \ldots, n\}$, there is a $\tau \in G$ such that $i\tau = j$.

**56.15 Examples:** (a) A subgroup $G$ of $S_n$ is transitive if and only if, for any $i \in \{1, 2, \ldots, n\}$, there is a $\sigma \in S_n$ such that $1\sigma = i$. The necessity of this condition is clear. Conversely, if the condition is satisfied and $i, j$ are in
{1,2,...,n}, there are \( \sigma, \tau \in G \) with \( 1\sigma = i \) and \( 1\tau = j \), so \( \sigma^{-1}\tau \in G \) maps \( i \) to \( j \); hence the condition is also sufficient.

**(b)** If \( H \leq G \leq S_n \) and \( H \) is transitive, then \( G \) is also transitive.

**(c)** \( A_3 = \langle \iota(123), (132) \rangle \) is a transitive subgroup of \( S_3 \) for there are permutations \( \sigma_i \) in \( A_3 \) with \( 1\sigma_i = i \) for any \( i = 1,2,3 \), viz. \( \sigma_1 = \iota, \sigma_2 = (123) \) and \( \sigma_3 = (132) \). Then \( S_3 \) is of course another transitive subgroup of \( S_3 \). On the other hand, \( \langle \iota(12) \rangle \) is not a transitive subgroup of \( S_3 \) for there is no permutation \( \sigma \) in \( \langle \iota(12) \rangle \) that maps 1 to 3. Likewise \( \langle \iota(13) \rangle \) and \( \langle \iota(23) \rangle \) are not transitive subgroups of \( S_3 \). Certainly \( \{1\} \) is not a transitive subgroup of \( S_3 \). Thus \( A_3 \) and \( S_3 \) are the only transitive subgroups of \( S_3 \).

**(d)** Let \( \sigma = (12...n) \in S_n \). Then \( \langle \sigma \rangle \) is a transitive subgroup of \( S_n \) since \( 1\sigma^i = i \) for any \( i = 1,2,...,n \).

**(e)** If \( G \) is a transitive subgroup of \( S_n \), so is any conjugate of \( G \). Indeed, if \( G \) is transitive and \( \tau \in S_n \), then, for any \( i,j \in \{1,2,...,n\} \), there is a \( \sigma \in G \) that maps \( i\tau^1 \) to \( j\tau^1 \), i.e., \( i\tau^1\sigma\tau = j \). Thus there is a \( \sigma^\tau \in G^\tau \) that maps \( i \) to \( j \) and \( G^\tau \) is therefore transitive.

**(f)** It follows from the last two examples that \( \langle (1234) \rangle \) and its conjugates \( \langle (1243) \rangle, \langle (1324) \rangle \) are transitive subgroups of \( S_4 \). Also \( V_4 = \langle \iota(12)(34),(13)(24),(14)(23) \rangle \) is a transitive subgroup of \( S_4 \). From \( V_4 \leq A_4 \) and \( V_4 \leq S_4 \), we see that \( A_4 \) and \( S_4 \) are transitive subgroups of \( S_4 \). Likewise \( D = \langle \iota(13),(24),(12)(34),(13)(24),(14)(23),(1234),(1432) \rangle \) and its conjugates

\[
\{ \iota(12),(34),(13)(24),(12)(34),(14)(32),(1234),(1423) \}
\]

\[
\{ \iota(14),(23),(12)(43),(14)(23),(13)(24),(1234),(1342) \}
\]

are transitive subgroups of \( S_4 \). On the other hand, \( \{ \iota(12),(34),(12)(34) \} \) and its conjugates are not transitive subgroups of \( S_4 \).

56.16 Theorem: Let \( K \) be a field and let \( f(x) \in K[x] \) be a monic polynomial having no multiple roots. Let \( E \) be a splitting field of \( f(x) \) and \( G = \text{Aut}_K E \) the Galois group of \( f(x) \). Let \( r_1, r_2, ..., r_n \in E \) be the roots of \( f(x) \). Let \( m_0 = 0 \) and \( m_k = n \).

1. Assume the notation so chosen that

\[
\{ r_{m_1}, r_{m_1+1}, ..., r_{m_2} \}, \{ r_{m_2+1}, r_{m_2+2}, ..., r_{m_3} \},
\]

715
are the disjoint orbits under the action of \( G \). Put

\[
 f_i(x) = (x - r_{m_i+1})(x - r_{m_i+2}) \ldots (x - r_m) \in E[x] \quad \text{for } i = 1, 2, \ldots, k.
\]

Then \( f_i(x) \in K[x] \) and \( f_i(x) \) is irreducible in \( K[x] \), so that

\[
 f(x) = f_1(x)f_2(x) \ldots f_k(x)
\]

is the canonical decomposition of \( f(x) \) into irreducible polynomials in \( K[x] \).

(2) Let \( f(x) = f_1(x)f_2(x) \ldots f_k(x) \) be the canonical decomposition of \( f(x) \) into monic irreducible polynomials in \( K[x] \) and let \( r_{m_i+1}, r_{m_i+2}, \ldots, r_m \) be the roots of \( f_i(x) \) \( (i = 1, 2, \ldots, k) \). Then

\[
 \{r_1, r_2, \ldots, r_n\} = \{r_1, r_2, \ldots, r_{m_1}\} \cup \{r_{m_1+1}, r_{m_1+2}, \ldots, r_{m_2}\} \cup \{r_{m_2+1}, r_{m_2+2}, \ldots, r_{m_3}\} \cup \ldots \cup \{r_{m_{i-1}+1}, r_{m_{i-1}+2}, \ldots, r_{m_i}\}
\]

is the partitioning of \( \{r_1, r_2, \ldots, r_n\} \) into disjoint orbits under the action of \( G \).

**Proof:** (1) We first prove that \( f_i(x) \in K[x] \). The coefficients of \( f_i(x) = (x - r_{m_i+1})(x - r_{m_i+2}) \ldots (x - r_m) \) are elementary symmetric polynomials in \( r_{m_i+1}, r_{m_i+2}, \ldots, r_m \). Any automorphism in \( G \) maps each one of these \( r_{m_i+1}, r_{m_i+2}, \ldots, r_m \) to one of them again and thus leaves the coefficients of \( f_i(x) \) unchanged. So the coefficients of \( f_i(x) \) are in the fixed field of \( G \). Now \( f(x) \) has no multiple roots, so the irreducible divisors of \( f(x) \) are separable over \( K \) and, since \( E \) is a splitting field of \( f(x) \) over \( K \), we infer \( E \) is a Galois extension of \( K \) (Theorem 55.7) and the fixed field of \( G \) is exactly \( K \). Hence \( f_i(x) \in K[x] \).

We prove next that \( f_i(x) \) is irreducible in \( K[x] \). Let \( g(x) \in K[x] \) be an irreducible divisor of \( f_i(x) \). In \( E \), there is a root of \( g(x) \), say \( r_{m_i+1} \). Then, for any \( \varphi \in G \), \( r_{m_i+1}\varphi \) is also a root of \( g(x) \). But \( \{r_{m_i+1}\varphi: \varphi \in G\} = \text{orbit of } r_{m_i+1} \) \( r_{m_i+1}, r_{m_i+2}, \ldots, r_m \). Thus, each of \( r_{m_i+1}, r_{m_i+2}, \ldots, r_m \) is a root of \( g(x) \). These roots are distinct, for \( f(x) \) has no multiple roots. Thus \( g(x) \) has at least \( m_i - m_{i-1} \) distinct roots. Then \( m_i - m_{i-1} \leq \deg g(x) \leq \deg f_i(x) = m_i - m_{i-1} \) and so \( g(x) = f_i(x) \). Thus \( f_i(x) = g(x) \) is irreducible in \( K[x] \).

It follows that \( f(x) = f_1(x)f_2(x) \ldots f_k(x) \) is the canonical decomposition of \( f(x) \) into irreducible polynomials in \( K[x] \).

(2) Suppose now \( f(x) = f_1(x)f_2(x) \ldots f_k(x) \) is the canonical decomposition of \( f(x) \) into irreducible polynomials in \( K[x] \). We are to show that the roots of
$f_i(x)$ make up the orbit of $r_{m_i+1}$. Indeed, if $\varphi \in G$, then $r_{m_i+1}\varphi$ is also a root of $f_i(x)$ and thus:

$$\text{orbit of } r_{m_i+1} \subseteq \{r_{m_i+1}, r_{m_i+2}, \ldots, r_m\}.$$ 

On the other hand, if $r \in E$ is any root of $f_i(x)$, then $K(r_{m_i+1}) \cong K(r)$ by a $K$-isomorphism $\psi$ that sends $r_{m_i+1}$ to $r$ (Theorem 53.2) and $\psi$ can be extended to a $K$-automorphism $\varphi$ (Theorem 53.7; $E$ is a splitting field of $f(x)$ over $K(r_{m_i+1})$ and over $K(r)$ by Example 53.5(e)). So there is a $\varphi \in G$ with $r_{m_i+1}\varphi = r$ and any root $r$ of $f_i(x)$ is in the orbit of $r_{m_i+1}$. Thus:

$$\{r_{m_i+1}, r_{m_i+2}, \ldots, r_m\} \subseteq \text{orbit of } r_{m_i+1}.$$ 

This completes the proof. \hfill \Box

56.17 Theorem: Let $K$ be a field, $f(x)$ a polynomial of positive degree $n$ in $K[x]$ and let $G$ be the Galois group of $f(x)$. If $f(x)$ is irreducible and separable over $K$, then $n$ divides $|G|$ and $G$ is isomorphic to a transitive subgroup of $S_n$.

**Proof:** Let $E$ be a splitting field of $f(x)$ over $K$. Then $E$ is a Galois extension of $K$ (Theorem 55.7) and, under the action of $G$, there is only one orbit of the roots of $f(x)$. Thus $G$ acts transitively on the set of roots of $f(x)$ and its isomorphic image in $S_n$ acts transitively on $\{1, 2, \ldots, n\}$. So $G$ is isomorphic to a transitive subgroup of $S_n$. Furthermore, if $r \in E$ is any root of $f(x)$, then $K(r)$ is an intermediate field of $E/K$ and $|K(r):K| = \deg f = n$ (Theorem 50.7) and, by the fundamental Theorem of Galois theory, $G$ has a subgroup $K(r)'$ of index $|G:K(r)'| = |K(r):K| = n$. So $n$ divides $|G|$ by Lagrange’s theorem. \hfill \Box

We shall regard the Galois group as a subgroup of $S_n$. It will be interesting to determine the role of $A_n$. This is connected with discriminants.

56.18 Theorem: Let $K$ be a field such that char $K \neq 2$ and let $f(x) \in K[x]$. Assume $\deg f = n > 0$ and let $E$ be a splitting field of $f(x)$ over $K$. Suppose $f(x)$ has $n$ distinct roots $r_1, r_2, \ldots, r_n$ in $E$. Put
\[ \delta = \prod_{i < j} (r_i - r_j) = (r_1 - r_2)(r_1 - r_3) \ldots (r_{n-1} - r_n) \text{ and } d = 8^2. \]

(1) For \( \varphi \in \text{Aut}_k E \subseteq S_n \), there holds \( \delta \varphi = \delta \) if and only if \( \varphi \) is in \( A_n \) and \( \delta \varphi = -\delta \) if and only if \( \varphi \) is in \( S_n \setminus A_n \).

(2) \( d \), which is an elements of \( E \), is actually in \( K \). In fact, \( d = a_n^{-2n-2}D(f) \), where \( a_n \) is the leading coefficient and \( D(f) \) is the discriminant of \( f(x) \).

**Proof:** (1) We have \( \delta \varphi = \prod_{i < j} (r_i - r_j) = (r_1 - r_2)(r_1 - r_3) \ldots (r_{n-1} - r_n) \), where \( r_i = r_{i\varphi} \). We divide the ordered pairs \((i,j)\) with \( i < j \) into two classes according as \( i' < j' \) or \( i' > j' \). Then \( \delta \varphi = \prod_{i < j} (r_i - r_j) \prod_{i' < j'} (r_i - r_{i'}) \)

\[ = \prod_{i < j} (r_i - r_j) \prod_{i' < j'} (-1)(r_{i'} - r_{i}) \]

\[ = \prod_{i < j} (r_i - r_j) \prod_{j < i} (-1)(r_{i'} - r_{i}) \quad \text{(interchange the dummy indices } i \text{ and } j \text{)} \]

\[ = \prod_{i < j} (r_i - r_j) \cdot (-1)^s \prod_{j < i} (r_{i'} - r_{i}) \quad \text{(where } s \text{ is the number of factors in} \]

\[ \text{the second product; hence } s \text{ is the} \]

\[ \text{number of inversions of the permutation } \left( \begin{array}{cccc}
1 & 2 & \ldots & n \\
1' & 2' & \ldots & n'
\end{array} \right) = \varphi \in \text{Aut}_k E \subseteq S_n \right) \]

\[ = (-1)^s \prod_{i < j} (r_i - r_j) \prod_{j < i} (r_{i'} - r_{i'}) = \mathbb{E}(\varphi) \prod_{i < j} (r_i - r_j) = \mathbb{E}(\varphi) \prod_{i < j} (r_i - r_j) = \mathbb{E}(\varphi) \delta. \]

This proves (1).

(2) The equation \( d = a_n^{-2n-2}D(f) \) is immediate from the definition of discriminant (Definition 56.8). This implies of course that \( d \) is in \( K \), since \( D(f) \), being \( a_n^{-1} \) times a determinant of a matrix with entries in \( K \), is an element of \( K \). Alternatively, we have \( \delta \varphi = \varphi \delta \) and thus \( d \varphi = (\delta^2) \varphi = (\delta \varphi)^2 = (\varphi \delta)^2 = \delta^2 = d \) for any \( \varphi \in \text{Aut}_k E \). So \( d \) is in the fixed field of \( \text{Aut}_k E \). Since the roots of \( f(x) \) are simple by hypothesis, the irreducible divisors of \( f(x) \)
are separable over \( K \) and thus \( E \) is Galois over \( K \) (Theorem 55.7), so the fixed field of \( \text{Aut}_K E \) is \( K \) and \( d \) is in \( K \). □

56.19 Theorem: Let \( K \) be a field such that \( \text{char} \ K \neq 2 \) and let \( f(x) \in K[x] \). Assume \( \deg f = n > 0 \) and let \( E \) be a splitting field of \( f(x) \) over \( K \). Suppose \( f(x) \) has \( n \) distinct roots \( r_1, r_2, \ldots, r_n \) in \( E \) so that \( E \) is a Galois extension of \( K \) (Theorem 55.7). Put \( \delta = \prod_{i<j}(r_i-r_j) \). Consider the Galois group \( \text{Aut}_K E \) as a subgroup of \( S_n \).

In the Galois correspondence, the intermediate field \( K(\delta) \) corresponds to \( \text{Aut}_K E \cap A_n \). In particular, \( \text{Aut}_K E \leq A_n \) if and only if \( \delta \in K \).

Proof: In the Galois correspondence, the subgroup of \( \text{Aut}_K E \) corresponding to the intermediate field \( K(\delta) \) is

\[
K(\delta)' = \{ \varphi \in \text{Aut}_K E : a\varphi = a \text{ for all } a \in K(\delta) \} \\
= \{ \varphi \in \text{Aut}_K E : \delta \varphi = \delta \} \\
= \{ \varphi \in \text{Aut}_K E : \varphi \in A_n \} \\
= \text{Aut}_K E \cap A_n
\]

by Theorem 56.18. In particular, \( \text{Aut}_K E \leq A_n \) if and only if \( \text{Aut}_K E \cap A_n = \text{Aut}_K E \), so if and only if \( K(\delta)' = \text{Aut}_K E = K' \), hence if and only if \( K(\delta) = K \), hence if and only if \( \delta \in K \). □

We now study Galois groups of polynomials of degree 2, 3, 4. We start with quadratic polynomials.

56.20 Theorem: Let \( K \) be a field and \( f(x) \) an irreducible polynomial in \( K[x] \) of degree 2. Let \( G \) be the Galois group of \( f(x) \), regarded as a subgroup of \( S_2 \). If \( f(x) \) is separable over \( K \), then \( G = S_2 \cong \mathbb{Z}_2 \). If \( f(x) \) is not separable over \( K \), then \( G = 1 \).

Proof: If \( f(x) \) is separable over \( K \), then \( G \) is a transitive subgroup of \( S_2 \) (Theorem 56.17). Since \( S_2 \) is the only transitive subgroup of \( S_2 \), the result follows. If \( f(x) = ax^2 + bx + c \) is not separable over \( K \), then \( f'(x) = 2ax + b = 0 \), so \( 2a = 0 = b \) (and \( a \neq 0 \)), so \( \text{char} \ K = 2 \) and \( f(x) = a(x^2 + e) \) for some \( e \in K \), and a splitting field of \( f(x) \) over \( K \) is \( K(r) \), where \( r \) is a root of \( f(x) \).
Then any $\phi$ in $G$ maps $r$ to $r$ and thus fixes $K(r)$. This means $G$ consists of the identity mapping on $K(u)$. Hence $G = 1$. □

56.21 Theorem: Let $K$ be a field and $f(x)$ an irreducible separable polynomial in $K[x]$ of degree 3. Let $G$ be the Galois group of $f(x)$, regarded as a subgroup of $S_3$. Then $G = S_3$ or $G = A_3$. More specifically, if $\text{char } K \neq 2$, then $G = A_3$ in case $D(f)$ is the square of an element in $K$, and $G = S_3$ in case $D(f)$ is not the square of any element in $K$.

Proof: $G$ is a transitive subgroup of $S_3$ (Theorem 56.17). Since $S_3$ and $A_3$ are the only transitive subgroups of $S_3$ (Example 56.15(c)), the result follows.

Assume in addition $\text{char } K \neq 2$. Then $G = A_3$ if and only if $\delta \in K$ in the notation of Theorem 56.19. Since $\delta^2 = a_3^{-4}D(f)$, where $a_3$ is the leading coefficient of $f(x)$ (Theorem 56.18), we conclude $G = A_3$ if and only if $a_3^{-4}D(f)$ is the square of an element in $K$, thus if and only if $D(f)$ is the square of an element in $K$. □

56.22 Examples: (a) Let $x^3 + 6x + 2 \in \mathbb{F}_7[x]$. This polynomial has no root in $\mathbb{F}_7$, hence is irreducible and then clearly separable over $\mathbb{F}_7$. Its discriminant $-4(6)^3 - 27(2)^2 = 4 + 1 \cdot 4 = 1 = 1^2$ (Example 56.10(b)) is a square in $\mathbb{F}_7$, so the Galois group of $x^3 + 6x + 2$ is $A_3$.

(b) Let $x^3 + 5x + 5 \in \mathbb{Q}[x]$. This polynomial is irreducible by Eisenstein's criterion and is separable over $\mathbb{Q}$ since $\text{char } \mathbb{Q} = 0$. The discriminant is equal to $-4(5)^3 - 27(5)^2 = -1175$, which is not a square in $\mathbb{Q}$. So the Galois group of $x^3 + 5x + 5$ is $S_3$.

Next we investigate polynomials of degree four. Here $S_4$ will come into play. We know that $V_4 = \{ 1, (12)(34), (13)(24), (14)(23) \}$ is an important normal subgroup of $S_4$. It will be useful to find the intermediate field corresponding to $V_4$ in the Galois correspondence.
56.23 Theorem: Let $K$ be a field such that char $K \neq 2$ and let \( f(x) \in K[x] \) be a polynomial of degree four. Let $E$ be a splitting field of $f(x)$ over $K$. Suppose $f(x)$ has four distinct roots $r_1, r_2, r_3, r_4$ in $E$ so that $E$ is a Galois extension of $K$ (Theorem 55.7). We put $\alpha = r_1 r_2 + r_3 r_4$, $\beta = r_1 r_3 + r_2 r_4$ and $\gamma = r_1 r_4 + r_2 r_3$ and consider the Galois group $Aut_k E$ as a subgroup of $S_4$ (Theorem 56.14).

In the Galois correspondence, the intermediate field $K(\alpha, \beta, \gamma)$ corresponds to $Aut_k E \cap V_4$.

**Proof:** In the Galois correspondence, the subgroup of $Aut_k E$ corresponding to the intermediate field $K(\alpha, \beta, \gamma)$ is

$$K(\alpha, \beta, \gamma)' = \{ \varphi \in Aut_k E: a \varphi = a \text{ for all } a \in K(\alpha, \beta, \gamma) \} = \{ \varphi \in Aut_k E: \alpha \varphi = \alpha, \beta \varphi = \beta, \gamma \varphi = \gamma \}.$$

If $\varphi = (12)(34) \in Aut_k E$, then $\varphi$ fixes $\alpha$ since $\alpha \varphi = (r_1 r_2 + r_3 r_4) \varphi = r_2 r_1 + r_4 r_3 = r_1 r_2 + r_3 r_4 = \alpha$. Similarly $\beta \varphi = (r_1 r_3 + r_2 r_4) \varphi = r_2 r_4 + r_1 r_3 = \beta$ and $\gamma \varphi = (r_1 r_4 + r_2 r_3) \varphi = r_2 r_3 + r_1 r_4 = \gamma$. Thus $(12)(34) \in K(\alpha, \beta, \gamma)'$ if $(12)(34)$ is in $Aut_k E$. In like manner, one verifies that $(13)(24)$ and $(14)(23)$ belong to $K(\alpha, \beta, \gamma)'$ whenever they are in $Aut_k E$. This proves $V_4 \cap Aut_k E \leq K(\alpha, \beta, \gamma)'$.

To complete the proof, we show, for any $\varphi \in Aut_k E$, that $\varphi \notin V_4$ implies $\varphi \notin K(\alpha, \beta, \gamma)'$. Indeed if $\varphi \notin V_4$, then $\varphi$ is in one of the cosets $V_4(12)$, $V_4(13)$, $V_4(23)$, $V_4(123)$, $V_4(132)$ of $V_4$ in $S_4$. If $\varphi \in V_4(12)$, then $\varphi = \psi(12)$ for some $\psi \in V_4 \cap Aut_k E$, therefore $(r_1 r_3 + r_2 r_4) \psi = (r_1 r_3 + r_2 r_4) \psi(12) = (r_1 r_3 + r_2 r_4)(12)$ and $\varphi$ does not fix $\beta$ since $r_1 r_3 + r_2 r_4 = \beta = \beta \varphi = (r_1 r_3 + r_2 r_4) \varphi = (r_1 r_3 + r_2 r_4)(12) = r_2 r_3 + r_1 r_4$ yields $(r_1 - r_2) r_3 = (r_1 - r_2) r_4$ and so $r_1 = r_2$ or $r_3 = r_4$, contrary to the hypothesis that the roots of $f(x)$ are distinct. Similarly, if $\varphi \in V_4(13)$, then $\varphi$ does not fix $\gamma$ and if $\varphi \in V_4(23)$, then $\varphi$ does not fix $\alpha$. If $\varphi \in V_4(123)$, then $\varphi$ does not fix $\alpha$ since $r_1 r_2 + r_3 r_4 = \alpha = \alpha \varphi = (r_1 r_2 + r_3 r_4) \varphi = (r_1 r_2 + r_3 r_4)(123) = r_2 r_3 + r_1 r_4$ yields $(r_1 - r_3) r_2 = (r_1 - r_3) r_4$ and so $r_1 = r_3$ or $r_2 = r_4$, contrary to the hypothesis. Similarly, if $\varphi \in V_4(132)$, then $\varphi$ does not fix $\alpha$. This proves that no automorphism in $Aut_k E \cap V_4$ can be in $K(\alpha, \beta, \gamma)'$. Hence we obtain $K(\alpha, \beta, \gamma)' \leq V_4 \cap Aut_k E$, as was to be proved. □
56.24 Definition: Let $K$ be a field and let $f(x) \in K[x]$ be a polynomial of degree four having four distinct roots $r_1, r_2, r_3, r_4$ in a splitting field of $f(x)$ over $K$. We put $\alpha = r_1 r_2 + r_3 r_4$, $\beta = r_1 r_3 + r_2 r_4$ and $\gamma = r_1 r_4 + r_2 r_3$. The polynomial $(x - \alpha)(x - \beta)(x - \gamma) \in K(\alpha, \beta, \gamma)[x]$ is called the resolvent cubic of $f(x)$.

56.25 Lemma: Let $K$ be a field and let $f(x) \in K[x]$ be a polynomial of degree four having four distinct roots in a splitting field of $f(x)$ over $K$. Then the resolvent cubic of $f(x)$ is a polynomial in $K[x]$. In fact, if $f(x) = x^4 + bx^3 + cx^2 + dx + e$, then the resolvent cubic of $f(x)$ is equal to
\[x^3 - (\alpha + \beta + \gamma)x^2 + (\alpha \beta + \alpha \gamma + \beta \gamma)x - (\alpha \beta \gamma),\]
where $\alpha = r_1 r_2 + r_3 r_4$, $\beta = r_1 r_3 + r_2 r_4$, $\gamma = r_1 r_4 + r_2 r_3$. Let $\sigma_m$ be the $m$-th elementary symmetric polynomial in 4 indeterminates. Then we have
\[
\begin{align*}
\alpha \beta + \alpha \gamma + \beta \gamma &= r_1^2 r_2^2 r_3^2 + \cdots = \\
&= (r_1 + r_2 + r_3 + r_4)(r_1 r_2 r_3 + r_1 r_2 r_4 + r_1 r_3 r_4 + r_2 r_3 r_4) - 4r_1 r_2 r_3 r_4 = \\
&= \sigma_1(r_1, r_2, r_3, r_4)\sigma_3(r_1, r_2, r_3, r_4) - \sigma_4(r_1, r_2, r_3, r_4) = b^2 d - 4e; \\
\alpha \beta \gamma &= \cdots = b^2 e - 4ce + d^2. 
\end{align*}
\]

56.26 Theorem: Let $K$ be a field and let $f(x) \in K[x]$ be a polynomial of degree four, which is irreducible and separable over $K$. Let $E$ be a splitting field of $f(x)$ over $K$ and let $r_1, r_2, r_3, r_4$ be the (distinct) roots of $f(x)$ in $E$. We put $\alpha = r_1 r_2 + r_3 r_4$, $\beta = r_1 r_3 + r_2 r_4$ and $\gamma = r_1 r_4 + r_2 r_3$. Let $G = Aut_KE$ be the Galois group of $f(x)$, considered as a subgroup of $S_4$. We put $|K(\alpha, \beta, \gamma):K| = m$. Then $G$ can be described as follows.

\[
\begin{align*}
G = S_4 & \iff m = 6. \\
G = A_4 & \iff m = 3. \\
G \cong D_8 & \iff m = 2 \text{ and } f(x) \text{ is irreducible over } K(\alpha, \beta, \gamma). \\
G = V_4 & \iff m = 1. \\
G \cong C_4 & \iff m = 2 \text{ and } f(x) \text{ is reducible over } K(\alpha, \beta, \gamma). 
\end{align*}
\]

Proof: Since $f(x)$ is irreducible and separable over $K$, its roots are distinct. We know that $G$ is a transitive subgroup of of $S_4$ and 4 divides
The transitive subgroups of $S_4$ whose orders are divisible by 4 are $S_4$, $A_4$, the Sylow 2-subgroups of $S_4$ (isomorphic to $D_8$), $V_4$ and the cyclic groups generated by 4-cycles like $\langle (1234) \rangle$ (Example 56.15(f)). Thus $G$ is one of $S_4$, $A_4$, $D_8$, $V_4$, $C_4$.

The intermediate field $K(\alpha,\beta,\gamma)$ corresponds to $V_4 \cap G$ (Theorem 56.23). Now $E$ is Galois over $K(\alpha,\beta,\gamma)$ and the Galois group $Aut_{K(\alpha,\beta,\gamma)} E = K(\alpha,\beta,\gamma)'$ is $V_4 \cap G$. Since $V_4 \trianglelefteq S_4$, we have $V_4 \cap G \trianglelefteq G$ and so $K(\alpha,\beta,\gamma)$ is a Galois extension of $K$ and the Galois group of $K(\alpha,\beta,\gamma)$ over $K$ is (isomorphic to) $G/(G \cap V_4)$ (Theorem 54.25(2)). We get

$$m = |K(\alpha,\beta,\gamma):K| = |Aut_K K(\alpha,\beta,\gamma)| = |G/(G \cap V_4)|$$

and

- $G = S_4 \quad \Rightarrow \quad m = |G/(G \cap V_4)| = |S_4/V_4| = 6$;
- $G = A_4 \quad \Rightarrow \quad m = |G/(G \cap V_4)| = |A_4/V_4| = 3$;
- $G \cong D_8 \quad \Rightarrow \quad m = |G/(G \cap V_4)| = |D_8/V_4| = 2$; moreover, $E$ is a splitting field of $f(x)$ over $K(\alpha,\beta,\gamma)$ and $Aut_{K(\alpha,\beta,\gamma)} E = K(\alpha,\beta,\gamma)' = V_4 \cap D_8 = V_4$ is a transitive subgroup of $S_4$, so $f(x)$ is irreducible over $K(\alpha,\beta,\gamma)$ by Theorem 56.16;

- $G = V_4 \quad \Rightarrow \quad m = |G/(G \cap V_4)| = |V_4/V_4| = 1$;
- $G \cong C_4 \quad \Rightarrow \quad m = |G/(G \cap V_4)| = |\{ 1, (1234), (13)(24), (1432) \}/\{ 1, (13)(24) \}| = 2$.

(especially after renaming the roots, we may assume, without loss of generality, that $G = \{ 1, (1234), (13)(24), (1432) \}$; moreover, $Aut_{K(\alpha,\beta,\gamma)} E = K(\alpha,\beta,\gamma)' = \langle (1234) \rangle \cap V_4 = \langle (13)(24) \rangle$ is not a transitive subgroup of $S_4$, so $f(x)$ is not irreducible over $K(\alpha,\beta,\gamma)$ by Theorem 56.16.

This proves the $\Rightarrow$ assertions in the statement of the theorem. As the five cases are mutually exclusive, the converse assertions are also valid. 

\[ \square \]

**56.27 Examples:** (a) The polynomial $f(x) = x^4 - 4x^2 + 1 \in \mathbb{Q}[x]$ has no integer roots and is easily verified to have no quadratic factors in $\mathbb{Z}[x]$, so $f(x)$ is irreducible over $\mathbb{Z}$ and over $\mathbb{Q}$ (Lemma 34.11). Since $\text{char } \mathbb{Q} = 0$, $f(x)$ is separable over $\mathbb{Q}$. In order to determine its Galois group $G$, we find the resolvent cubic of $f(x)$. The resolvent cubic of $f(x)$ is

$$x^3 - (-4)x^2 + (0 \cdot 0 - 4 \cdot 1)x - (0^2 - 1 - 4(-4)(1) + 0^2) = x^3 + 4x^2 - 4x - 16 = (x + 4)(x - 2)(x + 2)$$

723
and the roots $\alpha, \beta, \gamma$ of the resolvent cubic are $-4, -2, 2$. Thus $\Omega(\alpha, \beta, \gamma) = \Omega$ and $m = |\Omega(\alpha, \beta, \gamma):\Omega| = 1$. Theorem 56.26 yields $G = V_4$.

From $f(r) = 0 \iff (r^2 - 2)^2 = 3$, we see that the roots (say in $\mathbb{R}$) of $f(x)$ are $r_1 = \sqrt{2 + \sqrt{3}}$, $r_2 = \sqrt{2 - \sqrt{3}}$, $r_3 = -\sqrt{2 + \sqrt{3}}$, $r_4 = -\sqrt{2 - \sqrt{3}}$. Note that $r_2 = 1/r_1$, $r_3 = -r_1$ and $r_4 = -1/r_1$. Since

$(12)(34) \in V_4 = G$ fixes $r_1 + r_2 = \sqrt{6},$

$(13)(24) \in V_4 = G$ fixes $r_1^2$, hence also $r_1^2 - 2 = \sqrt{3},$

$(14)(23) \in V_4 = G$ fixes $r_1 + r_4 = \sqrt{2}$, the Galois correspondence is as depicted below.

| $\Omega(\sqrt{2 + \sqrt{3}})$ | 1 |
| $\Omega(\sqrt{6})$ | $\Omega(\sqrt{3})$ | $\Omega(\sqrt{2})$ | $\langle(12)(34)\rangle$ | $\langle(13)(24)\rangle$ | $\langle(14)(23)\rangle$ |

$(b)$ Let $f(x) = x^4 + 5x^2 + 5 \in \mathbb{Q}[x]$. Then $f(x)$ is irreducible over $\mathbb{Z}$ by Eisenstein's criterion and also over $\mathbb{Q}$ by Lemma 34.11. Thus $f(x)$ is separable over $\mathbb{Q}$. Let $G$ be the Galois group of $f(x)$. The resolvent cubic of $f(x)$ is $x^3 - 5x^2 + 20x + 100 = (x - 5)(x^2 - 20) = (x - 5)(x - 2\sqrt{5})(x + 2\sqrt{5})$, with roots $\alpha, \beta, \gamma = 5, 2\sqrt{5}, -2\sqrt{5}$. Hence $\Omega(\alpha, \beta, \gamma) = \Omega(\sqrt{5})$. So Theorem 56.26 gives $G \cong D_8$ or $G \cong C_4$. In fact, since

$$f(x) = \left(x^2 + \frac{5 + \sqrt{5}}{2}\right)\left(x^2 + \frac{5 - \sqrt{5}}{2}\right)$$

is reducible over $\Omega(\sqrt{5})$, we have $G \cong C_4$.

$(c)$ Let $f(x) = x^4 - 2 \in \mathbb{Q}[x]$. Then $f(x)$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion and Lemma 34.11. Let $G$ be the Galois group of $f(x)$. The resolvent cubic of $f(x)$ is $x^3 + 8x$, whose roots are $\alpha, \beta, \gamma = 0, 2\sqrt{2}i, -2\sqrt{2}i$. Therefore $m = |\Omega(\sqrt{2}i):\Omega| = 2$ and $G \cong D_8$ or $G \cong C_4$. It is easy to see that $f(x)$ is irreducible over $\Omega(\sqrt{2}i)$, so we get $G \cong D_8$ from Theorem 56.26.
Exercises

1. Find the resultant \( R(f,g) \) when \( f(x) = x^3 + 4x^2 - 3x^2 + x - 2 \in \mathbb{Q}[x] \) and \( g(x) = x - 3 \in \mathbb{Q}[x] \).

2. Let \( K \) be a field and \( f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \). \( g(x) = b_1 x + b_0 \) polynomials in \( K[x] \), with \( b_1 \neq 0 \). Show that \( R(f,g) = (-b_1)^n f(-b_1/b_0) \).

3. Let \( K \) be a field and \( f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \). \( g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0 \). If \( n \geq m \), show that \( R(f + cg, g) = R(f,g) \) for all \( c \in K \).

4. Let \( K \) be a field and \( f, g, h \in K[x] \). Prove that \( R(fh, g) = R(f, g)R(h, g) \).

5. Let \( K \) be a field and \( f, g, h \in K[x] \). Prove that \( D(fg) = D(f)D(g)[R(f,g)]^2 \) and that \( D(f(x-c)) = D(f(x)) \) for any \( c \in K \).

6. Let \( K \) be a field and \( f(x) = ax^3 + bx^2 + cx + d \in K[x] \). Prove that
\[
D(f) = b^2c^2 + 18abcd - 4a^3c^2 - 4b^3d - 27a^2d^2.
\]

7. Let \( K \) be a field and \( f(x) = x^4 + ax^2 + bx + c \in K[x] \). Prove that
\[
D(f) = -4a^3b^2 + 144abc^2 + 16a^4c - 128b^2c^2 + 256c^3 - 27b^4.
\]

8. Let \( K \) be a field, \( f(x) \) a polynomial of degree \( n \) in \( K[x] \), with leading coefficient \( a_n \) and let \( r_1, r_2, \ldots, r_n \) be the roots of \( f(x) \) in some splitting field of \( f(x) \) over \( K \). Put \( s_0 = n \) and \( s_m = r_1^m + r_2^m + \cdots + r_n^m \) for \( m \in \mathbb{N} \). Show that
\[
D(f) = a_n^{2n-2} \begin{vmatrix}
  s_0 & s_1 & s_2 & \cdots & s_{n-1} \\
  s_1 & s_2 & s_3 & \cdots & s_n \\
  \vdots & \vdots & \vdots & \ddots & \vdots \\
  s_{n-1} & s_n & s_{n+1} & \cdots & s_{2n-2}
\end{vmatrix}.
\]

(Hint: multiply two Vandermonde determinants.)

8. Where did we use the hypothesis \( char K \neq 2 \) in Theorem 56.18?

9. Find the discriminants and Galois groups of the following polynomials.

(a) \( x^3 + 3x^2 - 1 \in \mathbb{Q}[x] \).
10. Find the Galois groups of the following polynomials over the fields indicated.

(a) \(x^4 - 2\) over \(\mathbb{Q}(\sqrt{2})\) and over \(\mathbb{Q}(\sqrt{2}i)\).
(b) \((x^3 - 2)(x^2 - 5)\) over \(\mathbb{Q}\).
(c) \(x^4 - 8x^2 + 15\) over \(\mathbb{Q}\).
(d) \(x^4 + 4x^2 + 2\) over \(\mathbb{Q}\) and over \(\mathbb{Q}(\sqrt{2})\).
(e) \((x^2 - 2)(x^2 - 3)(x^2 - 5)\) over \(\mathbb{Q}\), over \(\mathbb{Q}(\sqrt{2})\), over \(\mathbb{Q}(\sqrt{6})\) and over \(\mathbb{Q}(\sqrt{2},\sqrt{3})\).

11. Let \(K\) be any arbitrary field and \(f(x) = x^3 - 3x + 1 \in K[x]\). Show that \(f(x)\) is either irreducible over \(K\) or splits in \(K\).

12. Let \(K\) be a field and \(f(x)\) an irreducible separable polynomial of degree three in \(K[x]\). Suppose \(r_1,r_2,r_3\) are the roots of \(f(x)\) in some splitting field of \(f(x)\) over \(K\). If the Galois group of \(f(x)\) is \(S_3\), show that, in the Galois correspondence, \(K(r_i)\) corresponds to the subgroup \(\{1,ik\}\) of \(S_3\), where \(\{i,j,k\} = \{1,2,3\}\).

13. Prove that \(S_4\) has no transitive subgroup of order six.

14. Let \(p\) be a prime number and \(G \leq S_p\). Show that \(G\) is transitive if and only if \(p\) divides the order of \(G\).