Invariant Theory of Finite Groups

Invariant theory has had a profound effect on the development of algebraic geometry. For example, the Hilbert Basis Theorem and Hilbert Nullstellensatz, which play a central role in the earlier chapters in this book, were proved by Hilbert in the course of his investigations of invariant theory.

In this chapter, we will study the invariants of finite groups. The basic goal is to describe all polynomials which are unchanged when we change variables according to a given finite group of matrices. Our treatment will be elementary and by no means complete. In particular, we do not presume a prior knowledge of group theory.

§1 Symmetric Polynomials

Symmetric polynomials arise naturally when studying the roots of a polynomial. For example, consider the cubic \( f = x^3 + bx^2 + cx + d \) and let its roots be \( \alpha_1, \alpha_2, \alpha_3 \). Then

\[
x^3 + bx^2 + cx + d = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3).
\]

If we expand the right-hand side, we obtain

\[
x^3 + bx^2 + cx + d = x^3 - (\alpha_1 + \alpha_2 + \alpha_3)x^2 + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)x - \alpha_1\alpha_2\alpha_3,
\]

and, thus,

\[
\begin{align*}
b &= -(\alpha_1 + \alpha_2 + \alpha_3), \\
c &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3, \\
d &= -\alpha_1\alpha_2\alpha_3.
\end{align*}
\]

This shows that the coefficients of \( f \) are polynomials in its roots. Further, since changing the order of the roots does not affect \( f \), it follows that the polynomials expressing \( b, c, d \) in terms of \( \alpha_1, \alpha_2, \alpha_3 \) are unchanged if we permute \( \alpha_1, \alpha_2, \alpha_3 \). Such polynomials are said to be symmetric. The general concept is defined as follows.

**Definition 1.** A polynomial \( f \in k[x_1, \ldots, x_n] \) is symmetric if

\[
f(x_{i_1}, \ldots, x_{i_n}) = f(x_1, \ldots, x_n)
\]
For every possible permutation $x_i, \ldots, x_n$ of the variables $x_1, \ldots, x_n$.

For example, if the variables are $x$, $y$, and $z$, then $x^2 + y^2 + z^2$ and $xyz$ are obviously symmetric. The following symmetric polynomials will play an important role in our discussion.

**Definition 2.** Given variables $x_1, \ldots, x_n$, we define $\sigma_1, \ldots, \sigma_n \in k[x_1, \ldots, x_n]$ by the formulas

\[
\sigma_1 = x_1 + \cdots + x_n,
\]

\[
\vdots
\]

\[
\sigma_r = \sum_{i_1 < i_2 < \cdots < i_r} x_{i_1}x_{i_2} \cdots x_{i_r},
\]

\[
\vdots
\]

\[
\sigma_n = x_1x_2 \cdots x_n.
\]

Thus, $\sigma_r$ is the sum of all monomials that are products of $r$ distinct variables. In particular, every term of $\sigma_r$ has total degree $r$. To see that these polynomials are indeed symmetric, we will generalize observation (1). Namely, introduce a new variable $X$ and consider the polynomial

\[
f(X) = (X - x_1)(X - x_2) \cdots (X - x_n)
\]

with roots $x_1, \ldots, x_n$. If we expand the right-hand side, it is straightforward to show that

\[
f(X) = X^n - \sigma_1 X^{n-2} + \sigma_2 X^{n-2} + \cdots + (-1)^{n-1}\sigma_{n-1} X + (-1)^n \sigma_n
\]

(we leave the details of the proof as an exercise). Now suppose that we rearrange $x_1, \ldots, x_n$. This changes the order of the factors on the right-hand side of (2), but $f$ itself will be unchanged. Thus, the coefficients $(-1)^r \sigma_r$ of $f$ are symmetric functions.

One corollary is that for any polynomial with leading coefficient 1, the other coefficients are the elementary symmetric functions of its roots (up to a factor of $\pm 1$). The exercises will explore some interesting consequences of this fact.

From the elementary symmetric functions, we can construct other symmetric functions by taking polynomials in $\sigma_1, \ldots, \sigma_n$. Thus, for example,

\[
\sigma_2^2 - \sigma_1 \sigma_3 = x^2 y^2 + x^2 yz + x^2 z^2 + xy^2 z + xyz^2 + y^2 z^2
\]

is a symmetric polynomial. What is more surprising is that all symmetric polynomials can be represented in this way.

**Theorem 3 (The Fundamental Theorem of Symmetric Polynomials).** Every symmetric polynomial in $k[x_1, \ldots, x_n]$ can be written uniquely as a polynomial in the elementary symmetric functions $\sigma_1, \ldots, \sigma_n$.

**Proof.** We will use lex order with $x_1 > x_2 > \cdots > x_n$. Given a nonzero symmetric polynomial $f \in k[x_1, \ldots, x_n]$, let $\text{LT}(f) = ax^\alpha$. If $\alpha = (\alpha_1, \ldots, \alpha_n)$, we first claim