THE ALGEBRAIC THEORY OF MODULAR SYSTEMS

Introduction

Definition. A modular system is an infinite aggregate of polynomials, or whole functions* of n variables $x_1, x_2, \ldots, x_n$, defined by the property that if F, F_1, F_2 belong to the system $F_1 + F_2$ and AF also belong to the system, where A is any polynomial in $x_1, x_2, \ldots, x_n$.

Hence if $F_1, F_2, \ldots, F_k$ belong to a modular system so also does $A_1F_1 + A_2F_2 + \ldots + A_kF_k$, where $A_1, A_2, \ldots, A_k$ are arbitrary polynomials.

Besides the algebraic or relative theory of modular systems there is a still more difficult and varied absolute theory. We shall only consider the latter theory in so far as it is necessary for the former.

In the algebraic theory polynomials such as F and aF, where a is a quantity not involving the variables, are not regarded as different polynomials, and any polynomial of degree zero is equivalent to 1. No restriction is placed on the coefficients of $F_1, F_2, \ldots, F_k$ except in so far as they may involve arbitrary parameters $u_1, u_2, \ldots$, in which case they are restricted to being rational functions of such parameters. The same restriction applies to the coefficients of the arbitrary polynomials $A_1, A_2, \ldots, A_k$ above.

In the absolute theory the coefficients of $F_1, F_2, \ldots, A_1, A_2, \ldots$ are restricted to a domain of integrity, generally ordinary integers or whole functions of parameters $u_1, u_2, \ldots$ with integral coefficients; and a polynomial of degree zero other than 1 or a unit is not equivalent to 1.

* We use the term *whole function* throughout the text (but not in the Note at the end) as equivalent to *polynomial* and as meaning a *whole rational function.*

Definitions. A modular system will be called a *module* (of polynomials).

Any polynomial F belonging to a module M is called a *member* (or element) of M.

According as we wish to denote that F is a member of M in the relative or absolute sense we shall write $F=0 \bmod M$, or $F \equiv 0 \bmod M$. The notation $F \equiv 0 \bmod M$ only comes into use in the sequel in connection with the Resultant.

A *basis* of a module M is any set of members $F_1, F_2, \ldots, F_k$ such that every member of M is of the form $X_1 F_1 + X_2 F_2 + \ldots + X_k F_k$, where $X_1, X_2, \ldots, X_k$ are polynomials.

Every module of polynomials has a basis consisting of a finite number of members (Hilbert's theorem, § 37).

The proof of this theorem is from first principles, and its truth will be assumed throughout.

The theory of modular systems is very incomplete and offers a wide field for research. The object of the algebraic theory is to discover those general properties of a module which will afford a means of answering the question whether a given polynomial is a member of a given module or not. Such a question in its simpler aspect is of importance in Geometry and in its general aspect is of importance in Algebra. The theory resembles Geometry in including a great variety of detached and disconnected theorems. As a branch of Algebra it may be regarded as a generalized theory of the solution of equations in several unknowns, and assumes that any given algebraic equation in one unknown can be completely solved. In order that a polynomial F may be a member of a module M whose basis $(F_1, F_2, \ldots, F_k)$ is given it is evident that F must vanish for all finite solutions (whether finite or infinite in number) of the equations $F_1 = F_2 = \ldots = F_k = 0$. These conditions are *sufficient* if M resolves into what are called *prime modules**; otherwise they are not sufficient, and F must satisfy further conditions, also connected with the solutions, which may be difficult to express concretely. The first step is to find all the solutions of the equations $F_1 = F_2 = \ldots = F_k = 0$; and this is completely accomplished in the theories of the resultant and resolvent.

* Cayley and Salmon constantly assume this. Salmon also discusses particular cases of a number of important and suggestive problems connected with modular systems (Sa).