In this chapter we shall introduce a new point of view. Diophantine problems over finite fields will be put into the context of elementary algebraic geometry. The notions of affine space, projective space, and points at infinity will be defined.

After these problems of language have been dealt with, we shall prove a very general theorem due to C. Chevalley, which states that a polynomial in several variables with no constant term over a finite field always has nontrivial zeros if the number of variables exceeds the degree.

Next, our interest turns to the problem of generalizing the results of Chapter 8 to arbitrary finite fields. This turns out to be relatively easy. These more general results are of interest for their own sake and are crucial to the discussion of the zeta function, which we shall take up in Chapter 11.

§1 Affine Space, Projective Space, and Polynomials

Let $F$ be a field and $A^n(F)$ the set of $n$-tuples $(a_1, a_2, \ldots, a_n)$ with $a_i \in F$. $A^n(F)$ can be considered as a vector space by defining addition and scalar multiplication in the usual way. We shall be concerned principally with the underlying set, which will be called affine $n$-space over $F$. As usual the point $(0, 0, \ldots, 0)$ will be called the origin. If there is no chance of confusion we shall denote the point $(a_1, a_2, \ldots, a_n)$ by the single letter $a$.

Projective $n$-space over $F$, $P^n(F)$, is a somewhat more difficult concept. We first consider $A^{n+1}(F)$, denoting its points by $(a_0, a_1, \ldots, a_n)$. On the set $A^{n+1}(F) - \{(0, 0, \ldots, 0)\}$ (affine $(n + 1)$-space from which the origin has been removed) we define an equivalence relation. $(a_0, a_1, \ldots, a_n)$ is said to be equivalent to $(b_0, b_1, \ldots, b_n)$ if there is a $\gamma \in F^*$ such that $a_0 = \gamma b_0$, $a_1 = \gamma b_1, \ldots, a_n = \gamma b_n$. This is easily seen to be an equivalence relation. The equivalence classes are called points of $P^n(F)$. If $a \in A^{n+1}(F)$ is distinct from the origin, then $[a]$ will denote the equivalence class containing $a$. $a$ will be called a representative of $[a]$. Geometrically, the points of $P^n(F)$
are in one-to-one correspondence with the lines in \( A^{n+1}(F) \) that pass through the origin.

If \( F \) is a finite field with \( q \) elements, then clearly \( A^n(F) \) has \( q^n \) elements. \( P^n(F) \) has \( q^n + q^{n-1} + \cdots + q + 1 \) elements. To see this, notice that \( A^{n+1}(F) - \{(0, 0, \ldots, 0)\} \) has \( q^{n+1} - 1 \) elements. Since \( F^* \) has \( q - 1 \) elements each equivalence class has \( q - 1 \) elements. Thus \( P^n(F) \) has \( (q^{n+1} - 1)/(q - 1) = q^n + q^{n-1} + \cdots + q + 1 \) elements.

In general \( P^n(F) \) has more points than \( A^n(F) \). This is made more precise as follows. If \( [x] \in P^n(F) \) and \( x_0 \neq 0 \), set \( \phi([x]) = (x_1/x_0, x_2/x_0, \ldots, x_n/x_0) \in A^n(F) \). This map is easily seen to be independent of the representative \( x \).

**Lemma 1.** Let \( \overline{H} \) be the set of \( [x] \in P^n(F) \) such that \( x_0 = 0 \). Then \( \phi \) maps \( P^n(F) - \overline{H} \) to \( A^n(F) \) and this map is one to one and onto. (If \( S \) and \( T \) are sets, then \( S - T \) is the set of elements in \( S \) but not in \( T \).)

**Proof.** If \( \phi([x]) = \phi([y]) \), then \( x_i/x_0 = y_i/y_0 \) for \( i = 0, 1, \ldots, n \). Let \( \gamma = y_0/x_0 \). Then \( \gamma x_i = y_i \) for \( i = 0, 1, \ldots, n \) and so \( [x] = [y] \).

If \( v = (v_1, v_2, \ldots, v_n) \in A^n(F) \), set \( w = (1, v_1, v_2, \ldots, v_n) \). Then \( \phi([w]) = v \). \( \square \)

The set \( \overline{H} \) is called the hyperplane at infinity. It is easy to see that \( \overline{H} \) has the structure of \( P^{n-1}(F) \). Thus \( P^n(F) \) is made up of two pieces, one a copy of \( A^n(F) \), called the finite points, and the other a copy of \( P^{n-1}(F) \), called the points at infinity.

Notice that \( P^0(F) \) consists of just one point. Thus \( P^1(F) \) has only one point at infinity. Similarly \( P^2(F) \) has a (projective) line at infinity, etc.

Now that affine space and projective space have been defined we take up the subject of polynomials and see how they determine sets called hypersurfaces.

Let \( F[x_1, x_2, \ldots, x_n] \) be the ring of polynomials in \( n \) variables over \( F \). If \( f \in F[x_1, \ldots, x_n] \), then

\[
 f(x) = \sum_{(i_1, i_2, \ldots, i_n)} a_{i_1i_2\ldots}i_n x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n},
\]

where the sum is over a finite set of \( n \)-tuples of nonnegative integers \((i_1, i_2, \ldots, i_n)\), where \( a_{i_1i_2\ldots}i_n \neq 0 \). A polynomial of the form \( x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n} \) is called a monomial. Its total degree is defined to be \( i_1 + i_2 + \cdots + i_n \); its degree in the variable \( x_m \) is defined as \( i_m \). The degree of \( f(x) \) is the maximum of the total degrees of monomials that occur in \( f(x) \) with nonzero coefficients. The degree in \( x_m \) is the maximum of the degrees in \( x_m \) of monomials that occur in \( f(x) \) with nonzero coefficients. Call these two numbers \( \deg f(x) \) and \( \deg_m f(x) \). Then

(a) \( \deg f(x)g(x) = \deg f(x) + \deg g(x) \).
(b) \( \deg_m f(x)g(x) = \deg_m f(x) + \deg_m g(x) \).