

June 28, 1966

To the Graduate Council:

I am submitting herewith a thesis written by William F. Lawkins entitled "Permutation Polynomials of Finite Fields." I recommend that it be accepted for nine quarter hours of credit in partial fulfillment of the requirements for the degree of Master of Arts, with a major in Mathematics.

David R. Hayes
Major Professor

We have read this thesis and
recommend its acceptance:

John E. Moore

Robert H. McConnell

Accepted for the Council:

Herbert A. Smith
Dean of the Graduate School

CHAPTER I

INTRODUCTION

A permutation polynomial of a finite field K is one for which the associated polynomial function is a one-to-one map from K onto itself. The purpose of this paper is to explain and demonstrate how algebraic geometry can be employed in determining permutation polynomials of finite fields of sufficiently large order.

In Chapter II, definitions and well-known results from elementary algebraic geometry, which are used throughout the paper, are stated.

As noted earlier, we shall deal only with finite fields whose order is sufficiently large. In Chapter III, results are obtained which are used later to establish criteria for the size of the finite fields to be considered. Also, by elementary means, the exact number of rational points on an absolutely irreducible projective quadratic curve is obtained.

In Chapter IV, results given by Chevalley [1], which are used in Chapter III, are displayed.

Chapters V through IX are devoted to determining the primary permutation polynomials of degrees four and five of finite fields of sufficiently large order, and the essential results of chapters VI through IX are compiled in Chapter X. The results for the cases which are considered in these chapters were known previously and can be found in Dickson's Linear Groups [2].

CHAPTER II

ELEMENTARY PROPERTIES OF AFFINE AND PROJECTIVE PLANES

Included in this chapter is a survey of definitions and results from the elementary theory of algebraic curves. Most of the results in this chapter were obtained from W. E. Jenner [3].

Let K be any finite field and suppose Ω is an algebraic closure of K . By the affine plane over Ω , denoted $A(\Omega)$, is meant the set of ordered pairs (x, y) where x and y belong to Ω . Such an ordered pair is called a point. If x and y belong to K , then (x, y) is called a rational point.

Let $\Omega[X, Y]$ be the polynomial ring in two indeterminates over Ω . An algebraic curve, or briefly, a curve, in $A(\Omega)$ is the set of points in $A(\Omega)$ which are zeros of a polynomial in $\Omega[X, Y]$. Further, a curve is called a line if the polynomial which determines it has total degree one. If a curve in $A(\Omega)$ is determined by a polynomial with coefficients in K , then the curve and polynomial are called rational.

A given curve in $A(\Omega)$ may be the proper union of two or more curves. A curve C in $A(\Omega)$ is said to be reducible if there exists a curve B in $A(\Omega)$ such that B is a proper subset of C ; otherwise C is absolutely irreducible.

The polynomial $f(X, Y) \in \Omega[X, Y]$ is absolutely irreducible if whenever f is expressed as the product of two polynomials in

$\Omega[X, Y]$, one of the factors is a unit.

Suppose that $f(X, Y)$ and $g(X, Y)$ belong to $\Omega[X, Y]$, and let C_f and C_g be the curves in $A(\Omega)$ determined by f and g , respectively. By Hilbert's Nullstellensatz ([6], page 5), if $C_g \subseteq C_f$, then $g|f^n$ for some positive integer n . From this result, we can obtain the following lemma.

Lemma 2.1. Suppose $f(X, Y) \in \Omega[X, Y]$ and f is absolutely irreducible. Then C_f is absolutely irreducible.

Proof. Suppose C_f is not absolutely irreducible. Then there exists a curve C in $A(\Omega)$ which is a proper subset of C_f .

Let $h(X, Y)$ be a polynomial in $\Omega[X, Y]$ which determines C . As a result of the preceding, $h|f^n$ for some n . It follows, as h is not a unit and f is absolutely irreducible, that $h = f^n$ for some n . But, since C is a proper subset of C_f , $h \neq f^n$ for any n . This completes the proof.

Many rational curves in $A(\Omega)$ are "big" in the sense that they are "unbounded" within the space. We want to define a space which is likened to $A(\Omega)$ but in which all the points are within reach, so to speak.

Define the set P as follows:

$$P = \Omega \times \Omega \times \Omega \setminus \{0\} ,$$

where $0 = (0, 0, 0)$. The relation R defined on P as

$((a_1, a_2, a_3), (b_1, b_2, b_3)) \in R$ if there exists $d \in \Omega$ such that

$(a_1, a_2, a_3) = (b_1d, b_2d, b_3d)$ is an equivalence relation. If a pair of 3-tuples are related under R , they are called proportional.

The projective plane over Ω , denoted $P(\Omega)$, is defined as the set of equivalence classes determined by R on P ; i.e., $P(\Omega) = P/R$. An equivalence class in $P(\Omega)$ is called a point. If (a_1, a_2, a_3) is any 3-tuple in a given equivalence class, then the equivalence class; or point, is denoted $(a_1, a_2, a_3)^\wedge$. Further, if in a given equivalence class of $P(\Omega)$ there exists a 3-tuple (b_1, b_2, b_3) such that b_1, b_2 , and b_3 belong to K , then the point $(b_1, b_2, b_3)^\wedge$ is called rational.

Suppose $F(X, Y, Z)$ is a homogeneous polynomial in $\Omega[X, Y, Z]$ and $(a_1, a_2, a_3) \in \Omega \times \Omega \times \Omega \setminus \{0\}$. If $F(a_1, a_2, a_3) = 0$, then $F(a_1d, a_2d, a_3d) = 0$ for each $d \in \Omega$. Under these conditions, we say that the point $(a_1, a_2, a_3)^\wedge$ is a zero of $F(X, Y, Z)$.

An algebraic curve in $P(\Omega)$ is the set of zeros in $P(\Omega)$ of a homogeneous polynomial in three indeterminates with coefficients in Ω . Further, if the total degree of the polynomial is one, then the curve is called a line. If a curve in $P(\Omega)$ is determined by a homogeneous polynomial with coefficients in K , then the curve and polynomial are called rational.

A given curve in $P(\Omega)$ may be the proper union of two or more curves. A curve $\hat{C}$ in $P(\Omega)$ is called reducible if there is a

curve $\hat{B}$ in $P(\Omega)$ such that $\hat{B}$ is a proper subset of $\hat{C}$;
 otherwise, $\hat{C}$ is absolutely irreducible.

The homogeneous polynomial $h(X, Y, Z) \in \Omega[X, Y, Z]$ is absolutely irreducible if whenever h is expressed as the product of two homogeneous polynomials in $\Omega[X, Y, Z]$, one of the factors is a unit.

If a, b , and c belong to Ω and are not all zero, then $ax + by + cz = 0$ is an equation for a line in $P(\Omega)$. It is possible to show that given a pair of distinct points in $P(\Omega)$, there exists a unique line which contains those points [3]. Further, an equation in the above form for that line can be easily found.

In many instances it is convenient to have parametric equations for a given line rather than an equation of the type shown in the preceding paragraph. Suppose $p_0 = (a_1, a_2, a_3)^\wedge$ and $p_1 = (b_1, b_2, b_3)^\wedge$ are distinct points. Then $(x_1, x_2, x_3)^\wedge$ is a point on the line in $P(\Omega)$ fixed by the given points if and only if

$$x_i = a_i s + b_i t ,$$

$i = 1, 2$, and 3 , for some s and t in Ω with not both s and t zero (see [3], page 35]. Clearly, if p_0 and p_1 are rational points, then the line determined by them is a rational line.

Next we want to consider intersections of lines with curves in $P(\Omega)$. Suppose the polynomial $F(X_1, X_2, X_3)$ determines the curve $\hat{C}$ in $P(\Omega)$, and let

$$X_i = a_i s + b_i t ,$$

$i = 1, 2$, and 3 , be parametric equations for the line $\hat{L}$. Then the intersections of $\hat{C}$ with $\hat{L}$ are obtained by finding the values of s and t such that

$$G(s, t) = F(a_1s + b_1t, a_2s + b_2t, a_3s + b_3t) = 0.$$

Suppose that $(a_1, a_2, a_3)^\wedge$ is a point of intersection of $\hat{L}$ with $\hat{C}$. Then $(1, 0)$ is a zero of $G(s, t)$. If we write

$$G(s, t) = t^n \cdot G'(s, t),$$

where n is the maximum power of t which divides $G(s, t)$, then the multiplicity of the intersection of $\hat{L}$ with $\hat{C}$ at $(a_1, a_2, a_3)^\wedge$ is n .

We now show that for a given rational point on a rational curve in $P(\Omega)$, there exists a rational line which intersects the curve at the given point with multiplicity greater than one.

Theorem 2.1. Suppose $F(X, Y, Z)$ is a homogeneous polynomial of degree $n > 1$ in $K[X, Y, Z]$. If $\hat{C}$ is the curve in $P(\Omega)$ determined by F and p_0 is a rational point on $\hat{C}$, there exists a rational line in $P(\Omega)$ which intersects $\hat{C}$ at p_0 with multiplicity greater than one.

Proof. Let $p_0 = (a_1, a_2, a_3)^\wedge$, where a_1, a_2 , and a_3 belong to K , and define $p = (b_1, b_2, b_3)^\wedge$ to be an arbitrary point in $P(\Omega)$ distinct from p_0 .

The intersections of the line determined by p_0 and p with $\hat{C}$ can be obtained from the solutions in s and t to the equation

$$(2.1) \quad G(s, t) = F(a_1 s + b_1 t, a_2 s + b_2 t, a_3 s + b_3 t) = 0.$$

Since F is a homogeneous polynomial of degree n ,

$$(2.2) \quad G(s, t) = \sum_{k=0}^n C_{n-k} s^{n-k} t^k,$$

where $C_{n-k} \in \Omega$ for $k = 0, 1, \dots, n$. Further, since p_0 is a point of intersection, $G(1, 0) = 0$. Thus $C_n = 0$.

It suffices to show that there exists a rational point p such that $C_{n-1} = 0$. In this case, $G(s, t)$ would certainly be divisible by t^2 .

In the following we use results from the theory of differentiation in polynomial rings over an arbitrary field, an account of which can be found in [5].

From (2.2) we obtain

$$\frac{\partial G}{\partial t} = C_{n-1} s^{n-1} + \sum_{k=2}^n k C_{n-k} s^{n-k} t^{k-1}.$$

Thus, $\left[\frac{\partial G}{\partial t} \right] (1, 0) = C_{n-1}$. Using (2.1), we get

$$\frac{\partial G}{\partial t} = \frac{\partial F}{\partial X} \cdot \frac{\partial X}{\partial t} + \frac{\partial F}{\partial Y} \cdot \frac{\partial Y}{\partial t} + \frac{\partial F}{\partial Z} \cdot \frac{\partial Z}{\partial t}.$$

Let $\left[\frac{\partial F}{\partial X} \right]_{(a_1, a_2, a_3)} = c_1$, $\frac{\partial F}{\partial Y}_{(a_1, a_2, a_3)} = c_2$, and

$\frac{\partial F}{\partial Z}_{(a_1, a_2, a_3)} = c_3$. Then, as $\frac{\partial X}{\partial t} = b_1$, $\frac{\partial Y}{\partial t} = b_2$, and $\frac{\partial Z}{\partial t} = b_3$,

$$c_{n-1} = \left[\frac{\partial G}{\partial t} \right]_{(1,0)} = c_1 b_1 + c_2 b_2 + c_3 b_3 .$$

Suppose $c_1 = c_2 = c_3 = 0$. Then $c_{n-1} = 0$ for each point p .

If p is rational, then the line determined by p_0 and p is rational.

Suppose c_1 , c_2 , and c_3 are not all zero. Without loss of generality, suppose $c_1 \neq 0$. Let b_2 and b_3 be arbitrary elements in K such that $(b_2, b_3) \neq (0,0)$ and $(b_2, b_3) \neq (a_2, a_3)$. Define

$$b_1 = - \frac{(c_2 b_2 + c_3 b_3)}{c_1} .$$

Then p is rational and

$$\left[\frac{\partial G}{\partial t} \right]_{(1,0)} = 0$$

for the point p . This completes the proof.

The space $P(\Omega)$ is a type of completion of $A(\Omega)$; in fact, we will show that $A(\Omega)$ can be embedded in $P(\Omega)$. Because $P(\Omega)$ is "complete," it is helpful in the study of affine curves to consider the projections they define in $P(\Omega)$. This shall become clearer as

we proceed.

First, let us show that $A(\Omega)$ can be embedded in $P(\Omega)$.

Define the mapping π on $A(\Omega)$ as follows:

$$\pi : (x, y) \rightarrow (x, y, 1)^{\wedge}.$$

The map π is one-to-one, but it is not onto. The points in $P(\Omega)$ which do not belong to the image of $A(\Omega)$ under π are of the form $(x, y, 0)^{\wedge}$, with x and y not both zero, and they are called points at infinity.

Two points at infinity determine a line in $P(\Omega)$. It is easy to show that the polynomial which determines this line is of the form

$$F(X, Y, Z) = c Z,$$

$c \in \Omega \setminus \{0\}$. Clearly, a point is on this line if and only if it is a point at infinity. For this reason, this line is called the line at infinity.

Define the map $\hat{\pi}$ on $\Omega[X, Y]$ as follows:

$$\hat{\pi} : f(X, Y) \rightarrow Z^n \cdot f\left(\frac{X}{Z}, \frac{Y}{Z}\right),$$

where degree $f = n$. The image of $f(X, Y)$ is a homogeneous polynomial and has degree n . Therefore, it determines a curve in $P(\Omega)$.

Suppose C is the curve in $A(\Omega)$ determined by f and $\hat{C}$ is the curve in $P(\Omega)$ determined by $\hat{\pi}(f)$. $\hat{C}$ is called the projection of C in $P(\Omega)$. The image of C under π is a subset

of $\hat{C}$; or, stated differently, the zeros of f are preserved under π as zeros of $\hat{\pi}(f)$. To see this, let (x, y) belong to $A(\Omega)$, with x and y not both zero, and suppose $f(x, y) = 0$. Let $p = (x, y, 1)^\wedge$. Then

$$[\hat{\pi}(f)]_p = 1^n \cdot f(x, y) = 0.$$

The projective curve $\hat{C}$ may include some points which are not images under π of any points on C . These, of course, are points at infinity. For example, consider the polynomial

$$f(X, Y) \equiv X^2 - Y.$$

By the definition of $\hat{\pi}$,

$$\hat{\pi}(f) \equiv X^2 - YZ.$$

The point $(0, 1, 0)^\wedge$ is a zero of $\hat{\pi}(f)$.

It is easy to verify that $\hat{\pi}$ is a ring isomorphism from $\Omega[X, Y]$ into $\Omega[X, Y, Z]$. Thus, if $f(X, Y) \in \Omega[X, Y]$ is absolutely irreducible, then, as the range of $\hat{\pi}$ is the set of all homogeneous polynomials in $\Omega[X, Y, Z]$ and the factors of a homogeneous polynomial are homogeneous, it follows that $\hat{\pi}(f)$ is absolutely irreducible, also.

The Hilbert Nullstellensatz, which we used earlier to show that the affine curve determined by an absolutely irreducible polynomial is absolutely irreducible, can also be applied to show that a curve in $P(\Omega)$ determined by an absolutely irreducible polynomial in $\Omega[X, Y, Z]$ is absolutely irreducible.

CHAPTER III

LANG-WEIL THEOREM AND SOME CONSEQUENCES

Throughout this chapter we shall suppose that K is a finite field of order q . We wish to show that given a positive integer d , if q is large relative to d , then for any polynomial $f(X, Y) \in K[X, Y]$ such that $f(X, Y) \neq X - Y$, $\deg f = d$, and f is absolutely irreducible, there exists a rational point in $A(\Omega)$ which is a zero of $f(X, Y)$ but is not a zero of $g(X, Y) = X - Y$. To do this, we use a powerful theorem by S. Lang and A. Weil [4] which gives an estimate for the number of rational points on an absolutely irreducible, rational curve in $P(\Omega)$. Using elementary algebraic geometry, we will demonstrate the Lang-Weil Theorem for polynomials of degree two. In fact, we will show that there are exactly $q + 1$ rational points on the projective curve in $P(\Omega)$ determined by an absolutely irreducible, rational curve in $A(\Omega)$ of degree two.

To begin with, let us consider a line in $P(\Omega)$ which is the projection of a rational line in $A(\Omega)$.

Theorem 3.1. Suppose a given rational line in $A(\Omega)$ is determined by the polynomial

$$f(X, Y) = aX + bY + c,$$

where a, b , and c are in K . Then the projection of that line in $P(\Omega)$ contains exactly $q + 1$ rational points.

Proof. One of a and b is not zero. Without loss of

generality, assume $a \neq 0$.

The projection of the given line is the set of points in $P(\Omega)$ which are zeros of the polynomial

$$(3.1) \quad F(X, Y, Z) \equiv aX + bY + cZ.$$

Clearly, given (d_2, d_3) , an arbitrarily fixed ordered pair in $K \times K$, there exists a unique $d_1 \in K$ such that (d_1, d_2, d_3) is a zero of (3.1). Since the order of $K \times K$ is q^2 , there are q^2 zeros of (3.1) of the type (d_1, d_2, d_3) . Call the set of all such 3-tuples R .

Let $R^* = R \setminus \{0\}$. Suppose (c_1, c_2, c_3) is an arbitrary element in R^* . For each $h \in K \setminus \{0\}$, $(c_1 h, c_2 h, c_3 h) \in R^*$, also. Since the order of $K \setminus \{0\}$ is $q - 1$, there are $q - 1$ elements in R^* proportional to (c_1, c_2, c_3) . Therefore, R^* contains

$$\frac{q^2 - 1}{q - 1} = q + 1 \text{ distinct classes of proportional elements.}$$

Let $\{(c_{1i}, c_{2i}, c_{3i})\}$, $i = 1, 2, \dots, q + 1$, be a maximal subset of R^* such that no two elements are proportional. Therefore, since R contains all the zeros in $K \times K \times K$ of (3.1), $\{(c_{1i}, c_{2i}, c_{3i})^\wedge\}$ is the set of all rational points in $P(\Omega)$ which are zeros of (3.1), $i = 1, 2, \dots, q + 1$. This completes the proof.

So, we see that the projection of an arbitrary rational line in $A(\Omega)$ contains exactly $q + 1$ rational points. Actually, any rational

line in $P(\Omega)$ contains $q + 1$ rational points. This result can be seen by showing that the line at infinity, which can be obtained from the zeros of the polynomial $F(X, Y, Z) \equiv cZ$, where $c \in K \setminus \{0\}$, contains exactly $q + 1$ rational points, because all other cases were considered in the preceding theorem.

Next, let us consider the projection of a curve in $A(\Omega)$ which is determined by an absolutely irreducible, rational polynomial of total degree two. First, however, consider the following lemma.

Lemma 3.1. Suppose $p = (a_1, a_2, a_3)^\wedge$ is a rational point in $P(\Omega)$. Then there exists a rational line in $P(\Omega)$ which does not contain p .

Proof. Suppose every rational line in $P(\Omega)$ contains p . Each polynomial

$$aX + bY + cZ \in K[X, Y, Z]$$

determines a rational line in $P(\Omega)$, and each rational line in $P(\Omega)$ can be obtained from the zeros of a polynomial of this type. Hence,

$$a_1x + a_2y + a_3z = 0$$

for each $(x, y, z) \in K \times K \times K$.

By Lemma 4.1, we have

$$a_1X + a_2Y + a_3Z \equiv 0.$$

Thus $a_1 = a_2 = a_3 = 0$. But $(0, 0, 0)^\wedge \notin P(\Omega)$. Hence, each rational line in $P(\Omega)$ can not contain p . This completes the proof.

Theorem 3.2. Let $f(X, Y) \in K[X, Y]$, and suppose $f(X, Y)$ is an absolutely irreducible polynomial of degree two. If C is the set of points in $A(\Omega)$ that are zeros of $f(X, Y)$ and $\hat{C}$ is the projection of C in $P(\Omega)$, then, if $\hat{C}$ contains one rational point, it contains exactly $q + 1$ rational points.

Proof. The polynomial which determines the curve $\hat{C}$ is

$$(3.2) \quad F(X, Y, Z) \equiv Z^2 \cdot f\left(\frac{X}{Z}, \frac{Y}{Z}\right).$$

Let $p_0 = (a_1, a_2, a_3)^\wedge$ be the given rational point on $\hat{C}$,

where a_1, a_2 , and a_3 belong to K . By the preceding lemma, there exists a rational line L in $P(\Omega)$ which does not contain p_0 .

Since L is rational, L contains exactly $q + 1$ rational points.

Let $p = (b_1, b_2, b_3)^\wedge$, where b_1, b_2 , and b_3 belong to

K , be an arbitrarily chosen rational point on L . The points p_0

and p determine a rational line in $P(\Omega)$, and parametric equations for that line are

$$X_i = a_i s + b_i t,$$

$i = 1, 2$, and 3 (See Chapter II). Denote this line by L' .

Since Ω is algebraically closed, we know L' intersects $\hat{C}$ exactly twice in $P(\Omega)$, counting multiplicities. One point of intersection is p_0 , clearly. Call the other p' , which may be p_0 itself. Define the map $\tau(p) = p'$ from the rational points on L

into $\hat{C}$. τ is well-defined. If it were not, we could assert the existence of a line which intersected $\hat{C}$ three times, counting multiplicities.

The intersections of L with $\hat{C}$ can be obtained from the solutions in s and t to the equation

$$G(s,t) = F(a_1s + b_1t, a_2s + b_2t, a_3s + b_3t) = 0.$$

Because F is a homogeneous, rational polynomial of degree 2 and $a_i, b_i \in K$, $i = 1, 2$, and 3 ,

$$G(s,t) \equiv As^2 + Bst + Ct^2,$$

where A, B , and C are in K .

Since p_0 is a point of intersection, $F(1,0) = 0$. Hence, $A = 0$.

Suppose $B = C = 0$. In this case every ordered pair (s,t) satisfies the equation $Bst + Ct^2 = 0$, which implies that L' is contained in $\hat{C}$ as a proper subset. But this is impossible as f is absolutely irreducible.

Suppose $C = 0$. Then $s = 0$ and $t = 1$ is a solution to the equation $Bst = 0$. Hence, in this case the points of intersection are p_0 and p , which are both rational.

Suppose $C \neq 0$. If $B = 0$, then G becomes

$$G(s,t) = Ct^2.$$

Hence, in this case $p' = p_0$. If $B \neq 0$, the G can be expressed

as

$$G(s, t) = t(Bs + Ct) .$$

Since $t = 0$ corresponds to p_0 , the solutions of $Bs + Ct = 0$ must correspond to p' . Set $t = t'$, where $t' \in K \setminus \{0\}$.

Then $s' = \frac{Ct'}{B}$ belongs to $K \setminus \{0\}$, also. Hence, p' is rational.

We now show that τ is a one-to-one mapping from the rational points on L onto those on $\hat{C}$.

Each rational point p' on $\hat{C}$ together with p_0 determines a rational line which intersects $\hat{C}$ exactly twice, counting multiplicities. If $p' \neq p_0$, this is clear. If $p' = p_0$, this follows by Theorem 2.1. Since the intersection of two rational lines in $P(\Omega)$ is a rational point, τ is an onto map. Suppose p_1 and p_2 are rational points on L and $\tau(p_1) = \tau(p_2) = p'$. Then the line determined by p_0 and p' with the property described above intersects L exactly once. Thus $p_1 = p_2$. Hence, τ is a one-to-one correspondence between the rational points on L and $\hat{C}$. This completes the proof.

By a theorem from Chevalley [1], which will be stated and proved in the next chapter, the hypothesis in the preceding theorem that there exists a rational point on $\hat{C}$ is always fulfilled. Further, the fact that $\hat{C}$ was the projection of a rational curve in $A(\Omega)$ was

not essential to the proof of the theorem. Actually, any rational curve in $P(\Omega)$ which is determined by an absolutely irreducible, quadratic polynomial contains exactly $q + 1$ rational points.

The following is a theorem by S. Lang and A. Weil which gives an estimate for the number of rational points on a rational curve in $P(\Omega)$ determined by an absolutely irreducible polynomial of degree d [4]. Denoting the number of rational points by N , we have

Theorem 3.3. Let $h(X, Y, Z)$ be a homogeneous polynomial in $K[X, Y, Z]$. If $\text{degree } h = d \geq 1$ and $h(X, Y, Z)$ is absolutely irreducible, then there exists a constant A , which depends only on d , such that

$$|N - q| \leq d^2 q^{1/2} + A.$$

Let d be a positive integer. Then, as a result of this theorem, if we choose K so that q is large enough relative to d , the curve in $P(\Omega)$ determined by any homogeneous polynomial in $K[X, Y, Z]$ of degree d contains arbitrarily many rational points.

In the following theorem, let N be the number of rational points on the curve in $P(\Omega)$ which is the projection of the curve in $A(\Omega)$ determined by $f(X, Y)$.

Theorem 3.4. Suppose $f(X, Y) \neq X - Y$ belongs to $K[X, Y]$ and let $\text{degree } f = d \geq 1$. If $N > 2d$, then there exists a rational point (a, b) in $A(\Omega)$ such that $f(a, b) = 0$ and $a \neq b$.

Proof. Denote by C and L , respectively, the curves determined by $f(X, Y)$ and the line $X = Y$ in $A(\Omega)$. Let

$$F(X, Y, Z) \equiv Z^d \cdot f\left(\frac{X}{Z}, \frac{Y}{Z}\right)$$

and

$$G(X, Y, Z) \equiv X - Y,$$

and denote the corresponding curve and line in $P(\Omega)$ by $\hat{C}$ and $\hat{L}$, respectively. Then $\hat{C}$ is the projection of C and $\hat{L}$ is the projection of L .

Since $f(X, Y)$ is absolutely irreducible, $\hat{C}$ is absolutely irreducible. According to Jenner ([3], page 47), since $\text{degree } F = d$, $\hat{L}$ has at most d distinct intersections with $\hat{C}$. For the same reason, $\hat{C}$ has at most d distinct intersections with the line at infinity. Hence, $\hat{C}$ contains at most $2d$ rational points which are either on $\hat{L}$ or the line at infinity.

Since $N > 2d$, there exists a rational point $(x, y, 1)^\wedge$ on $\hat{C}$ such that $x \neq y$. Thus, C contains a rational point which is not on L . This completes the proof.

Corollary 3.1. Suppose $f(X, Y) \in K[X, Y]$, $f(X, Y) \neq X - Y$, and the total degree of f is $d \geq 1$. Then, if $f(X, Y)$ is absolutely irreducible and q is large relative to d , $f(X, Y)$ has at least one zero $(x, y) \in K \times K$ such that $x \neq y$.

Proof. The proof is immediate from the results of Theorems 3.3 and 3.4.

RESULTS OF CHEVALLEY APPLIED TO QUADRATIC POLYNOMIALS

In this chapter we shall suppose that K is a finite field of order q . We wish to prove that a curve in $P(\Omega)$ which is determined by an absolutely irreducible, rational polynomial of degree two contains at least one rational point.

Define $A_n(K)$ to be the set of all n -tuples $(x_1, \dots, x_n)$ such that $x_i \in K, i = 1, 2, \dots, n$. If $x_i = 0, i = 1, 2, \dots, n$, denote $(x_1, \dots, x_n)$ by 0 .

For some positive integer n , let $F^*(X_1, \dots, X_n) \in K[X_1, \dots, X_n]$.

F^* is said to be in reduced form if no indeterminate in any term of F^* has an exponent greater than $q - 1$.

Suppose $F(X_1, \dots, X_n)$ is a polynomial in $K[X_1, \dots, X_n]$.

Then $F^*(X_1, \dots, X_n) \in K[X_1, \dots, X_n]$ is called a reduced form of F

if F^* is in reduced form and F^* is congruent to F with respect to the congruence relation determined by the ideal

$$(X_1^q - X_1, \dots, X_n^q - X_n) = \mathfrak{a} \text{ of } K[X_1, \dots, X_n].$$

Suppose F^* is a reduced form of F . By definition, we know

$$F \equiv F^* \pmod{\mathfrak{a}}.$$

Thus, for some $G_i \in K[X_1, \dots, X_n]$, $i = 1, 2, \dots, n$,

$$F - F^* \equiv \sum_{i=1}^n G_i (X_i^q - X_i) .$$

Since $a^q - a = 0$ for each $a \in K$,

$$(F - F^*)(x_1, \dots, x_n) = 0$$

for each n -tuple in $A_n(K)$. Hence, F and F^* determine identical maps from $A_n(K)$ into K . In particular, the zeros of F and F^* in $A_n(K)$ are the same.

Lemma 4.1. (Chevalley). Suppose $F(X_1, \dots, X_n) \in K[X_1, \dots, X_n]$ and let F be in reduced form. If each n -tuple in $A_n(K)$ is a zero of F , then F is the zero polynomial.

Proof. The proof is by induction on n . If $n = 1$, then F has the form

$$F \equiv \sum_{p=1}^q a_{q-p} X_1^{q-p},$$

where $a_{q-p} \in K$ for each $p = 1, 2, \dots, n$, because the order of

K is q and F was given to be in reduced form. By hypothesis, F has q zeros in $A_1(K)$. Therefore, since $q - 1 \leq \text{degree } F < q$, F must be the zero polynomial.

Assume the result for $n - 1$ indeterminates. For n indeterminates we have

$$F \equiv A_{q-1} X_n^{q-1} + A_{q-2} X_n^{q-2} + \dots + A_0,$$

where $A_{q-p} \in K[X_1, \dots, X_{n-1}]$ and is in reduced form for each

$p = 1, 2, \dots, q$. Let $(x_1, \dots, x_{n-1})$ be an arbitrarily fixed $(n-1)$ -tuple

in $A_{n-1}(K)$. By hypothesis, $F(x_1, \dots, x_{n-1}, x_n) = 0$ for each

$x_n \in K$. Thus, the initial induction step implies

$$\sum_{p=1}^q A_{q-p}(x_1, \dots, x_{n-1}) X_n^{q-p} \equiv 0.$$

So, $A_{q-p}(x_1, \dots, x_{n-1}) = 0$, $p = 1, 2, \dots, q$. As $(x_1, \dots, x_{n-1})$ was

chosen arbitrarily, the induction hypothesis implies $A_{q-p} \equiv 0$,

$p = 1, 2, \dots, q$. Therefore, $F \equiv 0$. This completes the proof.

Lemma 4.2 (Chevalley). Suppose $F(X_1, \dots, X_n) \in K[X_1, \dots, X_n]$

and let F be in reduced form. If each n -tuple in $A_n(K)$ except

0 is a zero of F and $F(0) = 1$, then

$$F \equiv (-1)^n \prod_{i=1}^n (X_i^{q-1} - 1).$$

Proof. Define the polynomial $G(X_1, \dots, X_n)$ as follows:

$$G \equiv (-1)^n \prod_{i=1}^n (X_i^{q-1} - 1).$$

Clearly, $G(0) = 1$. If $a = (a_1, \dots, a_n) \in A_n(K)$ and a is not

0 , then $a_i \neq 0$ for some $i = 1, 2, \dots, n$. Suppose $a_k \neq 0$,

$1 \leq k \leq n$. Since the order of K is q , $a_k^{q-1} - 1 = 0$. Thus,
 $G(a) = 0$.

Since $F(0) = G(0)$ and each n -tuple in $A_n(K)$ other than 0 is a zero of both F and G , every n -tuple in $A_n(K)$ is a zero of the polynomial $F - G$. As $F - G$ is in reduced form, by Lemma 4.1, $F - G \equiv 0$. Hence, $F \equiv G$. This completes the proof.

Theorem 4.1 (Chevalley). Suppose $F_1, \dots, F_s$ are polynomials in $K[X_1, \dots, X_n]$ such that $F_j(0) = 0$, $j = 1, 2, \dots, s$, and
 $\sum_{j=1}^s \text{degree } F_j < n$. Then there exists an n -tuple in $A_n(K)$ other than
 0 which is a zero for each F_j , $j = 1, 2, \dots, s$.

Proof. Define $F(X_1, \dots, X_n)$ as

$$F \equiv (-1)^s \prod_{j=1}^s (F_j^{q-1} - 1).$$

Suppose there does not exist an n -tuple in $A_n(K)$ other than 0 which is a zero of each F_j , $i = 1, 2, \dots, s$.

As $F_j(0) = 0$ for each $j = 1, 2, \dots, s$, $F(0) = 1$. Suppose $a = (a_1, \dots, a_n) \in A_n(K)$ and a is not 0 . By supposition, there exists F_k , $1 \leq k \leq s$, such that $F_k(a) \neq 0$. Because the order of K is q , $F_k(a)^{q-1} - 1 = 0$. Thus, $F(a) = 0$.

Let F^* be the reduced form of F . Since $F^*(0) = 1$ and

every other n -tuple in $A_n(K)$ is a zero of F^* , Lemma 4.2 implies

$$F^* \equiv (-1)^n \prod_{i=1}^n (X_i^{q-1} - 1).$$

The degree $F^* = n(q-1)$. Hence, as F^* is in reduced form, degree $F \geq n(q-1)$.

By the definition of F , the degree of F is

$$\left(\sum_{j=1}^s \text{degree } F_j \right) (q-1). \text{ Thus, } \sum_{j=1}^s \text{degree } F_j < n, \text{ degree } F < n(q-1).$$

But this is impossible, as degree $F^* = n(q-1)$. Therefore, the supposition that 0 is the only n -tuple in $A_n(K)$ which is a zero of each polynomial $F_1, \dots, F_s$ is false. This completes the proof.

Lemma 4.3. Suppose $F(X, Y, Z)$ is a homogeneous polynomial in $K[X, Y, Z]$ of degree two. If F is absolutely irreducible, then the curve in $P(\Omega)$ determined by F contains a rational point.

Proof. By the preceding theorem, since F has three indeterminates, degree $F = 2$, and F is homogeneous, there exists a non-zero 3-tuple $(a_1, a_2, a_3) \in A_3(K)$ such that $F(a_1, a_2, a_3) = 0$. Thus, $(a_1, a_2, a_3)^\wedge$ is a rational point on the curve in $P(\Omega)$ determined by F . This completes the proof.

PERMUTATION POLYNOMIALS OF DEGREE 4

A permutation polynomial over the finite field K of q elements is a polynomial $f \in K[X]$ such that the map $x \rightarrow f(x)$ on K is a bijection. In this chapter we wish to determine the quartic permutation polynomials for any finite field K where q is sufficiently large. First, we wish to make a few observations, use of which can be made both now and in the next chapter.

Let $f(X) \equiv \sum_{i=0}^n a_i X^i \in K[X]$, where n is a positive integer

and $a_n = 1$. There is clearly no loss of generality by letting

$a_n = 1$, as a constant times a permutation polynomial is a permutation polynomial. Because K is a finite field, f is a permutation polynomial of K if and only if the map $x \rightarrow f(x)$ is one-to-one; i.e., $f(x) - f(y) = 0$ only if $x = y$ (for all $x, y \in K$).

Consider the polynomial

$$f(X) - f(Y) \equiv \sum_{i=1}^n a_i (X^i - Y^i) \in K[X, Y].$$

One can easily verify that

$$\frac{X^i - Y^i}{X - Y} \equiv \sum_{j+K=i-1} X^j Y^K,$$

where j and K are non-negative integers, $i = 1, 2, \dots, n$. Let

$$h_{i-1}(X, Y) \equiv \frac{X^i - Y^i}{X - Y}, \quad i = 1, 2, \dots, n.$$

Define $g(X, Y)$ as follows:

$$(5.1) \quad g(X, Y) \equiv \frac{f(X) - f(Y)}{X - Y}.$$

It follows from the above that

$$g(X, Y) \equiv \sum_{i=1}^n a_i h_{i-1}(X, Y) \in K[X, Y].$$

Also, since $f(X) - f(Y) \equiv (X - Y) \cdot g(X, Y)$, it follows that for $f(X)$ to be a permutation polynomial, it is necessary and sufficient that the zeros in $K \times K$ of $g(X, Y)$ all belong to the diagonal set $\{(x, x) \mid x \in K\}$. This assertion can be restated in geometrical terms as follows:

The rational points on the affine curve determined by $g(X, Y)$ all lie on the line $X = Y$.

Let C_4 be a positive constant such that if K is a finite field of order q with $q > C_4$, then each absolutely irreducible polynomial except $X - Y$ in $K[X, Y]$ of degree ≤ 3 has at least one rational zero which is not on the line $X = Y$. The results of Chapter III serve to justify this assumption.

Consider the quartic

$$f(X) = X^4 + aX^3 + bX^2 + cX + d \in K[X].$$

As was noted earlier, $f(X)$ is a permutation polynomial if and only if

all the rational points on the affine curve in $A(\Omega)$ determined by the polynomial

$$(5.2) \quad g(X, Y) \equiv X^3 + X^2Y + XY^2 + Y^3 + a(X^2 + XY + Y^2) + b(X + Y) + c$$

are on the line $X = Y$.

Suppose $g(X, Y)$ is absolutely irreducible. Then, whenever $q > C_4$, as degree $g = 3$, there exists a rational point (x, y) in $A(\Omega)$ such that $x \neq y$ and $g(x, y) = 0$. It follows, therefore, if $q > C_4$, a necessary condition for $f(X)$ to be a permutation polynomial is that $g(X, Y)$ must factor in $\Omega[X, Y]$.

If $g(X, Y)$ is not absolutely irreducible, then, as the total degree $g = 3$, $g(X, Y)$ has a linear factor in $\Omega[X, Y]$.

Lemma 5.1. If $g(X, Y)$ is not absolutely irreducible, then it must have a factor of the form $X + Y + \gamma \in \Omega[X, Y]$.

Proof. It is well known that

$$\frac{X^4 - Y^4}{X - Y} \equiv \prod_{n=1}^3 (X - i^n Y),$$

where i is a square-root of -1 in Ω . Thus, if $g(X, Y)$ has a linear factor in $\Omega[X, Y]$, it must be of the form $X + iY + \gamma_1$, $X - iY + \gamma_2$, or $X + Y + \gamma_3$. We can assume either $X + iY + \gamma_1$ or $X - iY + \gamma_2$ is a linear factor of $g(X, Y)$, since otherwise, we would be finished. Without loss of generality, suppose

$$g(X, Y) \equiv (X + iY + \gamma) \cdot Q(X, Y).$$

Since $g(X, Y)$ is symmetric with respect to X and Y , we can obtain the following identity by interchanging X and Y .

$$\begin{aligned} g(X, Y) &\equiv (Y + iX + \gamma) \cdot Q(Y, X) \\ &\equiv (-iY + X - i\gamma) \cdot iQ(Y, X) \\ &\equiv (X - iY - i\gamma) \cdot Q^*(X, Y). \end{aligned}$$

Hence, $g(X, Y)$ also has the factor $X - iY - i\gamma$.

If the characteristic of K is not 2, then $X - iY - i\gamma \neq X + iY + \gamma$. So, as the total degree $g = 3$, $g(X, Y)$ must have a factor of the form $X + Y + \lambda$, also.

If the characteristic of K is 2, then $X + iY + \gamma \equiv X + Y + \gamma$. This completes the proof.

We now consider the problem of factoring $g(X, Y)$ in $\Omega[X, Y]$. By the preceding lemma, if $g(X, Y)$ factors in $\Omega[X, Y]$, we can say

$$(5.3) \quad g(X, Y) \equiv (X + Y + \gamma)(X^2 + Y^2 + \mu X + \eta Y + \delta),$$

for some γ , μ , η , and δ in Ω . In order to have such a factorization, γ , μ , η , and δ must satisfy the following equations, which are obtained by multiplying this factorization out and comparing the results to (5.2).

$$\gamma + \mu = a$$

$$(5.4) \quad \mu + \eta = a$$

$$\gamma + \eta = a.$$

$$(5.5) \quad \begin{aligned} \gamma\mu + \delta &= b \\ \gamma\eta + \delta &= b. \end{aligned}$$

$$(5.6) \quad \gamma\delta = c.$$

The augmented matrix obtained from equations (5.4) is

$$(5.7) \quad \begin{bmatrix} 1 & 1 & 0 & a \\ 0 & 1 & 1 & a \\ 1 & 0 & 1 & a \end{bmatrix}.$$

Suppose the characteristic of K is not 2. Then the row reduced form of (5.7) is

$$(5.8) \quad \begin{bmatrix} 1 & 0 & 0 & a/2 \\ 0 & 1 & 0 & a/2 \\ 0 & 0 & 1 & a/2 \end{bmatrix}.$$

Thus, $\gamma = a/2 \in K$.

Theorem 5.1. Suppose the characteristic of K is not 2
and $q > C_4$. Then there are no quartic permutation polynomials over
 K .

Proof. From the preceding, we have that $X + Y + a/2 | g(X, Y)$ is a necessary condition for $f(X)$ to be a permutation polynomial. As the characteristic of K is not 2, $X + Y + a/2 \neq X - Y$. The polynomial $X + Y + a/2$, and hence, $g(X, Y)$, has a zero (x, y) in $K \times K$ such that $x \neq y$. Therefore, $f(X)$ cannot be a permutation polynomial of K . This completes the proof.

Suppose the characteristic of K is 2. Then the row reduced

form of (5.7) is

$$(5.9) \quad \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & a \\ 0 & 0 & 0 & a \end{bmatrix}.$$

Hence, in order for $g(X, Y)$ to have a linear factor, it is necessary that $a = 0$.

Theorem 5.2. Suppose the characteristic of K is 2 and
 $q > C_4$. Then

$$f(X) \equiv X^4 + bX^2 + cX + d \in K[X]$$

is a permutation polynomial of K if and only if

$$h(X) \equiv X^3 + bX + c$$

has no non-zero zeros in K .

Proof. Since $a = 0$ and the characteristic of K is 2 , from the above, it is easy to verify that

$$\begin{aligned} g(X, Y) &\equiv (X + Y)^3 + b(X + Y) + c \\ &\equiv h(X + Y). \end{aligned}$$

Let $f(X)$ be a permutation polynomial of K , and suppose $\mu \in K$, $\mu \neq 0$, and $h(\mu) = 0$. As $h(\mu) = 0$, $h(X) \equiv (X - \mu) \cdot Q(X)$, where $Q(X) \equiv \frac{h(X)}{X - \mu} \in K[X]$. Hence, $h(X + Y) \equiv (X + Y - \mu) \cdot Q(X + Y)$. Therefore, $(X + Y - \mu)$ is a linear factor of $g(X, Y)$. But this is impossible, since $X + Y - \mu$, and thus, $g(X, Y)$, has rational zeros which are not on the line $X = Y$.

Suppose $h(X)$ has no non-zero zeros in K , and assume $f(X)$ is not a permutation polynomial of K . Then there exists an ordered pair $(x, y) \in K \times K$ such that $x \neq y$, or $x + y \neq 0$, and $g(x, y) = 0$. Hence, as $g(X, Y) \equiv h(X + Y)$, $h(x + y) = 0$. But this is impossible, because $x + y \neq 0$ and $x + y \in K$. This completes the proof.

LINEAR FACTORIZATION OF $g(X, Y)$

Suppose $f(X)$ is a 5-th degree, primary polynomial in $K[X]$, where K is a finite field with order sufficiently large. In this chapter we wish to determine necessary and sufficient conditions for f to be a permutation polynomial of K , where f is such that $g(X, Y)$ has a linear factor in $\Omega[X, Y]$. The reason for this condition will become evident. Further, we shall deduce some results which will be employed in later chapters.

The results of Chapter III imply the existence of a number C_5 such that each absolutely irreducible polynomial, except $X - Y$, over a finite field with order greater than C_5 has a rational zero which is not on the line $X = Y$. Throughout this chapter we shall assume that the order of K , q , is greater than C_5 .

Consider the polynomial

$$(5.1) \quad f(X) = X^5 + aX^4 + bX^3 + cX^2 + dX + e \in K[X].$$

In the preceding chapter, it was determined that $f(X)$ is a permutation polynomial of K if and only if the rational zeros of

$$(6.2) \quad g(X, Y) = X^4 + X^3Y + X^2Y^2 + XY^3 + Y^4 + \\ a(X^3 + X^2Y + XY^2 + Y^3) + \\ b(X^2 + XY + Y^2) + c(X + Y) + d$$

all lie on the line $X = Y$.

Suppose $g(X, Y)$ is absolutely irreducible. Then, as $q > C_5$,

$g(X, Y)$ has a rational zero off the line $X = Y$. Therefore, a necessary condition for $f(X)$ to be a permutation polynomial is $g(X, Y)$ must be reducible in $\Omega[X, Y]$.

The total degree of $g(X, Y)$ is 4. This implies that if $g(X, Y)$ is reducible, it must have either a factor of total degree one or a factor of total degree two. In the following section, we shall suppose that $g(X, Y)$ has a linear factor in $\Omega[X, Y]$.

Lemma 6.1. Suppose K is a finite field and $q > C_5$.

Further, let $f(X)$ be a permutation polynomial of K . Then, if $g(X, Y)$ has one linear factor in $\Omega[X, Y]$, it decomposes completely into linear factors in $\Omega[X, Y]$.

Proof. Let $h_1 \in \Omega[X, Y]$ be a linear factor of $g(X, Y)$. So

$$(6.3) \quad g(X, Y) = h_1 \cdot z,$$

where $z \in \Omega[X, Y]$ and the total degree $z = 3$. Suppose z is irreducible in $\Omega[X, Y]$.

Let E be the minimal Galois extension field of K which contains all the coefficients of h_1 and z . Let σ be an

arbitrary K -automorphism in the Galois group of $E|K$, and denote by $\hat{\sigma}$ the automorphism determined by "lifting" σ to the polynomial ring $E[X, Y]$. As $g(X, Y) \in K[X, Y]$, $\hat{\sigma}(g) = g$. Since h_1 and z are irreducible, by unique factorization we have

$$g(X, Y) = \hat{\sigma}(h_1 \cdot z) = h_1 \cdot z.$$

Hence, because the total degree $h_1 = 1$ and the total degree $z = 3$,

$$\hat{\sigma}(h_1) = h_1 \quad \text{and} \quad \hat{\sigma}(z) = z.$$

As σ was chosen arbitrarily and since $\hat{\sigma}(z) = z$, the coefficients of z must belong to the fixed field of the Galois group, which is K . Hence, $z \in K[X, Y]$. Since $q > C_5$ and, by supposition, z is irreducible in $\Omega[X, Y]$, z must have a rational zero not on the line $X = Y$. Since this zero would also be a zero of $g(X, Y)$, we have a contradiction because $f(X)$ is a permutation polynomial of K . Hence, z must be reducible.

Since the total degree $z = 3$ and z is reducible, it must have a linear factor $h_2 \in \Omega[X, Y]$. Hence

$$g(X, Y) = h_1 \cdot h_2 \cdot w,$$

where $w \in \Omega[X, Y]$ and the total degree $w = 2$. Suppose w is irreducible in $\Omega[X, Y]$.

Let E^* be the minimal Galois extension field of K which contains all the coefficients of h_1 , h_2 , and w . Let σ be an

arbitrary K -automorphism in the Galois group of $E^*|K$, and define

$\hat{\sigma}$ as before. As $g \in K[X, Y]$, $\hat{\sigma}(g) = g$. Since h_1, h_2 , and w are irreducible, by unique factorization,

$$g(X, Y) = \hat{\sigma}(h_1 \cdot h_2 \cdot w) = h_1 \cdot h_2 \cdot w.$$

Hence, as the total degree $h_1 = \text{total degree } h_2 = 1$ and total degree $w = 2$,

$\hat{\sigma}(w) = w$. As before, since σ was chosen arbitrarily, $\hat{\sigma}(w) = w$ implies that $w \in K[X, Y]$.

Since $q > C_5$ and w is irreducible in $\Omega[X, Y]$, w has a rational zero not on the line $X = Y$. But this is impossible since $f(X)$ is a permutation polynomial of K . Hence, as the total degree $w = 2$, w must factor linearly in $\Omega[X, Y]$. This completes the proof.

Suppose that $g(X, Y)$ has a linear factor $X + \gamma Y + \mu$. In order for this to happen, $X + \gamma Y$ must divide the homogeneous part of highest degree of $g(X, Y)$. As $\frac{X^5 - Y^5}{X - Y}$ is the homogeneous part of highest degree of $g(X, Y)$, $\gamma = -\zeta$, where ζ is one of the 5-th roots of unity in Ω which are zeros of

$$(6.4) \quad A(X) = 1 + X + X^2 + X^3 + X^4.$$

One can verify directly that

$$\begin{aligned} \frac{X^5 - Y^5}{(X-Y)(X - \zeta Y)} &= X^3 + (1 + \zeta)X^2Y + (1 + \zeta + \zeta^2)XY^2 + \\ &+ (1 + \zeta + \zeta^2 + \zeta^3)Y^3. \end{aligned}$$

Thus, the factorization of $g(X, Y)$ takes the form

$$(6.5) \quad g(X, Y) = (X - \zeta Y + \mu) [(X^3 + (1 + \zeta)X^2Y + (1 + \zeta + \zeta^2)XY^2 + (1 + \zeta + \zeta^2 + \zeta^3)Y^3) + (\beta_0 X^2 + \beta_1 XY + \beta_2 Y^2) + (\lambda_0 X + \lambda_1 Y) + \delta],$$

where $\beta_0, \beta_1, \beta_2, \lambda_0, \lambda_1$, and δ are to be determined.

As $g(X, Y)$ was defined in (6.2), the homogeneous part of degree 3 of $g(X, Y)$ is

$$(6.6) \quad aX^3 + aX^2Y + aXY^2 + aY^3.$$

From (6.5), it follows that the homogeneous part of degree 3 of $g(X, Y)$ must also equal

$$(6.7) \quad X(\beta_0 X^2 + \beta_1 XY + \beta_2 Y^2) - \zeta Y(\beta_0 X^2 + \beta_1 XY + \beta_2 Y^2) + \mu(X^3 + (1 + \zeta)X^2Y + (1 + \zeta + \zeta^2)XY^2 + (1 + \zeta + \zeta^2 + \zeta^3)Y^3).$$

By equating coefficients of (6.6) and (6.7), we determine the following system of equations

$$(6.8) \quad \begin{aligned} \beta_0 + \mu &= a \\ -\zeta\beta_0 + \beta_1 + (1 + \zeta)\mu &= a \\ -\zeta\beta_1 + \beta_2 + (1 + \zeta + \zeta^2)\mu &= a \\ -\zeta\beta_2 + (1 + \zeta + \zeta^2 + \zeta^3)\mu &= a. \end{aligned}$$

The augmented matrix of this system is

$$(6.9) \quad \begin{bmatrix} 1 & 0 & 0 & 1 & a \\ -\zeta & 1 & 0 & 1 + \zeta & a \\ 0 & -\zeta & 1 & 1 + \zeta + \zeta^2 & a \\ 0 & 0 & - & 1 + \zeta + \zeta^2 + \zeta^3 & a \end{bmatrix} .$$

Starting with the first row and working downward in (6.9), successively add ζ times each row to the row immediately below. By doing so, one produces the following row reduced form of (6.9).

$$(6.10) \quad \begin{bmatrix} 1 & 0 & 0 & 1 & a \\ 0 & 1 & 0 & 1 + 2\zeta & a(1 + \zeta) \\ 0 & 0 & 0 & 1 + 2\zeta + 3\zeta^2 & a(1 + \zeta + \zeta^2) \\ 0 & 0 & 0 & 1 + 2\zeta + 3\zeta^2 + 4\zeta^3 & a(1 + \zeta + \zeta^2 + \zeta^3) \end{bmatrix} .$$

Since ζ is a zero of $A(X) = 1 + X + X^2 + X^3 + X^4$,

$$(6.11) \quad a(1 + \zeta + \zeta^2 + \zeta^3) = -a\zeta^4 .$$

Also,

$$(6.12) \quad 1 + 2\zeta + 3\zeta^2 + 4\zeta^3 = A'(\zeta) .$$

As

$$(6.13) \quad (X - 1)A(X) = X^5 - 1,$$

we can obtain that

$$(6.14) \quad (X - 1)A'(X) - A(X) = 5X^4 .$$

By substituting ζ , it follows from (6.14) that

$$(6.15) \quad (\zeta - 1)A'(\zeta) = 5\zeta^4,$$

as $A(\zeta) = 0$.

Suppose now that the characteristic of K is not 5. Then $\zeta \neq 1$, since ζ is a zero of $A(X)$ and $A(1) = 5 \neq 0$. Hence, from (6.15) we get

$$(6.16) \quad A'(\zeta) = \frac{5\zeta^4}{\zeta-1} \neq 0,$$

since $\zeta - 1 \neq 0$.

Consider the matrix (6.10). Since the fourth element in the last row is non-zero by well-known theorems from linear algebra the system of equations (6.8) is uniquely solvable. Utilizing (6.11) and (6.12), we see from the last row of (6.10) that

$$\frac{5\zeta^4}{\zeta-1} \mu = -a\zeta^4,$$

or

$$(6.17) \quad \mu = \frac{a}{5} (1 - \zeta).$$

Theorem 6.1. Suppose K is a finite field and $q > 5$.

Further, suppose $f(X)$ is a permutation polynomial of K and $5 \nmid \deg f$.

Then, if $g(X, Y)$ has a linear factor,

$$(6.18) \quad g(X, Y) = \prod_{n=1}^4 [X - \zeta^n Y + \frac{a}{5}(1 - \zeta^n)],$$

where ζ is a primitive 5-th root of unity in Ω .

Proof. By Lemma 6.1, since $g(X, Y)$ has a linear factor and $f(X)$ is a permutation polynomial, $g(X, Y)$ decomposes linearly in $\Omega[X, Y]$. So

$$(6.19) \quad g(X, Y) = \prod_{i=1}^4 (X + \alpha_i Y + \mu_i),$$

with $\alpha_i, \mu_i \in \Omega$, $i = 1, 2, 3$, and 4 . From (6.18) it follows that

$$(6.20) \quad \frac{X^5 - Y^5}{X - Y} = \prod_{i=1}^4 (X + \alpha_i Y).$$

As noted earlier, $\alpha_1 = -\zeta$, where ζ is some zero of $A(X)$.

Since 5 is prime, ζ is a primitive 5-th root of unity in Ω . Hence,

$$\frac{X^5 - 1}{X - 1} = \prod_{n=1}^4 (X - \zeta^n).$$

It follows from this that

$$(6.21) \quad \frac{X^5 - Y^5}{X - Y} = \prod_{n=1}^4 (X - \zeta^n Y).$$

Using (6.20) and (6.21), we get

$$\prod_{n=1}^4 (X - \zeta^n Y) = \prod_{i=1}^4 (X + \alpha_i Y).$$

Thus, by renaming the α_i 's if necessary,

$$\alpha_i = -\zeta^i,$$

$i = 1, 2, 3$, and 4 .

It follows from (6.17), since $5 \nmid q$, that

$$\mu_i = \frac{a}{5} (1 - \zeta^i),$$

$i = 1, 2, 3$, and 4 . This completes the proof.

Hence, if $f(X)$ is a permutation polynomial of K , where $q > C_4$ and $5 \nmid q$, and $g(X, Y)$ has a linear factor in $\Omega[X, Y]$, from Theorem 6.1 we can conclude that

$$\begin{aligned} (6.22) \quad f(X) - f(Y) &= (X - Y)g(X, Y) \\ &= \prod_{n=0}^4 [X - \zeta^n Y + \frac{a}{5}(1 - \zeta^n)] \\ &= \prod_{n=0}^4 [(X + \frac{a}{5}) - (Y + \frac{a}{5})\zeta^n], \end{aligned}$$

where ζ is some primitive 5-th root of unity in Ω . By substituting $Y = 0$ in (6.22), we have

$$\begin{aligned} (6.23) \quad f(X) - e &= \prod_{n=0}^4 [(X + \frac{a}{5}) - \frac{a}{5}\zeta^n] \\ &= (X + \frac{a}{5})^5 - (\frac{a}{5})^5. \end{aligned}$$

Theorem 6.2. Suppose K is a finite field, $q > C_5$, and $5 \nmid q$. If f is such that g has a linear factor in $\Omega[X, Y]$, then f is a permutation polynomial of K if and only if

$$(6.24) \quad f(X) = (X + \frac{a}{5})^5 + d,$$

for some $a, d \in K$, and $5 \nmid q - 1$.

Proof. Suppose f is a permutation polynomial of K . It follows from (6.23) that f has the form

$$(6.25) \quad f(X) = \left(X + \frac{a}{5}\right)^5 + d,$$

for some $a, d \in K$. It remains to show that $5 \nmid q - 1$.

Suppose $5 \mid q - 1$. It suffices to show that $5 \mid q - 1$ implies that x^5 is not a permutation polynomial of K .

It is well-known that the multiplicative group of a finite field is cyclic. Hence, the multiplicative group of K , K^* , is cyclic. As $5 \mid q - 1$ and K^* is cyclic, it follows that there is a cyclic subgroup G of K^* such that order of G is 5. As order of G is 5 is prime, the order of each element of $G \setminus \{1\}$ is 5. It follows that x^5 is not a one-to-one map from K to K .

Suppose $f(X) = \left(X + \frac{a}{5}\right)^5 + d$ and $5 \nmid q - 1$. It follows that

$$\begin{aligned} f(X) - f(Y) &= \left(X + \frac{a}{5}\right)^5 - \left(Y + \frac{a}{5}\right)^5 \\ &= \prod_{n=0}^4 \left[\left(X + \frac{a}{5}\right) - \left(Y + \frac{a}{5}\right)\zeta^n\right], \end{aligned}$$

where ζ is a primitive 5-th root of unity in Ω . Hence,

$$g(X, Y) = \prod_{n=1}^4 \left[\left(X + \frac{a}{5}\right) - \left(Y + \frac{a}{5}\right)\zeta^n\right].$$

As $5 \nmid q$, $\zeta \neq 1$. Also, as $5 \nmid q - 1$, $\zeta \notin K$; otherwise K^*

would contain a subgroup of order 5. Let K be an arbitrary integer such that $1 \leq K \leq 4$. Hence, as $\zeta \notin K$,

$$(X + \frac{a}{5}) - (Y + \frac{a}{5})\zeta^K$$

has a rational zero (x, y) if and only if

$$x + \frac{a}{5} = 0$$

and

$$y + \frac{a}{5} = 0.$$

Clearly, this can only happen if $x = y = -\frac{a}{5}$.

Therefore, since K was chosen arbitrarily, the only rational zero of $g(X, Y)$ is $(-\frac{a}{5}, -\frac{a}{5})$, which is on the line $X = Y$. Hence, $f(X)$ is a permutation polynomial of K . This completes the proof.

Suppose now that the characteristic of K is 5. In this case,

$$X^5 - 1 = (X - 1)^5.$$

Hence, since $A(X) = \frac{X^5 - 1}{X - 1}$,

$$(6.26) \quad A(X) = (X - 1)^4.$$

As ζ is a zero of $A(X)$, we have by (6.26) that $\zeta = 1$. Since $\zeta = 1$ and characteristic of K is 5, the matrix (6.10) becomes

$$(6.27) \quad \begin{bmatrix} 1 & 0 & 0 & 1 & a \\ 0 & 1 & 0 & 3 & 2a \\ 0 & 0 & 1 & 1 & 3a \\ 0 & 0 & 0 & 0 & 4a \end{bmatrix}$$

It follows from the fourth row of this matrix, by well-known theorems from linear algebra, that in order for the original system (6.8) to be solvable, we must have

$$(6.28) \quad a = 0.$$

Setting $a = 0$ in (6.27), we obtain the following equalities.

$$(6.29) \quad \begin{aligned} \beta_0 &= -\mu \\ \beta_1 &= 2\mu \\ \beta_2 &= -\mu \end{aligned}$$

The homogeneous part of degree 2 of $g(X, Y)$ is

$$(6.30) \quad bX^2 + bXY + bY^2.$$

From the factorization of $g(X, Y)$ (6.5), we get that the homogeneous part of degree 2 of $g(X, Y)$ must also equal

$$(6.31) \quad \begin{aligned} &X(\lambda_0 X + \lambda_1 Y) - \zeta Y(\lambda_0 X + \lambda_1 Y) + \\ &\mu(\beta_0 X^2 + \beta_1 XY + \beta_2 Y^2). \end{aligned}$$

As $\zeta = 1$, by equating coefficients of (6.30) and (6.31) and utilizing (6.29), we get the following system of equations.

$$\begin{aligned}
 (6.32) \quad & \lambda_0 = b + \mu^2 \\
 & -\lambda_0 + \lambda_1 = b - 2\mu^2 \\
 & -\lambda_1 = b + \mu^2 .
 \end{aligned}$$

The augmented matrix of this system is

$$(6.33) \quad \begin{bmatrix} 1 & 0 & b + \mu^2 \\ -1 & 1 & b - 2\mu^2 \\ 0 & -1 & b + \mu^2 \end{bmatrix} .$$

The row reduced matrix of (6.33) is

$$(6.34) \quad \begin{array}{ccc} 1 & 0 & b + \mu^2 \\ 0 & 1 & 2b - \mu^2 \\ 0 & 0 & 3b \end{array} .$$

It follows from (6.34) that the system (6.32) is solvable if and only if

$$(6.35) \quad b = 0 .$$

Setting $b = 0$ in (6.32) and (6.34), we see that

$$\begin{aligned}
 (6.36) \quad & \lambda_0 = \mu^2 , \\
 & \lambda_1 = -\mu^2
 \end{aligned}$$

is a solution to the system (6.32).

The homogeneous part of degree 1 of $g(X, Y)$ is

$$(6.37) \quad cX + cY .$$

From (6.5) it follows that the homogeneous part of degree 1 of $g(X, Y)$ must also equal

$$(6.38) \quad X\delta - \zeta Y\delta + \mu(\lambda_0 X + \lambda_1 Y) .$$

As $\zeta = 1$, by equating coefficients of (6.37) and (6.38) and utilizing (6.36), we get the following system:

$$(6.39) \quad \begin{aligned} \delta &= c - \mu^3 \\ -\delta &= c + \mu^3 \end{aligned} .$$

Clearly, the equations in (6.39) are compatible if and only if

$$(6.40) \quad c = 0 .$$

Theorem 6.3. Suppose K is a finite field, $q > C_5$, and the characteristic of K is 5 . Then, if $f(X)$ is a permutation polynomial of K and $g(X, Y)$ has a linear factor in Ω , $f(X)$ has the form

$$f(X) = X^5 + dX + e \in K[X] .$$

Proof. This follows from the combined results of (6.28), (6.35), and (6.40). This completes the proof.

Theorem 6.4. Suppose K is a finite field such that $q > C_5$ and the characteristic of K is 5 . Then

$$(6.41) \quad f(X) = X^5 + dX + e \in K[X]$$

is a permutation polynomial of K if and only if either $d = 0$ or there does not exist $k \in K$ such that $k^4 = -d$.

Proof. As the characteristic of K is 5,

$$\begin{aligned}f(X) - f(Y) &= (X^5 - Y^5) + d(X - Y) \\&= (X - Y)^5 + d(X - Y) .\end{aligned}$$

Hence,

$$(6.42) \quad g(X, Y) = (X - Y)^4 + d .$$

If $d = 0$, it follows from (6.42) that all the zeros of $g(X, Y)$, including the rational ones, are on the line $X = Y$. Hence, in this case, $f(X)$ is a permutation polynomial of K .

Suppose there does not exist $k \in K$ such that $k^4 = -d$.

Let us suppose there exists $(x, y) \in K \times K$ such that $g(x, y) = 0$, also. As $g(x, y) = 0$,

$$(x - y)^4 + d = 0 ,$$

or

$$(6.43) \quad (x - y)^4 = -d .$$

Since $(x, y) \in K \times K$, $x - y \in K$. Thus, (6.43) contradicts our hypothesis that there does not exist $k \in K$ such that $k^4 = -d$. It follows, as $g(X, Y)$ has no rational zeros, that $f(X)$ is a permutation polynomial of K .

Suppose now that (6.41) is a permutation polynomial of K .

Let $\mu \in \Omega$ be such that $\mu^4 = -d$. Hence, $g(X, Y)$ has the following factorization in $\Omega[X, Y]$.

$$\begin{aligned}
 (6.44) \quad g(X, Y) &= (X - Y)^4 - \mu^4 \\
 &= [(X - Y)^2 - \mu^2] \cdot [(X - Y)^2 + \mu^2] \\
 &= [(X - Y) - \mu] \cdot [(X - Y) + \mu] \cdot \\
 &\quad [(X - Y) + 3\mu] \cdot [(X - Y) + 2\mu] .
 \end{aligned}$$

It follows from this factorization of $g(X, Y)$ that if $\mu \neq 0$ and $\mu \in K$, then $g(X, Y)$ has a rational zero off the line $X = Y$. For example, $g(\mu, 0) = 0$. But this contradicts $f(X)$ being a permutation polynomial of K . Hence, if $\mu \neq 0$, then $d \neq 0$ and $\mu \notin K$.

If $\mu = 0$, then it follows from (6.44) that all the rational zeros of $g(X, Y)$ are on the line $X = Y$, which is compatible with the fact that $f(X)$ is a permutation polynomial of K . As $\mu = 0$ and $d = -\mu^4$, $d = 0$. This completes the proof.

Theorem 6.5. Suppose K is a finite field, $q > C_5$, and the characteristic of K is 5 . If $f(X)$ is such that $g(X, Y)$ has a linear factor in $\Omega[X, Y]$, then $f(X)$ is a permutation polynomial of K if and only if

$$f(X) = X^5 + dX + e \in K[X],$$

where $d = 0$ or there does not exist $k \in K$ such that $K^4 = -d$.

Proof. This follows immediately from Theorems 6.3 and 6.4.

This completes the proof.

Suppose now that the irreducible factor of least total degree of g in $\Omega[X, Y]$ is quadratic. It follows, as the total degree $g = 4$, that g factors into irreducible quadratic factors in $\Omega[X, Y]$. Let

(6.45)

$$g = Q_1 \cdot Q_2 ,$$

where Q_1, Q_2 are the irreducible factors of g in $\Omega[X, Y]$.

As $q > C_5$ and Q_1, Q_2 are irreducible, neither Q_1 or Q_2 can belong to $K[X, Y]$ if $f(X)$ is a permutation polynomial of K .

First assume that p , the characteristic of K , is not 5. This assumption will be in force until otherwise stated. Consider the following well-known theorem.

Theorem 6.6. Let K be a finite field of order q , and suppose Φ_d is the cyclotomic polynomial in $K[X]$. If $p \nmid d$ and e is the minimal exponent such that

$$q^e \equiv 1 \pmod{d},$$

then Φ_d factors into $\frac{\phi(d)}{e}$ irreducible factors of degree e in $K[X]$. (Note: Hence $\phi(d)$ denotes the Euler totient function. This function gives the degree of Φ_d , as is well-known.)

For our purposes, let $d = 5$. Then, as a result of this theorem, since $\phi(5) = 4$, e can only be 1, 2, or 4, by elementary number theory.

Suppose $e = 1$. As $e = 1$, $\Phi_5(X) = \frac{X^5 - 1}{X - 1}$ factors linearly in $K[X]$. It follows from this that the homogeneous part of degree 4 of $g(X, Y)$, $\frac{X^5 - Y^5}{X - Y}$, factors linearly in $K[X, Y]$. Hence, the

homogeneous parts of degree 2 of Q_1 and Q_2 belong to $K[X, Y]$.

Let E be the minimal Galois extension field of K that contains all the coefficients of Q_1 and Q_2 . Let σ be an arbitrary K -automorphism of $E|K$ and define $\hat{\sigma}$ as earlier. Hence, by unique factorization, as $g \in K[X, Y]$ and Q_1, Q_2 are irreducible in $\Omega[X, Y]$.

$$g = \hat{\sigma}(Q_1 \cdot Q_2) = Q_1 \cdot Q_2.$$

As the homogeneous parts of degree 2 of Q_1 and Q_2 belong to $K[X, Y]$ and are not identical, as $p \neq 5$, it follows that $\hat{\sigma}(Q_1) = Q_1$ and $\hat{\sigma}(Q_2) = Q_2$. Hence, as σ was chosen arbitrarily, Q_1 and Q_2 belong to $K[X, Y]$. But this is impossible, as $f(X)$ is a permutation polynomial of K and $q > C_5$. Therefore, when $e = 1$, there are no permutation polynomials of degree 5 such that $g(X, Y)$ factors into irreducible quadratic factors in $\Omega[X, Y]$.

Suppose again that $f(X)$ is a 5-th degree, primary permutation polynomial of K such that

$$g = Q_1 \cdot Q_2,$$

where Q_1 and Q_2 are irreducible in $\Omega[X, Y]$. We wish to determine what the homogeneous parts of degree 2 of Q_1 and Q_2 must look like when $e = 2$ and $e = 4$.

Suppose $e = 2$. By Theorem 6.6, $\frac{X^5 - 1}{X - 1}$ factors quadratically

in $K[X]$. It follows that $\frac{X^5 - 1}{X - 1}$ factors like

$$(6.46) \quad [(X - \zeta)(X - \zeta^4)] \cdot [(X - \zeta^2)(X - \zeta^3)] ,$$

where ζ is a primitive 5-th root of unity in Ω , in $K[X]$.

Otherwise, since $\zeta \cdot \zeta^2 = \zeta^3$ and $\zeta \cdot \zeta^3 = \zeta^4$, K would contain a primitive 5-th root of unity, which is impossible as $e = 2$.

Let E be the minimal Galois extension of K which contains all the 5-th roots of unity. It follows from (6.46) that the K -automorphisms of $E|K$, σ_1 and σ_2 , are determined by

$$\sigma_1(\zeta) = \zeta$$

and

$$\sigma_2(\zeta) = \zeta^4 .$$

Suppose the quadratic parts of Q_1 and Q_2 are

$$(6.47) \quad \begin{aligned} &[(X - \zeta Y)(X - \zeta^4 Y)] \\ &[(X - \zeta^2 Y)(X - \zeta^3 Y)] \end{aligned} .$$

As the polynomials (6.47) belong to $K[X, Y]$, which follows from (6.46), and are not identical, we have by unique factorization that $\hat{\sigma}_i(Q_1) = Q_1$ and $\hat{\sigma}_i(Q_2) = Q_2$, $i = 1, 2$. But this is impossible as $q > C_5$.

The remaining possibilities for the homogeneous parts of degree 2 of Q_1 and Q_2 are

$$(6.48) \quad \begin{aligned} &[(X - \zeta Y)(X - \zeta^3 Y)] \\ &[(X - \zeta^2 Y)(X - \zeta^4 Y)] \end{aligned}$$

and

$$(6.49) \quad \begin{aligned} &[(X - \zeta Y)(X - \zeta^2 Y)] \\ &[(X - \zeta^3 Y)(X - \zeta^4 Y)] \end{aligned} \quad .$$

Both (6.48) and (6.49) are invariant under σ_i , $i = 1$ and 2 . As (6.49) may be obtained from (6.48) by substituting ζ^2 , which is also a primitive 5-th root of unity, for ζ , we may assume that (6.48) holds.

Now suppose $e = 4$. By Theorem 6.6, $\frac{X^5 - 1}{X - 1}$ is irreducible in $K[X]$. Let E be the minimal Galois extension of K which contains all the 5-th roots of unity. As $\frac{X^5 - 1}{X - 1}$ is irreducible over K , it follows that $[E : K] = 4$ and the K -automorphisms of E , σ_i , $i = 1, 2, 3$, and 4 , are determined by

$$\sigma_1(\zeta) = \zeta,$$

$$\sigma_2(\zeta) = \zeta^2,$$

$$\sigma_3(\zeta) = \zeta^3,$$

and

$$\sigma_4(\zeta) = \zeta^4,$$

where ζ is a primitive 5-th root of unity in Ω .

The possibilities for the homogeneous parts of degree 2 of Q_1

and Q_2 are

$$(6.50) \quad \begin{aligned} & [(X - \zeta Y)(X - \zeta^2 Y)] \\ & [(X - \zeta^3 Y)(X - \zeta^4 Y)] \end{aligned} ,$$

$$(6.51) \quad \begin{aligned} & [(X - \zeta Y)(X - \zeta^3 Y)] \\ & [(X - \zeta^2 Y)(X - \zeta^4 Y)] \end{aligned} ,$$

and

$$(6.52) \quad \begin{aligned} & [(X - \zeta Y)(X - \zeta^4 Y)] \\ & [(X - \zeta^2 Y)(X - \zeta^3 Y)] \end{aligned} .$$

Applying $\hat{\sigma}_2$ to (6.50), we get

$$\begin{aligned} & [(X - \zeta^2 Y)(X - \zeta^4 Y)] \\ & [(X - \zeta Y)(X - \zeta^3 Y)] \end{aligned} .$$

By unique factorization, as Q_1 and Q_2 are irreducible in $\Omega[X, Y]$,

it follows that $\hat{\sigma}_2(Q_1 \cdot Q_2) = Q_1 \cdot Q_2$. Hence, the above implies that

we can eliminate (6.50). Applying $\hat{\sigma}_3$ to (6.51), we get

$$\begin{aligned} & [(X - \zeta^3 Y)(X - \zeta^4 Y)] \\ & [(X - \zeta Y)(X - \zeta^2 Y)] \end{aligned} .$$

Hence, we can eliminate (6.51) as before.

The remaining possibility is (6.52), which is invariant under $\hat{\sigma}_i$, $i = 1, 2, 3$, and 4. Hence, the homogeneous parts of degree 2 of Q_1 and Q_2 must be given by (6.52).

For convenience, define $\alpha = -\zeta - \zeta^4$ and $\bar{\alpha} = -\zeta^2 - \zeta^3$.

, (6.52) becomes

$$[X^2 + \alpha XY + Y^2]$$

$$[X^2 + \bar{\alpha}XY + Y^2]$$

$$][X^2 + \bar{\alpha}X + 1] = \frac{X}{Y}$$

$$\alpha + \bar{\alpha} = 1$$

$$\alpha\bar{\alpha} + 2 = 1$$

QUADRATIC FACTORIZATION OF $g(X, Y)$ WHEN $e = 2$.

Suppose $f(X)$ is a primary, 5-th degree permutation polynomial of K . In this chapter we wish to show that the case where $e = 2$ and $g(X, Y)$ has irreducible quadratic factors in $\Omega[X, Y]$ cannot occur. We will do this by demonstrating the quadratic factorization of $g(X, Y)$ in $\Omega[X, Y]$ and showing that at least one of the factors is reducible.

As $\frac{X^5 - 1}{X - 1}$ factors quadratically in $K[X]$ when $e = 2$,

let

$$(7.1) \quad \frac{X^5 - 1}{X - 1} = (X^2 + \alpha X + 1)(X^2 + \bar{\alpha} X + 1),$$

where $\alpha, \bar{\alpha} \in K$. Using (7.1), one can show that α and $\bar{\alpha}$ are zeros of the polynomial

$$(7.2) \quad X^2 - X - 1.$$

If ζ is a primitive 5-th root of unity in Ω , then, as $\frac{\zeta^5 - 1}{\zeta - 1} = 0$,

it follows that ζ is a zero of one of the quadratic factors of

$\frac{X^5 - 1}{X - 1}$ in $K[X]$. Without loss of generality, suppose

$$(7.3) \quad \zeta^2 + \alpha\zeta + 1 = 0.$$

As $e = 2$, it follows from (6.48) that the factorization of

$g(X, Y)$ in $\Omega[X, Y]$ must take the form

$$(7.4) \quad [X^2 + (-\zeta - \zeta^3)XY + \zeta^4 Y^2 + \beta_1 X + \beta_2 Y + \lambda]x$$

$$[X^2 + (-\zeta^2 - \zeta^4)XY + \zeta Y^2 + \mu_1 X + \mu_2 Y + \delta] ,$$

where $\beta_1, \beta_2, \lambda, \mu_1, \mu_2$, and δ are to be determined.

The homogeneous part of degree 3 of g is

$$(7.5) \quad aX^3 + aX^2Y + aXY^2 + aY^3 .$$

By the factorization of $g(X, Y)$ (7.4), the homogeneous part of degree 3 of g must also equal

$$(7.6) \quad \begin{aligned} & \beta_1 X^3 + \beta_2 X^2 Y + \beta_1 (-\zeta^2 - \zeta^4) X^2 Y + \\ & \beta_2 (-\zeta^2 - \zeta^4) XY^2 + \beta_1 \zeta XY^2 + \\ & \beta_2 \zeta Y^3 + \mu_1 X^3 + \mu_1 (-\zeta - \zeta^3) X^2 Y + \\ & \mu_1 \zeta^4 XY^2 + \mu_2 X^2 Y + \mu_2 (-\zeta - \zeta^3) XY^2 + \\ & \mu_2 \zeta^4 Y^3 . \end{aligned}$$

By comparing coefficients of (7.5) and (7.6) and utilizing (7.3), we obtain the following system of equations.

$$(7.7) \quad \begin{aligned} \beta_1 + \mu_1 &= a \\ \alpha \zeta^3 \beta_1 + \beta_2 + \alpha \zeta^2 \mu_1 + \mu_2 &= a \\ \zeta \beta_1 + \alpha \zeta^3 \beta_2 + \zeta^4 \mu_1 + \alpha \zeta^2 \mu_2 &= a \\ \zeta \beta_2 + \zeta^4 \mu_2 &= a . \end{aligned}$$

The determinant of the coefficients of this system is

$$(7.8) \quad \begin{vmatrix} 1 & 0 & 1 & 0 \\ \alpha\zeta^3 & 1 & \alpha\zeta^2 & 1 \\ \zeta & \alpha\zeta^3 & \zeta^4 & \alpha\zeta^2 \\ 0 & \zeta & 0 & \zeta^4 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 & 0 \\ \alpha\zeta^3 & 1 & \alpha\zeta^2(1-\zeta) & 1 \\ \zeta & \alpha\zeta^3 & \zeta^4-\zeta & \alpha\zeta^2 \\ 0 & \zeta & 0 & \zeta^4 \end{vmatrix} =$$

$$\begin{vmatrix} 1 & \alpha^2(1-\zeta) & 1-\zeta^3 \\ \alpha\zeta^3 & \zeta^4-\zeta & \alpha\zeta(\zeta-1) \\ \zeta & 0 & 0 \end{vmatrix} = \zeta \begin{vmatrix} \alpha\zeta^2(1-\zeta) & 1-\zeta^3 \\ -\zeta(1-\zeta^3) & -\alpha\zeta(1-\zeta) \end{vmatrix}$$

$$= -\zeta^2(1-\zeta)^2 \begin{vmatrix} \alpha\zeta^2 & 1+\zeta+\zeta^2 \\ 1+\zeta+\zeta^2 & \alpha \end{vmatrix} =$$

$$-\zeta^2(1-\zeta)^2 [(\alpha\zeta)^2 - (1+\zeta+\zeta^2)^2] =$$

$$-\zeta^2(1-\zeta)^2 [(\alpha\zeta + 1 + \zeta + \zeta^2)(\alpha\zeta - 1 - \zeta - \zeta^2)] .$$

As $\zeta^2 + \alpha\zeta + 1 = 0$, the determinant (7.8) becomes

$$(7.9) \quad \begin{aligned} & -\zeta^3(1-\zeta)^2(2\alpha\zeta - \zeta) = \\ & -\zeta^4(1-\zeta)^2(2\alpha - 1). \end{aligned}$$

Hence, as $5 \nmid q$ and, by (7.2), $2\alpha - 1 \neq 0$, it follows that the determinant of the coefficients of the system (7.7) is non-zero. Hence, by well-known theorems from linear algebra, there exists a unique solution to the system.

The calculations which are necessary to obtain this solution are quite laborious; thus, we shall only give the results and leave it to the reader to check their validity.

$$\begin{aligned}
 \beta_1 &= \frac{a\alpha}{(2+\alpha)(1-2\alpha)} [(\alpha-2) + (\alpha+1)\zeta] \\
 \beta_2 &= \frac{a\alpha}{(2+\alpha)(1-2\alpha)} [3\alpha + (\alpha+3)\zeta] \\
 \mu_1 &= \frac{-a\alpha}{(2+\alpha)(1-2\alpha)} [(3+\alpha) + (1+\alpha)\zeta] \\
 \mu_2 &= \frac{-a\alpha}{(2+\alpha)(1-2\alpha)} [(\alpha+1) + (\alpha+3)\zeta] .
 \end{aligned}
 \tag{7.10}$$

(Note again that by (7.2) $2+\alpha \neq 0$.)

We note that

$$\begin{aligned}
 \beta_1 \mu_1 &= \left(\frac{1}{5}\right)^2 a^2 (7+\alpha) \\
 \beta_2 \mu_2 &= \left(\frac{1}{5}\right)^2 a^2 (7+\alpha) \\
 \beta_1 \mu_2 &= \left(\frac{1}{5}\right)^2 a^2 [5(1+\alpha) + 4(2+\alpha)\zeta] \\
 \beta_2 \mu_1 &= -\left(\frac{1}{5}\right)^2 a^2 [(7\alpha-1) + 4(2+\alpha)\zeta] \\
 \beta_1 \mu_2 + \beta_2 \mu_1 &= 2 \left(\frac{1}{5}\right)^2 a^2 (3-\alpha)
 \end{aligned}
 \tag{7.11}$$

The homogeneous part of degree 2 of g is

$$bX^2 + bXY + bY^2 .
 \tag{7.12}$$

It follows from (7.4) that the homogeneous part of degree 2 of g must also equal

$$\begin{aligned}
 (7.13) \quad & \delta X^2 + \delta(-\zeta - \zeta^3)XY + \delta\zeta^4 Y^2 + \beta_1\mu_1 X^2 + \\
 & \beta_1\mu_2 XY + \beta_2\mu_1 XY + \beta_2\mu_2 Y^2 + \lambda X^2 + \\
 & \lambda(-\zeta^2 - \zeta^4)XY + \lambda\zeta Y^2.
 \end{aligned}$$

By comparing coefficients of (7.12) and (7.13), we get the following system of equations.

$$\begin{aligned}
 (7.14) \quad & \lambda + \mu_1\beta_1 + \delta = b \\
 & (-\zeta^2 - \zeta^4)\lambda + \mu_1\beta_2 + \mu_2\beta_1 + (-\zeta - \zeta^3)\delta = b \\
 & \zeta\lambda + \mu_2\beta_2 + \zeta^4\delta = b.
 \end{aligned}$$

Utilizing (7.11) and (7.3), we see that the augmented matrix of this system is

$$(7.15) \quad \begin{bmatrix} 1 & 1 & b - (\frac{a}{5})^2 (7 + \alpha) \\ \zeta & \zeta^4 & b - (\frac{a}{5})^2 (7 + \alpha) \\ \alpha\zeta^3 & \alpha\zeta^2 & b - 2(\frac{a}{5})^2 (3 - \alpha) \end{bmatrix}.$$

A triangular form of this matrix is

$$(7.16) \quad \begin{bmatrix} 1 & 1 & b - (\frac{a}{5})^2 (7 + \alpha) \\ 0 & \zeta(\zeta^3 - 1) & [b - (\frac{a}{5})^2 (7 + \alpha)](1 - \zeta) \\ 0 & 0 & b - \frac{2}{5} a^2 \end{bmatrix} ,$$

as can be seen by a straightforward though laborious calculation.

Hence, it follows, by well-known theorems from linear algebra, that we must have

$$b = \frac{2}{5} a^2$$

in order for the system (7.14) to be solvable. Setting $b = \frac{2}{5} a^2$

in (7.14) and (7.16), one derives the following solution to (7.14) from the matrix (7.16).

$$(7.17) \quad \begin{aligned} \lambda &= - (\frac{a}{5})^2 (2\alpha - 1)\alpha(1 + \zeta^4) \\ \delta &= - (\frac{a}{5})^2 (2\alpha - 1)\alpha(1 + \zeta) . \end{aligned}$$

We now note that

$$\begin{aligned} [X^2 + (-\zeta - \zeta^3)XY + \zeta^4 Y + \beta_1 X + \beta_2 Y + \lambda] = \\ [X - \zeta Y + \frac{a}{5} (1 - \zeta)] \times [X - \zeta^3 Y + \frac{a}{5} (1 - \zeta^3)] . \end{aligned}$$

Hence, if $f(X)$ is a permutation polynomial of K , $g(X, Y)$ cannot have irreducible quadratic factors in $\Omega[X, Y]$ if $e = 2$.

QUADRATIC FACTORIZATION OF $g(X, Y)$ WHEN $e = 4$.

In this chapter we wish to obtain results which will enable us to determine the primary, 5-th degree permutation polynomials of K when $e = 4$ and $g(X, Y)$ has irreducible quadratic factors in $\Omega[X, Y]$.

It follows from (6.53) that $g(X, Y)$ must have a quadratic factorization in $\Omega[X, Y]$ of the form

$$(8.1) \quad [X^2 + \alpha XY + Y^2 + \beta_1 X + \beta_2 Y + \lambda]x \\ [X^2 + \bar{\alpha}XY + Y^2 + \mu_1 X + \mu_2 Y + \delta] ,$$

where $\beta_1, \beta_2, \lambda, \mu_1, \mu_2$, and δ are to be determined.

The homogeneous part of degree 3 of $g(X, Y)$ is

$$(8.2) \quad aX^3 + aX^2Y + aXY^2 + aY^3 .$$

It follows from (8.1) that the homogeneous part of degree 3 of $g(X, Y)$ must also equal

$$(8.3) \quad \mu_1 X^3 + \mu_2 X^2 Y + \alpha \mu_1 X^2 Y + \alpha \mu_2 XY^2 + \\ \mu_1 XY^2 + \mu_2 Y^3 + \beta_1 X^3 + \bar{\alpha} \beta_1 X^2 Y + \\ \beta_1 XY^2 + \beta_2 X^2 Y + \bar{\alpha} \beta_2 XY^2 + \beta_2 Y^3 .$$

By equating coefficients of (8.2) and (8.3), we get the following system of equations

$$\beta_1 + \mu_1 = a$$

$$\bar{\alpha}\beta_1 + \beta_2 + \alpha\mu_1 + \mu_2 = a$$

(8.4)

$$\beta_1 + \bar{\alpha}\beta_2 + \mu_1 + \alpha\mu_2 = a$$

$$\beta_2 + \mu_2 = a .$$

The determinant of the coefficients of this system is

$$(8.5) \quad \begin{vmatrix} 1 & 0 & 1 & 0 \\ \bar{\alpha} & 1 & \alpha & 1 \\ 1 & \bar{\alpha} & 1 & \alpha \\ 0 & 1 & 0 & 1 \end{vmatrix} =$$

$$\begin{vmatrix} 1 & 0 & 0 & 0 \\ \bar{\alpha} & 1 & \alpha - \bar{\alpha} & 1 \\ 1 & \bar{\alpha} & 0 & \alpha \\ 0 & 1 & 0 & 1 \end{vmatrix} = \begin{vmatrix} 1 & \alpha - \bar{\alpha} & 1 \\ \bar{\alpha} & 0 & \alpha \\ 1 & 0 & 1 \end{vmatrix}$$

$$-(\alpha - \bar{\alpha}) \begin{vmatrix} \bar{\alpha} & \alpha \\ 1 & 1 \end{vmatrix} = -(\alpha - \bar{\alpha})(\bar{\alpha} - \alpha) =$$

$$(\bar{\alpha} - \alpha)^2 .$$

Utilizing (6.54), we see that

$$\begin{aligned}
 (8.6) \quad (\bar{\alpha} - \alpha)^2 &= (\alpha + \bar{\alpha})^2 - 4\alpha\bar{\alpha} \\
 &= 1^2 + 4 \\
 &= 5 .
 \end{aligned}$$

Hence, as $5 \nmid q$, the determinant of the coefficients of the system (8.4) is non-zero. It follows that the system is uniquely solvable. As the calculations necessary to obtain the solution to the system (8.4) are laborious, we shall simply state the solution.

$$\begin{aligned}
 (8.7) \quad \beta_1 &= \frac{a\alpha}{\alpha - \bar{\alpha}} \\
 \beta_2 &= \frac{a\alpha}{\alpha - \bar{\alpha}} \\
 \mu_1 &= \frac{-a\bar{\alpha}}{\alpha - \bar{\alpha}} \\
 \mu_2 &= \frac{-a\bar{\alpha}}{\alpha - \bar{\alpha}} .
 \end{aligned}$$

Because $\alpha\bar{\alpha} = -1$ and $(\bar{\alpha} - \alpha)^2 = 5$, $\beta_1 = \beta_2$, and $\mu_1 = \mu_2$, it follows that

$$(8.8) \quad \mu_1 \beta_1 = \mu_2 \beta_2 = \frac{a^2}{5}$$

and

$$(8.9) \quad \mu_1 \beta_2 + \mu_2 \beta_1 = \frac{2a^2}{5} .$$

The homogeneous part of degree 2 of g is

$$(8.10) \quad bX^2 + bXY + bY^2 .$$

It follows from the factorization of $g(X, Y)$ (8.1) that the

homogeneous part of degree 2 of g must also equal

$$(8.10) \quad \delta X^2 + \alpha \delta XY + \delta Y^2 + \beta_1 \mu_1 X^2 + \beta_1 \mu_2 XY + \\ \beta_2 \mu_1 XY + \beta_2 \mu_2 Y^2 + \lambda X^2 + \bar{\alpha} \lambda XY + \lambda Y^2 .$$

By equating coefficients of (8.10) and (8.11), we determine the following system of equations.

$$(8.12) \quad \begin{aligned} \lambda + \beta_1 \mu_1 + \delta &= b \\ \bar{\alpha} \lambda + \beta_1 \mu_2 + \beta_2 \mu_1 + \alpha \delta &= b \\ \lambda + \beta_2 \mu_2 + \delta &= b . \end{aligned}$$

Utilizing (9.8), we see that the first and last of these equations are the same. Thus, using (9.8) and (9.9), we can reduce this system to the following one.

$$(8.13) \quad \begin{aligned} \lambda + \delta &= b - \frac{a^2}{5} \\ \bar{\alpha} \lambda + \alpha \delta &= b - \frac{2a^2}{5} . \end{aligned}$$

The determinant of the coefficients of the system (8.13) is

$$(8.14) \quad \begin{vmatrix} 1 & 1 \\ \bar{\alpha} & \alpha \end{vmatrix} = \alpha - \bar{\alpha} .$$

It follows from (8.6) that, as $5 \nmid q$, $\alpha - \bar{\alpha} \neq 0$. Hence, the system (8.13) is uniquely solvable. Using determinants, we get that

$$(8.15) \quad \lambda = \frac{\alpha(5b - a^2) - (5b - 2a^2)}{5(\alpha - \bar{\alpha})} .$$

Consider the following irreducible factor of $g(X, Y)$.

$$(8.16) \quad [X^2 + \alpha XY + Y^2 + \beta_1 X + \beta_2 Y + \lambda] .$$

Assume (x, y) is a rational zero of (8.16). Utilizing (8.7) and (8.15), we have

$$(8.17) \quad x^2 + \alpha xy + y^2 + \frac{a\alpha}{\alpha - \bar{\alpha}} x + \frac{a\alpha}{\alpha - \bar{\alpha}} y + \frac{a(5b - a^2)}{5(\alpha - \bar{\alpha})} - \frac{(5b - 2a^2)}{5(\alpha - \bar{\alpha})} = 0 .$$

Multiplying both sides of the equation (8.17) by $5(\alpha - \bar{\alpha})$ and substituting $\bar{\alpha} = 1 - \alpha$ and $\alpha^2 = 1 + \alpha$, we get the following equation.

$$(8.18) \quad (10\alpha - 5)x^2 + (5\alpha + 10)xy + (10\alpha - 5)y^2 + 5a\alpha x + 5a\alpha y + 5ba - a^2\alpha - 5b + 2a^2 = 0 .$$

As $e = 4$, it follows that $\alpha \notin K$. Hence, as by assumption (x, y) is a rational zero of (8.16), we get from (8.18) that

$$(8.19) \quad 2x^2 + xy + 2y^2 + ax + ay + b - \frac{a^2}{5} = 0$$

and

$$(8.20) \quad x^2 - 2xy + y^2 + b - \frac{2}{5} a^2 = 0 .$$

From (8.20), we have

$$(8.21) \quad (x - y)^2 + b - \frac{2}{5} a^2 = 0 .$$

As $(x, y) \in K \times K$, $x - y = r \in K$. So,

$$(8.22) \quad r^2 = -b + \frac{2}{5}a^2.$$

By substituting $x = y + r$ in (8.19) and collecting terms, we obtain

$$(8.23) \quad 5y^2 + (2a + 5r)y + 2r^2 + ar + b - \frac{a^2}{5} = 0.$$

Suppose now that the characteristic of K is not 2.

Utilizing (8.22), we find that the discriminant of (8.23) is $5r^2$.

If $r = 0$, it follows from (8.21) that all the rational zeros of (8.16) are on the line $X = Y$.

Suppose $r \neq 0$. As y is rational, the discriminant $5r^2$ must be a square in K by the quadratic formula, which is valid in any field of characteristic $\neq 2$. Thus, as $r \neq 0$, 5 must be a square in K . As the discriminant of $X^2 - X - 1$ is 5, it follows that $\alpha \in K$, which is a contradiction. Thus we can conclude that (8.16) has no rational zeros (x, y) with $x \neq y$.

Suppose now that the characteristic of K is 2. Then $r^2 = b$, and (8.23) becomes $y^2 + ry + ar + b + a^2 = 0$, or

$$(8.24) \quad (y + a)^2 + r(y + a) + r^2 = 0.$$

Clearly, the equation (8.24) holds, as $y \in K$, if and only if there exists $z \in K$ such that

$$(8.25) \quad z^2 + rz + r^2 = 0.$$

We can assume $r \neq 0$, since $r = 0$ implies by (8.21) that all the rational zeros of (8.16) are on the line $X = Y$.

The polynomial $Z^2 + rZ + r^2$ factors in $\Omega[X]$ as follows.

$$(8.26) \quad Z^2 + rZ + r^2 = (Z - wr)(Z - w^2r),$$

where w is a primitive 3-rd root of unity in Ω . Hence,

$Z^2 + rZ + r^2$ has a zero in K if and only if $w \in K$.

The order of the multiplicative cyclic group of the field K is $q - 1$. Since the characteristic of K is 2, $q - 1 = 2^n - 1$ for some n . As the cube roots of unity form a subgroup of the multiplicative group and since $w \in K \setminus \{1\}$, $3 \mid 2^n - 1$. So, because $2^n \equiv 1 \pmod{3}$ and $2 \equiv -1 \pmod{3}$, $(-1)^n - 1 \equiv 0 \pmod{3}$. Hence, n must be even.

It follows, as n is even, that $q = 4^{n'}$, for some n' .

But

$$(4^{n'})^2 \equiv (-1)^{2n'} \equiv 1 \pmod{5}.$$

As $e = 4$, by assumption, this is impossible. Thus (8.16) has no rational zeros.

Therefore, we have demonstrated for all possible cases that (8.16) has no rational zeros which are not on the line $X = Y$. It follows as $[X^2 + \bar{\alpha}XY + Y^2 + \mu_1X + \mu_2Y + \delta]$ is the image of the factor (8.16) under the K -automorphism which carries α into $\bar{\alpha}$, this factor has no rational zeros off the line $X = Y$, either.

QUADRATIC FACTORIZATION OF $g(X, Y)$ WHEN THE
CHARACTERISTIC OF K IS 5

The purpose of this chapter is to determine the primary, 5-th degree permutation polynomials of the finite field K , where the characteristic of K , p , is 5 and $g(X, Y)$ has irreducible quadratic factors in $\Omega[X, Y]$. Throughout this section, we shall suppose that g has irreducible quadratic factors in $\Omega[X, Y]$.

The homogeneous part of degree 3 of $g(X, Y)$ is

$$(9.1) \quad aX^3 + aX^2Y + aXY^2 + aY^3.$$

As $p = 5$, the factorization of g in $\Omega[X, Y]$ must have the form

$$(9.2) \quad [(X - Y)^2 + \beta_1 X + \beta_2 Y + \lambda]x \\ [(X - Y)^2 + \mu_1 X + \mu_2 Y + \delta],$$

where β_1 , β_2 , λ , μ_1 , μ_2 , and δ are to be determined. It follows from this factorization that the homogeneous part of degree 3 of g must also equal

$$(9.3) \quad \mu_1 X^3 + \mu_2 X^2 Y - 2\mu_1 X^2 Y - 2\mu_2 XY^2 + \\ \mu_1 XY^2 + \mu_2 Y^3 + \beta_1 X^3 - 2\beta_1 X^2 Y + \\ \beta_1 XY^2 + \beta_2 X^2 Y - 2\beta_2 XY^2 + \beta_2 Y^3.$$

By comparing the coefficients of (9.1) and (9.3), we get the following system of equations.

$$\begin{aligned}
 \beta_1 + \mu_1 &= a \\
 -2\beta_1 + \beta_2 - 2\mu_1 + \mu_2 &= a \\
 \beta_1 - 2\beta_2 + \mu_1 - 2\mu_2 &= a \\
 \beta_2 + \mu_2 &= a.
 \end{aligned}
 \tag{9.4}$$

The augmented matrix of this system is

$$\begin{bmatrix}
 1 & 0 & 1 & 0 & a \\
 -2 & 1 & -2 & 1 & a \\
 1 & -2 & 1 & -2 & a \\
 0 & 1 & 0 & 1 & a
 \end{bmatrix}
 \tag{9.5}$$

The row-reduced matrix of (9.5) is

$$\begin{bmatrix}
 1 & 0 & 1 & 0 & a \\
 0 & 1 & 0 & 1 & 3a \\
 0 & 0 & 0 & 0 & 6a \\
 0 & 0 & 0 & 0 & -2a
 \end{bmatrix}
 \tag{9.6}$$

as one can easily verify. It follows from (9.6) that in order for the system (9.4) to be solvable, we must have

$$a = 0.
 \tag{9.7}$$

Setting $a = 0$ in the system (9.4) and the matrix (9.6), we see from (9.6) that the following are solutions to (9.4).

$$(9.8) \quad \begin{aligned} \mu_1 &= -\beta_1 \\ \mu_2 &= -\beta_2 . \end{aligned}$$

The homogeneous part of degree 2 of g is

$$(9.9) \quad bX^2 + bXY + bY^2 .$$

From the factorization of $g(X, Y)$ (9.2) we get that this part must also equal

$$(9.10) \quad \begin{aligned} &\delta X^2 - 2\delta XY + \delta Y^2 + \beta_1 \mu_1 X^2 + \\ &\beta_1 \mu_2 XY + \beta_2 \mu_1 XY + \beta_2 \mu_2 Y^2 + \\ &\lambda X^2 - 2\lambda XY + \lambda Y^2 . \end{aligned}$$

By comparing the coefficients of (9.9) and (9.10) and utilizing (9.8), we derive the following system of equations,

$$(9.11) \quad \begin{aligned} \delta + \lambda &= b + \beta_1^2 \\ 2\delta + 2\lambda &= -b - 2\beta_1 \beta_2 \\ \delta + \lambda &= b + \beta_2^2 . \end{aligned}$$

The augmented matrix of the above system is

$$(9.12) \quad \begin{bmatrix} 1 & 1 & b + \beta_1^2 \\ 2 & 2 & -b - 2\beta_1 \beta_2 \\ 1 & 1 & b + \beta_2^2 \end{bmatrix} ,$$

and the row-reduced form of (9.12) is

$$(9.13) \quad \begin{bmatrix} 1 & 1 & b + \beta_1^2 \\ 0 & 0 & -3b - 2\beta_1\beta_2 - 2\beta_1^2 \\ 0 & 0 & \beta_2^2 - \beta_1^2 \end{bmatrix} .$$

From (9.13), it follows that we must have

$$(9.14) \quad -3b - 2\beta_1\beta_2 - 2\beta_1^2 = 0$$

and

$$(9.15) \quad \beta_2^2 - \beta_1^2 = 0$$

in order for there to exist a solution to the system (9.11). As a result of (9.15), β_1 and β_2 must be related by

$$(9.16) \quad \beta_1 = \beta_2$$

or

$$(9.17) \quad \beta_1 = -\beta_2 .$$

In either case, it follows from (9.13) that

$$(9.17.5) \quad \delta + \lambda = b + \beta_1^2 .$$

First, suppose $\beta_2 = \beta_1$. Thus, by (9.14), $-3b - 2\beta_1^2 - 2\beta_1^2 =$

As $p = 5$, it follows from this equation that

$$(9.18) \quad \beta_1^2 = \frac{b}{2} ,$$

or

$$(9.19) \quad \beta_1 = \sqrt{\frac{b}{2}} \quad ,$$

where $\sqrt{\frac{b}{2}}$ is a square-root of $\frac{b}{2}$ in Ω .

By comparing the linear part of $g(X, Y)$ with that which we derive from (9.2), we find that

$$\beta_1 \delta + \mu_1 \lambda = c$$

and

$$\beta_2 \delta + \mu_2 \lambda = c.$$

As $\beta_1 = \beta_2$, by recalling (9.8), we get that these equations are identical and are equal to the equation

$$(9.20) \quad \beta_1 \delta - \beta_1 \lambda = c.$$

As $\beta_1^2 = \frac{b}{2}$, by (9.18), from (9.17.5) we get that

$$(9.21) \quad \delta = -b - \lambda.$$

Setting $\delta = -b - \lambda$ and $\beta_1 = \sqrt{\frac{b}{2}}$ in (9.20) and solving for λ , we get

$$(9.22) \quad \lambda = \frac{-\left[\frac{b^2}{2} + c\sqrt{\frac{b}{2}}\right]}{b} \quad ,$$

which only makes sense if $b \neq 0$. For the time being, suppose $b \neq 0$.

As the constant term in $g(X, Y)$ is d , it follows from the factorization of $g(X, Y)$ (9.2) that

$$(9.23) \quad \lambda \delta = d.$$

Substituting (9.21) in this, we get

$$(9.24) \quad \lambda(-b - \lambda) = d.$$

Utilizing (9.22), it follows from (9.24) that

$$(9.25) \quad d = \frac{3}{2} b^2 - \frac{c^2}{2b}.$$

Suppose now that $b = 0$. It immediately follows from (9.19) that $\beta_1 = 0$. Hence, by (9.20), $c = 0$.

As $a = b = c = 0$, $g(X, Y)$ looks like

$$(X - Y)^4 + d.$$

Clearly, in this case, $g(X, Y)$ factors linearly in $\Omega[X, Y]$.

But this is a contradiction.

Hence, if $g(X, Y)$ factors into irreducible quadratic factors in $\Omega[X, Y]$ and $\beta_1 = \beta_2$, then we have

$$(9.26) \quad \begin{aligned} a &= 0 \\ b &\neq 0 \\ d &= \frac{3}{2} b^2 - \frac{c^2}{2b}. \end{aligned}$$

Returning to (9.15), suppose now that $\beta_2 = -\beta_1$. Making this substitution in (9.14), we see that $b = 0$.

Comparing the linear coefficients of $g(X, Y)$ to those which we get from the factorization (9.2) and utilizing (9.8), we get the following equations.

$$(9.27) \quad \begin{aligned} \beta_1 \delta - \beta_1 \lambda &= c \\ \beta_2 \delta - \beta_2 \lambda &= c . \end{aligned}$$

Substituting $\beta_2 = -\beta_1$ in these equations, we get the system

$$\begin{aligned} \beta_1 \delta - \beta_1 \lambda &= c \\ -\beta_1 \delta + \beta_1 \lambda &= c \end{aligned}$$

Clearly, these equations are compatible only if $c = 0$. Hence, $a = b = c = 0$. As noted earlier, this contradicts our assumption that $g(X, Y)$ has irreducible quadratic factors in $\Omega[X, Y]$.

Theorem 9.1. Suppose K is a finite field of order q such that the characteristic of K is 5 and $q > C_5$. Then $f(X)$ is a primary permutation polynomial of degree 5 of K such that $g(X, Y)$ has irreducible quadratic factors in $\Omega[X, Y]$ if and only if

$$f(X) = X^5 + bX^3 + cX^2 + dX + e ,$$

where $\frac{b}{2}$ is not a square in K and $d = \frac{3}{2}b^2 - \frac{c^2}{2b}$. (Note:

$\frac{b}{2}$ not a square in K implies $b \neq 0$.)

Proof. Suppose f is a permutation polynomial of K such that $g(X, Y)$ has irreducible quadratic factors in $\Omega[X, Y]$. As g has an irreducible quadratic factorization in $\Omega[X, Y]$, we have by (9.26) that $a = 0$, $b \neq 0$, and $d = \frac{3}{2}b^2 - c^2/2b$. Suppose a

square root of $\frac{b}{2}$, $\sqrt{\frac{b}{2}}$, belongs to K . In this case, it

follows from (9.19), (9.8), (9.22), and (9.21), as $\beta_1 = \beta_2$, that

the irreducible quadratic factors of $g(X, Y)$ (9.2) belong to

$K[X, Y]$. As $q > C_5$ and $f(X)$ is a permutation polynomial of K ,

we have a contradiction. Hence, $\sqrt{\frac{b}{2}} \notin K$.

Suppose now that

$$f(X) = X^5 + bX^3 + cX^2 + dX + e,$$

where $\frac{b}{2}$ is not a square in K and $d = \frac{3}{2}b^2 - \frac{c^2}{2b}$. It follows

from earlier results in this chapter that any quadratic factor of

$g(X, Y)$ has the form

$$(9.28) \quad X^2 - 2XY + Y^2 + \sqrt{\frac{b}{2}}X + \sqrt{\frac{b}{2}}Y - \frac{b}{2} - \frac{c}{5}\sqrt{\frac{b}{2}},$$

where $\sqrt{\frac{b}{2}}$ is some square root of $\frac{b}{2}$. Suppose (x, y) is a

rational zero of (9.28) which is not on the line $X = Y$. As $\sqrt{\frac{b}{2}} \notin K$,

this can happen only if

$$(9.29) \quad x^2 - 2xy + y^2 - \frac{b}{2} = 0$$

and

$$(9.30) \quad x + y - \frac{c}{5} = 0.$$

From (9.30) we have $x = \frac{c}{b} - y$. Substituting this in (9.29), we get

$$\begin{aligned} 0 &= \left(\frac{c}{b} - y\right)^2 - 2\left(\frac{c}{b} - y\right)y + y^2 - \frac{b}{2} \\ &= y^2 - \frac{c}{b}y + \left(\frac{c^2}{2b^2} - \frac{b}{2}\right). \end{aligned}$$

The discriminant of

$$(9.31) \quad Y^2 - \frac{c}{b} Y + \frac{c^2}{2^2 b^2} - \frac{b}{2^3}$$

is

$$\frac{c^2}{b^2} - 4 \left[\frac{c^2}{2^2 b^2} - \frac{b}{2^3} \right] = \frac{b}{2} .$$

Since $\sqrt{\frac{b}{2}} \notin K$ and $p \neq 2$, by the quadratic formula, the polynomial (9.31) has no zeros in K . Hence, there does not exist a rational zero of (9.28) which is not on the line $X = Y$. This completes the proof.

PERMUTATION POLYNOMIALS OF DEGREE 5

The purpose of the following theorem is to organize and display the primary results obtained in Chapters VI through IX.

Theorem 10.1 (Dickson). Suppose K is a finite field, and
let q be the order of K and p the characteristic of K .
If $q > C_5$, then the primary, 5-th degree permutation polynomials of
 $K[X]$ are as follows:

$$(10.1) \quad f(X) = \left(X + \frac{a}{5}\right)^5 + d ,$$

where $p \neq 5$ and $5 \nmid q - 1$;

$$(10.2) \quad f(X) = X^5 + dX + e ,$$

where $p = 5$ and either $d = 0$ or there does not exist $k \in K$
such that $k^4 = -d$;

$$(10.3) \quad f(X) = X^5 + aX^4 + bX^3 + cX^2 + dX + e ,$$

where $q \equiv \pm 2 \pmod{5}$, $c = \frac{a}{5^2} [15b - 4a^2]$, and $d = b^2 - \frac{a^2b}{5} - \frac{a^4}{5^2}$;

$$(10.4) \quad f(X) = X^5 + bX^3 + cX^2 + dX + e ,$$

where $p = 5$, $\frac{b}{2}$ is not a square in K , and $d = \frac{3}{2}b^2 - \frac{c^2}{2b}$.

Further, any primary permutation polynomial of degree 5 over a finite field of order $q > C_5$ must fall into one of the above categories.

Proof. Partition the class of all primary 5-th degree polynomials in $K[X]$ into the following three mutually exclusive sets: first, the set S_1 in which $g(X, Y)$ is absolutely irreducible; second, the set S_2 in which $g(X, Y)$ has a linear factor in $\Omega[X, Y]$; and thirdly, the set S_3 in which $g(X, Y)$ has a quadratic factor, but no linear one, in $\Omega[X, Y]$.

As $q > C_5$, there are no permutation polynomials of K for which $g(X, Y)$ is absolutely irreducible. Hence S_1 contains no primary permutation polynomials.

Suppose $g(X, Y)$ has a linear factor in $\Omega[X, Y]$. By Theorems 6.2 and 6.4, it follows that the primary permutation polynomials of K in S_2 are exactly those polynomials in (10.1) and (10.2).

Suppose now that $g(X, Y)$ has a quadratic factor in $\Omega[X, Y]$, but not a linear one. If the characteristic of K is 5, it follows from Theorem 9.1 that the primary permutation polynomials in S_3 are exactly the polynomials (10.4).

Suppose $p \neq 5$. It follows from the results of Chapters VI, VII, and VIII that the only fields for which there exist permutation polynomials in S_3 are those for which $e = 4$. It follows, by direct substitution, that $e = 4$ is equivalent to $q \equiv \pm 2 \pmod{5}$,

as q must be congruent to ± 1 or ± 2 modulo 5.

By the results of Chapter VIII, multiplying out the factorization of $g(X, Y)$, we see that the polynomials in S_3 must have the form (10.3). Also, by definition, all $g(X, Y)$ determined by polynomials of the form (10.3) factor quadratically in the manner found in Chapter VIII. Hence, all such polynomials are permutation polynomials of K . This completes the proof.

esis
26
585
p. 2

BIBLIOGRAPHY

BIBLIOGRAPHY

- Chevalley, C., "Démonstration d'une Hypothèse de M. Artin," Hamburg universität Mathematischen Seminar Abhandlungen. Vol. II. Leipzig: Verlag B. G. Leubner, 1936. pp. 73-75.
- Dickson, L. E., Linear Groups. New York: Dover Publications, Inc., 1958.
- Jenner, W. E., Rudiments of Algebraic Geometry. New York: Oxford University Press, 1963.
- Lang, S. and A. Weil., "Number of Points of Varieties in Finite Fields," American Journal of Mathematics, Vol. 76(1963), 819-827.
- Van Der Waerden, B. L., Modern Algebra. Vol. I. New York: Frederick Ungar, 1953.
- _____, Modern Algebra. Vol. II. New York: Frederick Ungar, 1950.