Rev. Mat. Iberoamericana **19** (2003), 265–286

Galois theory of special trinomials

Shreeram S. Abhyankar

Abstract

This is the material which I presented at the 60th birthday conference of my good friend José Luis Vicente in Seville in September 2001. It is based on the nine lectures, now called sections, which were given by me at Purdue in Spring 1997. This should provide a good calculational background for the Galois theory of vectorial (= additive) polynomials and their iterates.

1. Introduction

Let $q > 1$ be a power of a prime p, let

$$k \subset K \subset \Omega$$

be fields of characteristic p where Ω is an algebraic closure of K, and let us use the abbreviation

$$\langle i \rangle = 1 + q + \cdots + q^i.$$

For any integer $m > 1$, in my papers *Nice Equations For Nice Groups* [2] and *Projective Polynomials* [3], we considered the Galois groups of the trinomials

$$F_{m,q} = F_{m,q}(Y) = Y^{\langle m-1 \rangle} + Y + X$$

and

$$\Phi_{m,q} = \Phi_{m,q}(Y) = F_{m,q}(Y^{q-1}) = Y^{q^m-1} + Y^{q-1} + X$$

and

$$\widehat{\Phi}_{m,q} = \widehat{\Phi}_{m,q}(Y) = Y\Phi_{m,q}(Y) = Y^{q^m} + Y^q + XY.$$

2000 Mathematics Subject Classification: 12F10, 14H30, 20D06, 20E22.
Keywords: Galois Groups, Iterates, Norms, Projective Polynomials, Splitting Fields, Vectorial Polynomials.

Here $\widehat{\Phi}_{m,q}$ is a monic separable vectorial q-polynomial of q-degree m over $k(X)$, $\Phi_{m,q}$ is the subvectorial associate of $\widehat{\Phi}_{m,q}$, and $F_{m,q}$ is the projective associate of $\widehat{\Phi}_{m,q}$. In the above two papers we showed that if $\mathrm{GF}(q) \subset k$ then $\mathrm{Gal}(F_{m,q}, k(X)) = \mathrm{PGL}(m,q)$ and $\mathrm{Gal}(\Phi_{m,q}, k(X)) = \mathrm{Gal}(\widehat{\Phi}_{m,q}, k(X)) = \mathrm{GL}(m,q)$. In Sections 2 to 4, without using these results about the Galois groups, we shall make a detailed study of the splitting fields of these trinomials in case of $m = 2$. In Section 9 we shall extend the considerations of Section 2 to slightly more general trinomials.

Quite generally, by a vectorial q-polynomial of q-degree m over K, where $m \geq 0$ is any integer, we mean a polynomial of the form

$$\widehat{\Phi} = \widehat{\Phi}(Y) = \sum_{i=0}^{m} a_i Y^{q^{m-i}} \quad \text{where} \quad a_i \in K \text{ with } a_0 \neq 0.$$

Its subvectorial associate is

$$\Phi = \Phi(Y) = \sum_{i=0}^{m} a_i Y^{q^{m-i}-1}$$

and its projective associate is

$$F = F(Y) = \sum_{i=0}^{m} a_i Y^{\langle m-1-i \rangle}$$

where we note that $\Phi(Y) = F(Y^{q-1})$ and $\widehat{\Phi}(Y) = Y\Phi(Y)$. These polynomials are monic if $a_0 = 1$ and separable if $a_m \neq 0$.

In Section 5 we shall study such a monic separable vectorial q-polynomial $\widehat{\Phi}$ of any q-degree $m \geq 0$, and in Section 6 we shall revert to the case of $m = 2$. Note that the set V of all roots of $\widehat{\Phi}$ in Ω is an m-dimensional $\mathrm{GF}(q)$-vector-subspace of Ω with $\mathrm{GF}(q) \subset K(V)$; moreover, if $\mathrm{GF}(q) \subset K$ then in a natural manner we have $\mathrm{Gal}(\Phi, K) = \mathrm{Gal}(\widehat{\Phi}, K) < \mathrm{GL}(V) \approx \mathrm{GL}(m,q)$ and $\mathrm{Gal}(F, K) < \mathrm{PGL}(V) \approx \mathrm{PGL}(m,q)$, where $<$ denotes subgroup and $\approx$ denotes isomorphism; see (4.1.1) of my paper on Semilinear Transformations [4].

For every integer $n \geq 0$ let $\widehat{\Phi}^{[[n]]}$ be the n-th iterate of $\widehat{\Phi}$, i.e., inductively we put $\widehat{\Phi}^{[[n]]} = \widehat{\Phi}(\widehat{\Phi}^{[[n-1]]}(Y))$ with $\widehat{\Phi}^{[[0]]}(Y) = Y$ and $\widehat{\Phi}^{[[1]]}(Y) = \widehat{\Phi}(Y)$. Let us say that we are in the generic case to mean that $\mathrm{GF}(q) \subset k \subset K = k(a_1, \ldots, a_m)$ with $m \geq 1 = a_0$ and the elements $a_1, \ldots, a_m$ are algebraically independent over k. In the paper just cited, it is shown that in the generic case we have $\mathrm{Gal}(\widehat{\Phi}, K) = \mathrm{GL}(m,q)$. In my paper [6] with Ganesh Sundaram on the Galois Theory of Moore-Carlitz-Drinfeld Modules, it is shown that

in the generic case we have $\mathrm{Gal}(\widehat{\Phi}^{[[n]]}, K) = \mathrm{GL}(m,q,n)$ with $\mathrm{GL}(m,q,n) = \mathrm{GL}(m, \mathrm{GF}(q,n))$ where $\mathrm{GF}(q,n)$ is the residue class ring of the univariate polynomial ring $\mathrm{GF}(q)[T]$ by the ideal generated by T^n. In Sections 7 and 8 we shall give a sketch of this material.

Now we may ask if the above iteration result is true for the specialization $\widehat{\Phi}_{m,q}$ of $\widehat{\Phi}$, i.e., is it true that if $\mathrm{GF}(q) \subset k$ then for all m,q,n we have $\mathrm{Gal}(\widehat{\Phi}_{m,q}^{[[n]]}, k(X)) = \mathrm{GL}(m,q,n)$. In the concluding Remark of Section 7 we shall indicate how the calculations of Section 3 show this not to be true in case of $(m,p,n) = (2,2,2)$.

2. Degree Two

To study the case of $m = 2$ let $F = F_{2,q}$ and $\Phi = \Phi_{2,q}$ and $\widehat{\Phi} = \widehat{\Phi}_{2,q}$. Assume that

$$\mathrm{GF}(q) \subset k \subset K = k(X).$$

Note that now

$$F = F(Y) = Y^{1+q} + Y + X \tag{2.1}$$

and

$$\Phi = \Phi(Y) = F(Y^{q-1}) = Y^{q^2-1} + Y^{q-1} + X \tag{2.2}$$

and

$$\widehat{\Phi} = \widehat{\Phi}(Y) = Y\Phi(Y) = Y^{q^2} + Y^q + XY. \tag{2.3}$$

We want to solve the equations $F = 0$ and $\widehat{\Phi} = 0$ and/or compute their Galois groups. Note that $\mathrm{Gal}(\widehat{\Phi}, K) = \mathrm{Gal}(\Phi, K) < \mathrm{GL}(2,q)$, where the Galois group of $\widehat{\Phi}$ acts on the two-dimensional vector space $V = \mathrm{GF}(q)^2 =$ the set of all roots of $\widehat{\Phi}$, whereas the Galois group of Φ acts on the nonzero vectors of V. Likewise $\mathrm{Gal}(F, K) < \mathrm{PGL}(2,q)$ acting on the projective line $\mathcal{P}(V) =$ the set of all roots of F. Let $F'(Y)$ be the twisted derivative of $F(Y)$ at a root y of $F(Y)$ in the algebraic closure Ω of K, i.e., let

$$y^{1+q} + y + X = 0 \tag{2.4}$$

and

$$F'(Y) = Y^{-1}[F(Y+y) - F(y)] = Y^q + yY^{q-1} + (y^q + 1). \tag{2.5}$$

Let $F^\dagger(Y)$ be obtained by dividing the roots of $F'(Y)$ by $y+1$, i.e., let

$$F^\dagger(Y) = (y+1)^{-q}F'((y+1)Y) = Y^q + \frac{y}{y+1}Y^{q-1} + 1 \tag{2.6}$$

where by (2.4) we know that $y \neq 0 \neq y+1$. Let $E(Y)$ be obtained by reciprocating $F^\dagger(Y)$, i.e.,

$$E(Y) = Y^q F^\dagger(Y^{-1}) = Y^q + \frac{y}{y+1}Y + 1. \tag{2.7}$$

Let $E'(Y)$ be the twisted derivative of $E(Y)$ at a root η of $E(Y)$ in Ω, i.e., let

$$\eta^q + \frac{y}{y+1}\eta + 1 = 0 \tag{2.8}$$

and

$$E'(Y) = Y^{-1}[E(Y+\eta) - E(\eta)] = Y^{q-1} + \frac{y}{y+1}. \tag{2.9}$$

Let ζ be a root of $E'(Y)$ in Ω and note that then

$$\zeta^{q-1} + \frac{y}{y+1} = 0. \tag{2.10}$$

By (2.8) and (2.10) we see that

$$0 = \zeta^{-q}(\eta^q - \zeta^{q-1}\eta + 1) = (\eta\zeta^{-1})^q - (\eta\zeta^{-1}) + \zeta^{-q}$$

and hence upon letting

$$\tau = \eta\zeta^{-1} \quad \text{and} \quad T = \tau + \zeta^{-1} \tag{2.11}$$

we get

$$T^q - \tau = 0. \tag{2.12}$$

Upon letting SF denote splitting field (in Ω), by (2.4), (2.6), (2.8), (2.10), (2.11) and (2.12) we see that $\mathrm{SF}(F,K) = k(X,y,\eta,\zeta,\tau,T) = k(y,\eta,\zeta,\tau,T) = k(\eta,\zeta,\tau,T) = k(\zeta,\tau,T) = k(\tau,T) = k(T)$ and hence

$$\mathrm{SF}(F,K) = k(T). \tag{2.13}$$

By (2.4), (2.6), (2.8), (2.10), (2.11) and (2.12) we also see that

$$\zeta = \frac{1}{T - T^q} \quad \text{and} \quad \eta = \frac{T^q}{T - T^q} \tag{2.14}$$

and

$$y = \frac{-\zeta^{q-1}}{1+\zeta^{q-1}} = \frac{-1-\eta^q}{1+\eta+\eta^q} = \frac{-1}{1+(T-T^q)^{q-1}}. \tag{2.15}$$

By (2.7) to (2.10) we see that

$$E(Y) = \prod_{i\in \mathrm{GF}(q)} (Y-\eta-i\zeta)$$

and hence upon letting

$$z_i = y + \frac{y+1}{\eta+i\zeta} = \frac{-(T+i)^{q(q-1)}}{1+(T-T^q)^{q-1}} \quad \text{for all} \quad i \in \mathrm{GF}(q) \tag{2.16}$$

and

$$z = z_0 = y + \frac{y+1}{\eta} = \frac{-T^{q(q-1)}}{1+(T-T^q)^{q-1}} \tag{2.17}$$

by (2.1) and (2.4) to (2.7) we see that

$$F(Y) = (Y-y)\prod_{i\in \mathrm{GF}(q)} (Y-z_i) = (Y-y)(Y-z)\prod_{0\neq i\in \mathrm{GF}(q)} (Y-z_i) \tag{2.18}$$

where, about the denominator in (2.15) to (2.17), we note that

$$1+(T-T^q)^{q-1} = \frac{(T-T^q)+(T-T^q)^q}{T-T^q} = \frac{1-T^{(q+1)(q-1)}}{1-T^{q-1}} \tag{2.19}$$

and hence

$$1+(T-T^q)^{q-1} = 1+T^{q-1}+T^{2(q-1)}+\cdots+T^{q(q-1)}. \tag{2.20}$$

Remark (2.21). Let $\overline{F} = \overline{F}(X,Y) = F = Y^{1+q}+Y+X$. Let $\overline{E} = \overline{E}(Y,Z) = (Y+1)Z^q+YZ+(Y+1)$ be obtained from E by changing (y,Y) to (Y,Z) and multiplying by $Y+1$. Let $\overline{E}' = \overline{E}'(Y,W) = (Y+1)W^{q-1}+Y$ be obtained from E' by changing (y,Y) to (Y,W) and multiplying by $Y+1$. Then, geometrically speaking, the above calculations can be paraphrased by saying that we have rationally parametrized first the plane curve $\overline{F}=0$ in the (X,Y)-plane, then the space curve $\overline{F}=\overline{E}=0$ given as an intersection of two surfaces in the three-space of (X,Y,Z), and finally the curve $\overline{F}=\overline{E}=\overline{E}'=0$ in the four-space of (X,Y,Z,W) given as an intersection of three solids. Details of this view point can be found in my 1990 AMS book [1] on Algebraic Geometry for Scientists and Engineers.

3. Characteristic Two

In the situation of Section 2, let us consider the case of $q = p = 2$. Since $1 = -1$, signs do not matter. So this is the easiest case to calculate. Also it is the case of coding theory and various other applications.

Upon letting $x = z_1$, by (2.15) to (2.18) we now have

$$F(Y) = (Y - x)(Y - y)(Y - z) \tag{3.1}$$

with

$$y = \frac{1}{1 + T + T^2} \quad \text{and} \quad z = \frac{T^2}{1 + T + T^2} \tag{3.2}$$

and

$$x = y + z = \frac{1 + T^2}{1 + T + T^2}. \tag{3.3}$$

For any ξ in $\{x, y, z\}$ let

$$F_\xi(Y) = \widehat{\Phi}(Y) + \xi = Y^4 + Y^2 + XY + \xi.$$

Then for any r in $\{x, y, z\}$, upon letting

$$G_r(Y) = \frac{Y^2}{1 + r^2} + \frac{rY}{1 + r^2}$$

we have

$$G_r(Y)^2 + G_r(Y) + \frac{\xi}{1 + r^4} = \frac{F_\xi(Y)}{1 + r^4}$$

(where by (2.1) and (3.1) we know that $r \neq 0 \neq 1 + r$ and $1 + r^2 \neq 0 \neq 1 + r^4$) and hence, for any $h(\xi) \in \Omega$ with $F_\xi(h(\xi)) = 0$, we have $[k(T, h(\xi)) : k(T, G_r(h(\xi)))] = 1$ or 2, and $[k(T, G_r(h(\xi))) : k(T)] = 1$ or 2. We want to determine these field degrees and to examine the linear disjointness of the various fields. To do this, we shall tacitly use the following:

Standard Results from Chapter IX on Cyclic Fields of Albert's 1937 book [7] entitled *Modern Higher Algebra*. For a moment let K be any field of characteristic $p > 0$ and let $K^{\bowtie}$ be the additive subgroup of K consisting of elements of the form $x^p - x$ with x varying over K. Then $Y^p - Y - \alpha$ with $\alpha \in K$ is irreducible over $K \Leftrightarrow \alpha \notin K^{\bowtie} \Leftrightarrow Y^p - Y - \alpha$ has no root in K, and if that is so then $\mathrm{Gal}(Y^p - Y - \alpha, K) = Z_p$ where by Z_p we denote cyclic group of order p. Conversely, if L is a p-cyclic extension of K (i.e., if L is a Galois extension of K with Galois group Z_p) then it is the splitting field (as well as a root field) of an irreducible polynomial of the form $Y^p - Y - \alpha$.

Finally, if β is a root of $Y^p - Y - \alpha$ with $\alpha \in K \setminus K^{\bowtie}$ and $\beta' \in K(\beta)$ then: the minimal monic polynomial of β' over K is of the form $Y^p - Y - \alpha'$ with $\alpha' \in K \Leftrightarrow \beta' = i\beta + \theta$ for some $0 \neq i \in \mathrm{GF}(p)$ and $\theta \in K$.

Reverting to the assumption of $K = k(T)$ and $q = p = 2$, by (3.2) we get

$$\frac{y}{1+y^4} = \frac{(1+T+T^2)^3}{T^4(1+T)^4} \tag{3.4}$$

and

$$\frac{y}{1+z^4} = \frac{(1+T+T^2)^3}{(1+T)^4} \tag{3.5}$$

and by adding (3.4) and (3.5) we get

$$\frac{y}{1+y^4} + \frac{y}{1+z^4} = \frac{(1+T+T^2)^3}{T^4} \tag{3.6}$$

and by expanding the cube we get

$$(1+T+T^2)^3 = 1+T+T^3+T^5+T^6. \tag{3.7}$$

Now

F_y is irreducible over K
$\iff$ the three fields $k(T, G_r(h(y)))_{r\in\{x,y,z\}}$ are exactly all the distinct proper subfields of $\mathrm{SF}(F_y, k(T))$ which properly contain $k(T)$
$\iff k(T, G_y(h(y))) \neq k(T) \neq k(T, G_z(h(y))) \neq k(T, G_y(h(y)))$

and in view of (3.4) and (3.7) we see that

$k(T, G_y(h(y))) = k(T)$
$\iff$ for some $P \in k[T]$ and monic $Q \in k[T]$ with $\mathrm{GCD}(P, Q) = 1$ we have $\dfrac{P^2}{Q^2} + \dfrac{P}{Q} = \dfrac{y}{1+y^4}$
$\iff$ for $Q = T^2 + T^4$ and some $P \in k[T]$ we have
$P^2 + PQ = 1 + T + T^3 + T^5 + T^6$
which is *impossible* because $P^2 + PQ$ has no term in T

and therefore $k(T, G_y(h(y))) \neq k(T)$, and likewise in view of (3.5) and (3.7)

we see that

$$
\begin{aligned}
&k(T, G_z(h(y))) = k(T)\\
&\iff \text{for some } P \in k[T] \text{ and monic } Q \in k[T] \text{ with } \mathrm{GCD}(P,Q) = 1\\
&\qquad \text{we have } \frac{P^2}{Q^2} + \frac{P}{Q} = \frac{y}{1+z^4}\\
&\iff \text{for } Q = 1+T^2 \text{ and some } P \in k[T] \text{ we have } P^2 + PQ = (1+T+T^2)^3\\
&\iff (\text{by } T \mapsto 1+T) \text{ for } Q = T^2 \text{ and some } P \in k[T] \text{ we have}\\
&\qquad P^2 + PQ = 1 + T + T^3 + T^5 + T^6\\
&\qquad \text{which is } \textit{impossible} \text{ because } P^2 + PQ \text{ has no term in } T
\end{aligned}
$$

and therefore $k(T, G_z(h(y))) \neq k(T)$, and similarly in view of (3.6) and (3.7) we see that

$$
\begin{aligned}
&k(T, G_y(h(y))) = k(T, G_z(h(y)))\\
&\iff \text{for some } P \in k[T] \text{ and monic } Q \in k[T] \text{ with } \mathrm{GCD}(P,Q) = 1\\
&\qquad \text{we have } \frac{P^2}{Q^2} + \frac{P}{Q} = \frac{y}{1+y^4} + \frac{y}{1+z^4}\\
&\iff \text{for } Q = T^2 \text{ and some } P \in k[T] \text{ we have}\\
&\qquad P^2 + PQ = 1 + T + T^3 + T^5 + T^6\\
&\qquad \text{which is } \textit{impossible} \text{ because } P^2 + PQ \text{ has no term in } T
\end{aligned}
$$

and therefore $k(T, G_z(h(y))) \neq k(T, G_z(h(y)))$, and hence F_y is irreducible over K. By symmetry it follows that F_z and F_x are also irreducible over K.

By (3.2) and (3.3) we get

$$\frac{y}{1+x^4} = \frac{(1+T+T^2)^3}{T^4} \tag{3.8}$$

and by adding (3.8) to T^2 times (3.8) we get

$$\frac{y}{1+x^4} + \frac{z}{1+x^4} = \frac{(1+T+T^2)^3(1+T^2)}{T^4} \tag{3.9}$$

and by (3.7) we get

$$(1+T+T^2)^3(1+T^2) = 1 + T + T^2 + T^6 + T^7 + T^8 \tag{3.10}$$

and by (3.9) and (3.10) we see that

$$\begin{aligned}
&k(T, G_x(h(y))) = k(T, G_x(h(z)))\\
&\iff \text{for some } P \in k[T] \text{ and monic } Q \in k[T] \text{ with } \mathrm{GCD}(P,Q) = 1\\
&\qquad \text{we have } \frac{P^2}{Q^2} + \frac{P}{Q} = \frac{y}{1+x^4} + \frac{z}{1+x^4}\\
&\iff \text{for } Q = T^2 \text{ and some } P \in k[T] \text{ we have}\\
&\qquad P^2 + PQ = 1 + T + T^2 + T^6 + T^7 + T^8\\
&\qquad \text{which is } \textit{impossible} \text{ because } P^2 + PQ \text{ has no term in } T
\end{aligned}$$

and therefore $k(T, G_x(h(y))) \neq k(T, G_x(h(z)))$.

By adding (3.8) to T^2 times (3.4) we get

$$\frac{y}{1+x^4} + \frac{z}{1+y^4} = \frac{(1+T+T^2)^5}{T^4(1+T)^4} \tag{3.11}$$

and by (3.7) we get

$$(1+T+T^2)^5 = 1 + T + T^2 + T^4 + T^5 + T^6 + T^8 + T^9 + T^{10} \tag{3.12}$$

and by (3.11) and (3.12) we see that

$$\begin{aligned}
&k(T, G_x(h(y))) = k(T, G_y(h(z)))\\
&\iff \text{for some } P \in k[T] \text{ and monic } Q \in k[T] \text{ with } \mathrm{GCD}(P,Q) = 1\\
&\qquad \text{we have } \frac{P^2}{Q^2} + \frac{P}{Q} = \frac{y}{1+x^4} + \frac{z}{1+y^4}\\
&\iff \text{for } Q = T^2 + T^4 \text{ and some } P \in k[T] \text{ we have}\\
&\qquad P^2 + PQ = 1 + T + T^2 + T^4 + T^5 + T^6 + T^8 + T^9 + T^{10}\\
&\qquad \text{which is } \textit{impossible} \text{ because } P^2 + PQ \text{ has no term in } T
\end{aligned}$$

and therefore $k(T, G_x(h(y))) \neq k(T, G_y(h(z)))$. Consequently by symmetry we get $k(T, G_z(h(y))) \neq k(T, G_x(h(z)))$.

By adding (3.8) to T^2 times (3.5) we get

$$\frac{y}{1+x^4} + \frac{z}{1+z^4} = \frac{(1+T+T^2)^3(1+T^4+T^6)}{T^4(1+T)^4} \tag{3.13}$$

and by (3.7) we get

$$(1+T+T^2)^3(1+T^4+T^6) = 1 + T + T^3 + T^4 + T^{10} + T^{11} + T^{12} \tag{3.14}$$

and by (3.13) and (3.14) we see that

$$\begin{aligned}
&k(T, G_x(h(y))) = k(T, G_z(h(z))) \\
&\iff \text{for some } P \in k[T] \text{ and monic } Q \in k[T] \text{ with } \mathrm{GCD}(P, Q) = 1 \\
&\qquad \text{we have } \frac{P^2}{Q^2} + \frac{P}{Q} = \frac{y}{1+y^4} + \frac{z}{1+y^4} \\
&\iff \text{for } Q = T^2 + T^4 \text{ and some } P \in k[T] \text{ we have} \\
&\qquad P^2 + PQ = 1 + T + T^3 + T^4 + T^{10} + T^{11} + T^{12} \\
&\qquad \text{which is } \textit{impossible} \text{ because } P^2 + PQ \text{ has no term in } T
\end{aligned}$$

and therefore $k(T, G_x(h(y))) \neq k(T, G_z(h(z)))$. Consequently by symmetry we get $k(T, G_y(h(y))) \neq k(T, G_x(h(z)))$.

By adding (3.4) to T^2 times (3.4) we get

$$\frac{y}{1+y^4} + \frac{z}{1+y^4} = \frac{(1+T+T^2)^3}{T^4(1+T)^2} \tag{3.15}$$

and by (3.7) and (3.15) we see that

$$\begin{aligned}
&k(T, G_y(h(y))) = k(T, G_y(h(z))) \\
&\iff \text{for some } P \in k[T] \text{ and monic } Q \in k[T] \text{ with } \mathrm{GCD}(P, Q) = 1 \\
&\qquad \text{we have } \frac{P^2}{Q^2} + \frac{P}{Q} = \frac{y}{1+y^4} + \frac{z}{1+y^4} \\
&\iff \text{for } Q = T^2 + T^3 \text{ and some } P \in k[T] \text{ we have} \\
&\qquad P^2 + PQ = 1 + T + T^3 + T^5 + T^6 \\
&\qquad \text{which is } \textit{impossible} \text{ because } P^2 + PQ \text{ has no term in } T
\end{aligned}$$

and therefore $k(T, G_y(h(y))) \neq k(T, G_y(h(z)))$. Consequently by symmetry we get $k(T, G_z(h(y))) \neq k(T, G_z(h(z)))$.

By adding (3.4) to T^2 times (3.5) we get

$$\frac{y}{1+y^4} + \frac{z}{1+z^4} = \frac{(1+T+T^2)^5}{T^4(1+T)^2} \tag{3.16}$$

and by (3.12) and (3.16) we see that

$$\begin{aligned}
&k(T, G_y(h(y))) = k(T, G_z(h(z))) \\
&\iff \text{for some } P \in k[T] \text{ and monic } Q \in k[T] \text{ with } \mathrm{GCD}(P,Q) = 1 \\
&\qquad \text{we have } \frac{P^2}{Q^2} + \frac{P}{Q} = \frac{y}{1+y^4} + \frac{z}{1+z^4} \\
&\iff \text{for } Q = T^2 + T^3 \text{ and some } P \in k[T] \text{ we have} \\
&\qquad P^2 + PQ = 1 + T + T^2 + T^4 + T^5 + T^6 + T^8 + T^9 + T^{10} \\
&\qquad \text{which is } \textit{impossible} \text{ because } P^2 + PQ \text{ has no term in } T
\end{aligned}$$

and therefore $k(T, G_y(h(y))) \neq k(T, G_z(h(z)))$.

By adding T^2 times (3.4) to (3.5) we get

$$\frac{z}{1+y^4} + \frac{y}{1+z^4} = \frac{(1+T+T^2)^3}{T^2(1+T)^2} \tag{3.17}$$

and by (3.7) and (3.17) we see that

$$\begin{aligned}
&k(T, G_y(h(z))) = k(T, G_z(h(y))) \\
&\iff \text{for some } P \in k[T] \text{ and monic } Q \in k[T] \text{ with } \mathrm{GCD}(P,Q) = 1 \\
&\qquad \text{we have } \frac{P^2}{Q^2} + \frac{P}{Q} = \frac{z}{1+y^4} + \frac{y}{1+z^4} \\
&\iff \text{for } Q = T + T^2 \text{ and } P = 1 + aT + bT^2 + T^3 \text{ with } a, b \text{ in } k \\
&\qquad \text{we have } P^2 + PQ = 1 + T + T^3 + T^5 + T^6 \\
&\iff \text{for some } a, b \text{ in } k \text{ we have} \\
&\qquad 1 + T + (a^2 + a + 1)T^2 + (a+b)T^3 + (b^2 + b + 1)T^4 + T^5 + T^6 \\
&\qquad\quad = 1 + T + T^3 + T^5 + T^6 \\
&\iff \text{for some } a, b \text{ in } k \text{ we have} \\
&\qquad a^2 + a + 1 = 0 = b^2 + b + 1 \text{ and } a + b = 1 \\
&\qquad \text{which is } \textit{possible} \text{ exactly when } \{a, b\} = \mathrm{GF}(4) \setminus \mathrm{GF}(2)
\end{aligned}$$

and therefore $k(T, G_y(h(z))) = k(T, G_z(h(y))) \Leftrightarrow \mathrm{GF}(4) \subset k$. Thus

$$\begin{cases} [\mathrm{SF}(F_x F_y, k(T)) : k(T)] = 8 \text{ or } 16 \\ \text{according as } \mathrm{GF}(4) \subset k \text{ or } \mathrm{GF}(4) \not\subset k. \end{cases} \tag{3.18}$$

4. General Characteristic

To continue with the discussion of Section 2, in the case of general (p, q), we take $S \in \Omega$ with

$$S^{q-1} + 1 + (T - T^q)^{q-1} = 0 \tag{4.1}$$

and we note that then by (2.13) to (2.18) we have

$$\mathrm{SF}(\widehat{\Phi}, K) = k(S, T) \tag{4.2}$$

and we let

$$v = \frac{1}{S} \quad \text{and} \quad w = \frac{T^q}{S} \tag{4.3}$$

and we note that then

$$v^{q-1} = y \quad \text{and} \quad w^{q-1} = z \tag{4.4}$$

and we let

$$w_i = w + iv = \frac{T^q + i}{S} \quad \text{for all} \quad i \in \mathrm{GF}(q) \tag{4.5}$$

and we note that then

$$w_i^{q-1} = z_i \quad \text{for all} \quad i \in \mathrm{GF}(q) \tag{4.6}$$

and

$$w = w_0. \tag{4.7}$$

Now

$$V = \{iv + jw : (i, j) \in \mathrm{GF}(q)^2\} \tag{4.8}$$

and we have

$$\widehat{\Phi}(Y) = \prod_{\xi \in V} (Y - \xi) = \prod_{i \in \mathrm{GF}(q)} \prod_{j \in \mathrm{GF}(q)} (Y - iv - jw). \tag{4.9}$$

Moreover, upon letting

$$W = \{v\} \cup \{w_i : i \in \mathrm{GF}(q)\} \quad \text{and} \quad V^* = V \setminus \{0\} \tag{4.10}$$

we see that

$$V^* = \{c\xi : \xi \in W \text{ and } c \in \mathrm{GF}(q)^*\} \tag{4.11}$$

and

$$\xi \mapsto \xi^{q-1} \text{ gives a bijection } W \to \mathcal{P}(V) = \{y\} \cup \{z_i : i \in \mathrm{GF}(q)^*\} \tag{4.12}$$

and we have

$$F(Y) = \prod_{x \in \mathcal{P}(V)} (Y - x) = \prod_{\xi \in W} (Y - \xi^{q-1}). \tag{4.13}$$

Before proceeding further with this, we shall discuss general vectorial polynomials.

5. General Vectorial Polynomials

Let $\widehat{\Phi}(Y)$ be any monic separable vectorial q-polynomial of q-degree $m \geq 0$ in Y over K, let V be the set of all roots of $\widehat{\Phi}$ in an algebraically closed overfield Ω of K, and note that then V is an m-dimensional GF(q)-vector-subspace of Ω. Let $I(V)$ be the image of the injective homomorphism of (the additive group of) V into $\mathrm{Aut}_\Omega(\Omega(Y))$ which sends every $t \in V$ to the Ω-automorphism of $\Omega(Y)$ given by $Y \mapsto Y - t$. Now

$$\widehat{\Phi}(Y) = \prod_{t \in V} (Y - t)$$

and hence

$$\widehat{\Phi}(Y) = N_{I(V)}(Y)$$

where, for any finite group I of automorphisms of any field M, the I-norm of any $\mu \in M$ may be defined by

$$N_I(\mu) = \prod_{\sigma \in I} \mu^\sigma.$$

Note that then M is a finite Galois extension of the fixed field $M^I = \{\nu \in M : \nu^\sigma = \nu \text{ for all } \sigma \in I\}$ and we have

$$N_I(\mu) = N_{M/M^I}(\mu)$$

where N_{M/M^I} is the norm in the usual field theory sense. Conversely, for any finite dimensional GF(q)-vector-subspace V of Ω, let us put

$$\Phi_V(Y) = N_{I(V)}(Y).$$

Then by the Converse of Linearity proved in (3.9) of my paper [5] on the Galois Theory of Semilinear Transformations, we see that $\Phi_V(Y)$ is a monic separable vectorial q-polynomial of q-degree $\dim V$ over Ω. Thus $\widehat{\Phi}(Y) \mapsto V$ gives a bijection of the set of all separable monic vectorial q-polynomials over Ω, and the inverse bijection is given by $V \mapsto \Phi_V$.

We now proceed to show that in this correspondence, composition of vectorial polynomials corresponds to the transitivity of norm which says that "the norm of a norm is a norm", i.e., for any finite algebraic field extensions $M^* \subset M' \subset M$ and any $\mu \in M$ we have

$$N_{M/M^*}(\mu) = N_{M'/M^*}(N_{M/M'}(\mu)).$$

To illustrate this principle, first note that, in conformity with Lüroth's Theorem, we have

$$\Omega(Y)^{I(V)} = \Omega(\Phi_V(Y)).$$

As a generalization of $I(V)$, for any $\mathrm{GF}(q)$-vector-subspace U of V, let $I(V,U)$ be the image of the homomorphism of V into $\mathrm{Aut}_\Omega(\Omega(Y))$ which sends every $t \in V$ to the Ω-automorphism of $\Omega(Y)$ given by $Y \mapsto Y - \Phi_U(t)$; note that the kernel of this homomorphism is U and so we could have denote the image by $I(V/U)$ rather than by $I(V,U)$ but then a comma is a frequent substitute for a solidus; at any rate, if $V = U \oplus U'$ then $I(V,U)$ is the image of the injective homomorphism of U' into $\mathrm{Aut}_\Omega(\Omega(Y))$ which sends every $t \in U'$ to the Ω-automorphism of $\Omega(Y)$ given by $Y \mapsto Y - \Phi_U(t)$. Let us put

$$\Phi_{V,U}(Y) = N_{I(V,U)}(Y).$$

Then by taking $M = \Omega(Y)$ and $M' = \Omega^{I(U)} = \Omega(\Phi_U(Y))$ and $M^* = \Omega^{I(V)} = \Omega(\Phi_V(Y))$ in the transitivity of norms, we have $\Phi_V(Y) = N_{M'/M^*}(\Phi_U(Y))$, and clearly the RHS equals $\prod_{t\in U'} \Phi_U(Y-t)$ which by the additivity of $\Phi_U(Y)$ equals $\prod_{t\in U'}[\Phi_U(Y) - \Phi_U(t)]$ which in turn obviously equals $\Phi_{V,U}(\Phi_U(Y))$, and thus we get

$$(^*) \qquad \Phi_V(Y) = \Phi_{V,U}(\Phi_U(Y)).$$

Concerning the definition of $I(V)$ and $\Phi_V(Y)$, for any subfield L of Ω, let $I^*(L,V)$ be the group of all $L(V)$-automorphisms of $L(V)(Y)$ of the form $Y \mapsto Y - t$ with $t \in V$, and note that then for any $\mu \in L(V)(Y)$ we have $N_{I(V)}(\mu) = N_{I^*(L,V)}(\mu)$ and hence

$$\Phi_V(Y) = N_{I^*(L,V)}(Y)$$

and so in particular

$$\Phi_V(Y) = N_{I^*(\mathrm{GF}(p),V)}(Y)$$

and also note that if $V \neq \{0\}$ then $\mathrm{GF}(q) \subset \mathrm{GF}(p)(V)$.

For any $\xi \in \Omega$, consider the affine q-polynomial

$$(5.1) \qquad F_\xi(Y) = \widehat{\Phi}(Y) - \xi$$

and let $h(\xi) \in \Omega$ be such that

$$F_\xi(h(\xi)) = 0. \tag{5.2}$$

Note that then

$$F_\xi(Y) = \prod_{t \in V}(Y - h(\xi) - t) \tag{5.3}$$

and hence

$$K(V) = \mathrm{SF}(\widehat{\Phi}, K) \subset \mathrm{SF}(F_\xi, K(\xi)) = K(V)(h(\xi)). \tag{5.4}$$

It follows that, for any subspace U of V, upon letting

$$F_{\xi,U}(Y) = \Phi_{V,U}(Y) - \xi$$

we get

$$F_{\xi,U}(\Phi_U(h(\xi))) = 0 \quad \text{with} \quad \Phi_U(h(\xi)) \in \mathrm{SF}(F_\xi, K(\xi))$$

and this gives a way of exhibiting several fields between $K(\xi)$ and $\mathrm{SF}(F_\xi, K(\xi))$.

In particular, if $\dim U = m - 1$ then for any $s \in V \setminus U$ we have

$$F_{\xi,U}(Y) = Y^q - \Phi_U(s)^{q-1}Y - \xi \quad \text{with} \quad \Phi_U(s) \neq 0$$

and upon letting

$$F_{\xi,U,s}(Y) = Y^q - Y - \frac{\xi}{\Phi_U(s)^q} \quad \text{and} \quad G_{U,s}(Y) = \frac{\Phi_U(Y)}{\Phi_U(s)}$$

we get

$$F_{\xi,U,s}(G_{U,s}(h(\xi))) = 0 \quad \text{with} \quad G_{U,s}(h(\xi)) \in \mathrm{SF}(F_\xi, K(\xi)).$$

On the other hand, if $\dim U = 1$ then for any $0 \neq r \in U$, upon letting

$$\Phi_r(Y) = \Phi_U(Y)$$

we have

$$\Phi_r(Y) = Y^q - r^{q-1}Y \tag{5.5}$$

and if actually $\dim U = m - 1 = 1$ then for any $s \in V \setminus U$, i.e., for any basis (r, s) of V, we have

$$\Phi_r(s) \neq 0 \tag{5.6}$$

and upon letting

$$F_{\xi,r,s}(Y) = F_{\xi,U,s}(Y) \quad \text{and} \quad G_{r,s}(Y) = G_{U,s}(Y)$$

we get

$$F_{\xi,r,s}(Y) = Y^q - Y - \frac{\xi}{\Phi_r(s)^q} \quad \text{and} \quad G_{r,s}(Y) = \frac{\Phi_r(Y)}{\Phi_r(s)} \tag{5.7}$$

and

$$F_{\xi,r,s}(G_{r,s}(h(\xi))) = 0 \quad \text{with} \quad G_{r,s}(h(\xi)) \in \mathrm{SF}(F_\xi, K(\xi)) \tag{5.8}$$

and by (5.3) we see that

$$F_\xi(Y) = \prod_{(i,j)\in \mathrm{GF}(q)^2} (Y - h(\xi) - ir - js). \tag{5.9}$$

6. Again Degree Two

Let us revert to the situation of Sections 2 and 4, i.e., assume $m = 2$ and let $\widehat{\Phi}(Y) = Y^{q^2} + Y^q + XY$. For any $\xi \in \Omega$, let $F_\xi(Y) \in K(\xi)[Y]$ and $h(\xi) \in \Omega$ be as in (5.1) and (5.2), and note that then we have (5.3) and (5.4). Let $B(V)$ be the set of all bases (r, s) of V over $\mathrm{GF}(q)$. For any $r \in \Omega$, let $\Phi_r(Y)$ be as in (5.5), and note that then for any $(r, s) \in B(V)$ we have (5.6). For any $(r, s) \in B(V)$, let $F_{\xi,r,s}(Y)$ and $G_{r,s}(Y)$ be as in (5.7), and note that then we have (5.8). Finally, for any $(r, s) \in B(V)$ we have (5.9).

7. Iterated Vectorial Polynomials

Again let $\widehat{\Phi}(Y)$ be any monic separable vectorial q-polynomial of q-degree $m \geq 0$ over K, let V be the $\mathrm{GF}(q)$-vector space of all roots of $\widehat{\Phi}(Y)$ in Ω, and for any integer $n \geq 0$, let $V^{[n]}$ be the set of all roots of its n-th iterate $\widehat{\Phi}^{[[n]]}$ in Ω. Note that then $\widehat{\Phi}^{[[n]]}$ is a monic separable vectorial q-polynomial of q-degree mn in Y over K and hence $V^{[n]}$ is an (mn)-dimensional $\mathrm{GF}(q)$-vector-subspace of Ω, with $V^{[1]} = V$. We get a $\mathrm{GF}(q)$-linear epimorphism $\widetilde{\Phi} : \Omega \to \Omega$ given by $z \mapsto \widehat{\Phi}(z)$. For its n-th power $\widetilde{\Phi}^n : \Omega \to \Omega$ we have $\widetilde{\Phi}^n(z) = \widehat{\Phi}^{[[n]]}(z)$ for all $z \in \Omega$. For every $n' < n$ we clearly have $V^{[n']} \subset V^{[n]}$ and $\widetilde{\phi}^{n'}(V^{[n]}) = V^{[n-n']}$, and moreover $\widetilde{\Phi}^{n'}|V^{[n]}$ gives a $\mathrm{GF}(q)$-linear epimorphism $V^{[n]} \to V^{[n-n']}$ with kernel $V^{[n']}$. Let $\mathrm{GF}(q, n) = \mathrm{GF}(q)[T]/T^n$ where T is an indeterminate, and let $\overline{T}$ be the image of T under the canonical epimorphism of $\mathrm{GF}(q)[T]$ onto $\mathrm{GF}(q, n)$. For every $\overline{r} = \sum_{i=0}^{n-1} r_i \overline{T}^i \in \mathrm{GF}(q, n)$ with $r_i \in \mathrm{GF}(q)$ and every $z \in \Omega$ we define $\overline{r}z \in \Omega$ by putting $\overline{r}z = \sum_{i=0}^{n-1} r_i \widetilde{\Phi}^i(z)$, and we note that this makes $V^{[n]}$ a $\mathrm{GF}(q, n)$-module, and then, for every $\overline{r} \in \mathrm{GF}(q, n)$ and $z \in V^{[n]}$ we have

$\sigma(\overline{r}z) = \overline{r}\sigma(z)$ for every K-automorphism σ of Ω. It follows that, in a natural manner, $\mathrm{Gal}(\widehat{\Phi}^{[[n]]}, K)$ is a subgroup of the group of all $\mathrm{GF}(q,n)$-linear automorphisms of the module $V^{[n]}$. By taking any elements $u_1, \dots, u_m$ of $V^{[n]}$ such that $\widetilde{\Phi}^{n-1}(u_1), \dots, \widetilde{\Phi}^{n-1}(u_m)$ is a free $\mathrm{GF}(q)$-basis of V, we see that $u_1, \dots, u_m$ is a free $\mathrm{GF}(q,n)$-basis of $V^{[n]}$, and hence $V^{[n]}$ is a free $\mathrm{GF}(q,n)$-module of rank m. So we may identify the group of all $\mathrm{GF}(q,n)$-linear automorphisms of the module $V^{[n]}$ with $\mathrm{GL}(m,q,n) = \mathrm{GL}(m, \mathrm{GF}(q,n))$.

To generalize this, for every $r = r(T) = \sum r_i T^i \in \mathrm{GF}(q)[T]$ with $r_i \in \mathrm{GF}(q)$ (and $r_i = 0$ for all except finitely many i) we put $\widehat{\Phi}^{[r]} = \widehat{\Phi}^{[r]}(Y) = \sum r_i \widehat{\Phi}^{[i]}(Y)$ and for every $z \in \Omega$ we define $rz \in \Omega$ by putting $rz = \widehat{\Phi}_r(z)$ and we note that this makes Ω a $\mathrm{GF}(q)[T]$-module. Actually, for all r, s in $\mathrm{GF}(q)[T]$ and a, b in $\mathrm{GF}(q)$, we have $\widehat{\Phi}^{[ar+bs]}(Y) = a\widehat{\Phi}^{[r]}(Y) + b\widehat{\Phi}^{[s]}(Y)$ and $\widehat{\Phi}^{[rs]} = \widehat{\Phi}^{[r]}(\widehat{\Phi}^{[s]}(Y)) = \widehat{\Phi}^{[s]}(\widehat{\Phi}^{r]}(Y))$, and hence this puts a $\mathrm{GF}(q)[T]$-module structure on a certain commutative subring of the noncommutative ring (under composition) of all vectoral q-polynomials in Y with coefficients in Ω (namely, the subring "generated" by $\widehat{\Phi}$). At any rate, for every $r \in \mathrm{GF}(q)[T]$, this makes the set $V(\widehat{\Phi}^{[r]})$ of all roots of $\widehat{\Phi}^{[r]}$ in Ω a $(\mathrm{GF}(q)[T]/r)$-module since these roots are "killed" by r. In case $r \neq 0$, this module structure commutes with the action of $\mathrm{Gal}(\widehat{\Phi}^{[r]}, K)$ making this Galois group a subgroup of the GL of the module $V(\widehat{\Phi}^{[r]})$; note that the coefficient of Y in $\widehat{\Phi}^{[r]}(Y)$ is r and hence $\widehat{\Phi}^{[r]}(Y)$ is separable. This is what is known as the Drinfeld module. The above case corresponds to $r(T) = T^n$.

Going back to the case of $\widehat{\Phi}^{[[n]]}$ with $n > 0$ we may think of $\mathrm{GL}(m,q,n)$ as consisting of $m \times m$ matrices $A(\overline{T}) = (A_{ij}(\overline{T}))$ whose entries $A_{ij}(\overline{T})$ are polynomials of degree $\leq n-1$ over $\mathrm{GF}(q)$ and whose determinant, as a polynomial in $\overline{T}$, has a nonzero constant term. Now $A(\overline{T}) \mapsto A(0)$ gives an epimorphism $\theta : \mathrm{GL}(m,q,n) \to \mathrm{GL}(m,q)$. Clearly $|\ker(\theta)| = q^{(n-1)m^2}$ and hence

$$|\mathrm{GL}(m,q,n)| = q^{(n-1)m^2} |\mathrm{GL}(m,q)|.$$

Assuming $n > 1$, let $K' = \mathrm{SF}(\widehat{\Phi}, K) = K(V)$ and $K'' = \mathrm{SF}(\widehat{\Phi}^{[[n]]}, K)K(V^{[n]})$, and identify $\mathrm{Gal}(\Phi, K)$ and $\mathrm{Gal}(\Phi^{[[n]]}, K)$ with corresponding subgroups of $\mathrm{GL}(m,q)$ and $\mathrm{GL}(m,q,n)$ respectively. For any $\xi \in \Omega$ upon letting

$$\Psi_\xi(Y) = \Phi^{[[n-1]]}(Y) - \xi \quad \text{and} \quad R(\xi) = \{\eta \in \Omega : \Psi_\xi(\eta) = 0\}$$

we have

$$\Psi_\xi = \prod_{\eta \in R(\xi)} (Y - \eta) \quad \text{and} \quad |R(\xi)| = q^{(n-1)m}$$

and, fixing any $h(\xi) \in R(\xi)$, by the vectoriality of $\Psi^{[[n-1]]}$ we see that

$$\mathrm{SF}(\Psi_\xi, K') = K'(h(\xi)).$$

Now

$$\Phi(Y) = \prod_{t\in V}(Y-t) \quad \text{and} \quad \Phi^{[[n]]}(Y) = \Phi(\Phi^{[[n-1]]}(Y))$$

and hence

$$\Phi^{[[n]]}(Y) = \prod_{t\in V}\prod_{t\in V}\Psi_t(Y)$$

and therefore, for any basis $t_1,\dots,t_m$ of V, by the vectoriality of $\Phi^{[[n-1]]}$ we see that

$$K'' = \mathrm{SF}(\Phi^{[[n]]}, K') = \mathrm{SF}(\prod_{1\le i\le m}\Psi_{t_i}, K') = K'(h(t_1),\dots,h(t_m)). \tag{7.1}$$

It follows that

(7.2)

$$\mathrm{Gal}(\Phi^{[[n]]}, K) = \mathrm{GL}(m,q,n) \Longleftrightarrow \begin{cases} \mathrm{Gal}(\Phi, K) = \mathrm{GL}(m,q) \text{ and} \\ [K'(h(t_1),\dots,h(t_m)) : K'] = q^{n-1}m^2. \end{cases}$$

Remark on the Trinomial Case. In view of (7.1) and (7.2), by (3.18) we conclude that

$$[\mathrm{GL}(2,2,2) : \mathrm{Gal}(\widehat{\Phi}_{2,2}^{[[2]]}, k(X))] = 2 \Longleftrightarrow \mathrm{GF}(4) \subset k \tag{7.3}$$

and

$$\mathrm{Gal}(\widehat{\Phi}_{2,2}^{[[2]]}, k(X)) = \mathrm{GL}(2,2,2) \Longleftrightarrow \mathrm{GF}(4) \not\subset k. \tag{7.4}$$

8. Regular Local Domains

Let S be an m-dimensional regular local domain where $m > 0$ is any integer, let $(Z_1,\dots,Z_m)$ be a basis of the maximal ideal $M(S)$ of S, let L be the quotient field of S, and let $\overline{\Omega}$ be an algebraically closed overfield of L; (the characteristic of S may or may not be zero, and could be different from the characteristic of its residue field). For example S could be the ring of (formal or convergent) power series in $Z_1,\dots,Z_m$ with coefficients in a field k, where in the convergent case we require k to be equipped with a metric (such as the real or the complex or the p-adic field); or S could the polynomial ring $k[Z_1,\dots,Z_m]$ localized at the origin $Z_1 = \cdots = Z_m = 0$, i.e., localized at the prime ideal generated by $Z_1,\dots,Z_m$; or S could be any ring "between" the said localized ring and the power series ring. For $m = 2$ think of the origin in the plane, and for $m = 3$ think of the corner of the room. The passage from the polynomial case to the regular local case, i.e., effectively to the

power series case, gives us greater versatility of parametrization. This was exhibited in Proposition (5.3) of my *Projective Polynomials* paper [3]. In the proof of the said Proposition, the following easy-to-prove fact was called:

GEC (= Generalized Eisenstein Criterion) Let R be a local domain dominated by S. Let $F(Y) = Y^d + \sum_{l=1}^{d} A_l Y^{d-l}$ with $A_l \in M(R)$ for $1 \leq l < d$ and $A_d \in M(R)^2$ where $d > 0$ is any integer. Then $F(Y) - Z_1$ is irreducible in $L[Y]$ and, upon taking $Z^* \in \overline{\Omega}$ with $F(Z^*) = Z_1$ and upon letting $S^* =$ the integral closure of S in $L(Z^*)$, we have that S^* is an m-dimensional regular local domain dominating S such that S^* is residually rational over S, the quotient field of S^* is $L(Z^*)$, and $M(S^*) = (Z^*, Z_2, \ldots, Z_m)S^*$.

An obvious double induction applied to GEC immediately yields the following:

Corollary. Let R be a local domain dominated by S. Let $n \geq 0$ be an integer and for $1 \leq i \leq m$ and $1 \leq j \leq n$ let $F_{i,j}(Y) = Y^{d(i,j)} + \sum_{l=1}^{d(i,j)} A_{i,j,l} Y^{d(i,j)-l}$ with $A_{i,j,l} \in M(R)$ for $1 \leq l < d(i,j)$ and $A_{i,j,d(i,j)} \in M(R)^2$ where $d(i,j) > 0$ is an integer. For $1 \leq i \leq m$ let $Z_{i,0} = Z_i$, and for $1 \leq i \leq m$ and $1 \leq j \leq n$ let $Z_{i,j} \in \overline{\Omega}$ with $F_{i,j}(Z_{i,j}) = Z_{i,j-1}$. Let $S_0 = S$ and $L_0 = L$, and for $1 \leq j \leq n$ let $L_j = L(Z_{1,j}, \ldots, Z_{m,j})$ and $S_j =$ the integral closure of R in L_j. Then for $1 \leq j \leq n$, the polynomials $F_{1,j}(Y) - Z_{1,j-1}, \ldots, F_{m,j}(Y) - Z_{m,j-1}$ are irreducible in $L_{j-1}[Y]$, the field L_{j-1} is a subfield of the field L_j with $[L_j : L_{j-1}] = d(1,j) \ldots d(m,j)$, the ring S_j is an m-dimensional regular local domain dominating S_{j-1} such that S_j is residually rational over S_{j-1}, the quotient field of S_j is L_j, and $M(S_j) = (Z_{1,j}, \ldots, Z_{m,j})S_j$.

Remark on the Generic Case. To apply this Corollary, recall that $q > 1$ is any power of any prime p. Consider the generic vectorial q-polynomial $\widehat{\Phi}(Y) = Y^{q^m} + X_1 Y^{q^{m-1}} + \cdots + X_m Y$ where $X_1, \ldots, X_m, Y$ are indeterminates over a field k with $\mathrm{GF}(q) \subset k$, let R be the localization of $k[X_1, \ldots, X_m]$ at the prime ideal generated by $(X_1, \ldots, X_m)$, and let $K = k(X_1, \ldots, X_m)$. Then $\mathrm{SF}(\widehat{\Phi}, k(X_1, \ldots, X_m)) = k(Z_1, \ldots, Z_m) = L =$ the quotient field of the m-dimensional regular local domain S obtained by localizing $k[Z_1, \ldots, Z_m]$ at the ideal generated by $(Z_1, \ldots, Z_m)$, and we have

$$\widehat{\Phi}(Y) = \prod_{(a_1,\ldots,a_m) \in \mathrm{GF}(q)^m} (Y - a_1 Z_1 - \cdots - a_m Z_m)\,.$$

Clearly S dominates R and the elements $X_1, \ldots, X_m$ belong to $M(R)$, and therefore by taking $F_{ij} = \widehat{\Phi}$ for all i, j in the Corollary we see that for the n-th iterate $\widehat{\Phi}^{[[n]]}$ of $\widehat{\Phi}$ we have $\mathrm{Gal}(\widehat{\Phi}^{(n)}, K) = \mathrm{GL}(m, q, n)$. For further details about the generic case see Section 3 of my paper [5] on the Galois Theory of Semilinear Transformations.

9. General Degree Two

To generalize the parametrization given in Section 2, let $F, \Phi, \widehat{\Phi}$ be obtained by putting $(2, A, B)$ for $(m, 1, X)$ in $F_{m,q}, \Phi_{m,q}, \widehat{\Phi}_{m,q}$ respectively, where $A \neq 0 \neq B$ are elements in an overfield K of k with

$$\mathrm{GF}(q) \subset k \subset K = k(A, B).$$

Note that now

$$F = F(Y) = Y^{1+q} + AY + B\,, \tag{9.1}$$

$$\Phi = \Phi(Y) = F(Y^{q-1}) = Y^{q^2-1} + AY^{q-1} + B\,, \tag{9.2}$$

$$\widehat{\Phi} = \widehat{\Phi}(Y) = Y\Phi(Y) = Y^{q^2} + AY^q + BY. \tag{9.3}$$

Let $F'(Y)$ be the twisted derivative of $F(Y)$ at a root y of $F(Y)$ in the algebraic closure Ω of K, i.e., let

$$y^{1+q} + Ay + B = 0 \tag{9.4}$$

and

$$F'(Y) = Y^{-1}[F(Y+y) - F(y)] = Y^q + yY^{q-1} + y^{q-1}Y + (y^q + A). \tag{9.5}$$

Let $E(Y)$ be obtained by reciprocating $F'(Y)$, i.e.,

$$E(Y) = (y^q + A)^{-1}Y^q F'(Y^{-1}) = Y^q + (y^q + A)^{-1}Y + (y^q + A)^{-1}.$$

To simplify notation, let

$$\xi = -(y^q + A)^{-1} \tag{9.6}$$

and note that then

$$E(Y) = -\xi Y^q F'(Y^{-1}) = Y^q - \xi Y - \xi. \tag{9.7}$$

Let $E'(Y)$ be the twisted derivative of $E(Y)$ at a root η of $E(Y)$ in Ω, i.e., let

$$\eta^q - \xi\eta - \xi = 0 \tag{9.8}$$

$$E'(Y) = Y^{-1}[E(Y+\eta) - E(\eta)] = Y^{q-1} - \xi. \tag{9.9}$$

Let ζ be a root of $E'(Y)$ in Ω and note that then

$$\zeta^{q-1} - \xi = 0. \tag{9.10}$$

By (9.8) and (9.10) we see that

$$0 = \zeta^{-q}(\eta^q - \zeta^{q-1}\eta - \zeta^{q-1}) = (\eta\zeta^{-1})^q - (\eta\zeta^{-1}) - \zeta^{-1}$$

and hence upon letting

$$\tau = \eta\,\zeta^{-1} \tag{9.11}$$

we get

$$\tau^q - \tau - \zeta^{-1} = 0. \tag{9.12}$$

By (9.4), (9.6), (9.8), (9.10), (9.11) and (9.12) we get

$$\begin{aligned}\mathrm{SF}(F,K) &= k(A,B,y,\xi,\eta,\zeta,\tau) = k(A,y,\xi,\eta,\zeta,\tau) = k(A,\xi,\eta,\zeta,\tau,y)\\ &= k(A,\eta,\zeta,\tau,y) = k(A,\zeta,\tau,y) = k(A,\tau,y)\end{aligned}$$

and hence

$$\mathrm{SF}(F,K) = k(A,\tau,y). \tag{9.13}$$

By (9.4), (9.6), (9.8), (9.10), (9.11) and (9.12) we also see that

$$\zeta = \frac{1}{\tau^q - \tau}\,, \tag{9.14}$$

$$\eta = \tau\zeta = \frac{1}{\tau^{q-1} - 1}\,, \tag{9.15}$$

$$\xi = \zeta^{q-1} = \frac{\eta^q}{\eta + 1} = \frac{1}{(\tau^q - \tau)^{q-1}} \tag{9.16}$$

and

$$y^q = -A - (\tau^q - \tau)^{q-1}. \tag{9.17}$$

By (9.7) to (9.10) we see that

$$E(Y) = \prod_{j \in \mathrm{GF}(q)} (Y - \eta - j\zeta)$$

and hence upon letting

$$z = y + \eta^{-1} \tag{9.18}$$

by (9.1) and (9.4) to (9.7) we see that

$$\begin{aligned}F(Y) &= (Y-y)\prod_{j\in\mathrm{GF}(q)}\left(Y - y - \frac{1}{\eta + j\zeta}\right)\\ &= (Y-y)(Y-z)\prod_{0\neq j\in\mathrm{GF}(q)}\left(Y - y - \frac{1}{\eta + j\zeta}\right).\end{aligned} \tag{9.19}$$

To reproduce some of the results of Section 2, now assume that

$$(A,B) = (1,X). \tag{9.20}$$

Then by (9.1) we see that F is irreducible over K and, upon letting $T = \tau^{1/q} \in \Omega$, by (9.13) and (9.17) we see that

$$K = k(X) \quad \text{and} \quad \mathrm{SF}(F,K) = k(T)\,, \tag{9.21}$$

$$T^q = \tau \tag{9.22}$$

$$y = -1 - (T^q - T)^{q-1}. \tag{9.23}$$

In view of (9.22), by (9.14) to (9.18) we get

$$\zeta = \frac{1}{(T^q - T)^q}, \tag{9.24}$$

$$\eta = T^q\zeta = \frac{1}{(T^{q-1} - 1)^q}, \tag{9.25}$$

$$\xi = \zeta^{q-1} = \frac{\eta^q}{\eta + 1} = \frac{1}{(T^q - T)^{q(q-1)}}, \tag{9.26}$$

$$y = -1 - (T^q - T)^{q-1} \tag{9.27}$$

$$z = -1 - (T^q - T)^{q-1} + (T^{q-1} - 1)^q. \tag{9.28}$$

References

[1] Abhyankar, S. S.: *Algebraic Geometry for Scientists and Engineers*. Mathematical Surveys and Monographs **35**. American Mathematical Society, Providence, RI, 1990.

[2] Abhyankar, S. S.: Nice equations for nice groups. *Israel J. Math.* **88** (1994), 1–23.

[3] Abhyankar, S. S.: Projective polynomials. *Proc. Amer. Math. Soc.* **125** (1997), 1643–1650.

[4] Abhyankar, S. S.: Semilinear transformation. *Proc. Amer. Math. Soc.* **127** (1999), 2511–2525.

[5] Abhyankar, S. S.: Galois theory of semilinear transformations. In *Aspects of Galois theory (Gainesville, FL, 1996)*, 1–37. London Math. Soc. Lecture Note Ser. **256**. Cambridge Univ. Press, Cambridge, 1999.

[6] Abhyankar, S. S. and Sundaram, G. S.: Galois theory of Moore-Carlitz-Drinfeld modules. *C. R. Acad. Sci. Paris Sér. I Math.* **325** (1997), 349–353.

[7] Albert, A. A.: *Modern Higher Algebra*. Chicago University Press, Chicago, 1937.

Recibido: 20 de febrero de 2002

Shreeram S. Abhyankar
Mathematics Department
Purdue University
West Lafayette, IN 47907, USA
ram@cs.purdue.edu

This work was partly supported by NSF Grant DMS 99-88166 and NSA grant MDA 904-99-1-0019.