ELSEVIER

Discrete Mathematics 133 (1994) 25–46

DISCRETE MATHEMATICS

Alternating group coverings of the affine line for characteristic two☆

Shreeram S. Abhyankar[a,*], Jun Ou[a], Avinash Sathaye[b]

[a] *Mathematics Department, Purdue University, West Lafayette, IN 47907, USA*
[b] *Mathematics Department, University of Kentucky, Lexington, KY 40506, USA*

Received 15 December 1992

Abstract

Unramified coverings of the affine line in characteristic two are constructed having alternating groups as Galois groups. The proof uses Jacobson's criterion for the Galois group of an equation to be contained in the alternating group. Alternative proofs use the Berlekamp discriminant or the Revoy discriminant. These are related to the Arf invariant.

1. Introduction

In [1], the algebraic fundamental group $\pi_A(L_k)$ of the affine line L_k over an algebraically closed ground field k of nonzero characteristic p was considered, and it was conjectured that $\pi_A(L_k)$ coincides with the set of all quasi p-groups; note that $\pi_A(L_k)$ is defined to be the set of all finite Galois groups of unramified coverings of L_k, and a quasi p-group is a finite group which is generated by all its p-Sylow subgroups. *The main aim of this paper is to prove that for* $p=2$ *and every positive integer* m *different from* 3, 4, 6, 7 *we have* $A_m \in \pi_A(L_k)$. We shall deduce this from some results of [3] and [6]. The deduction will be based on Jacobson's criterion for the Galois group of an equation to be contained in the alternating group. With an eye on future applications, we shall give several versions of Jacobson's criterion as well as the said deduction.

In greater detail, in support of the above conjecture, in [1], the equation $Y^n - XY^t + 1 = 0$, with $n = q + t$, giving an unramified covering of the X-axis L_k was written down, and it was suggested that its Galois group $\bar{G}_{n,q}$ be computed; here q is a positive power of p, and t is a positive integer nondivisible by p. In [3], this computation was carried out when either $q = p$ or $t = 1$, and as a consequence of it and

☆ Partly supported by NSF grant DMS 91-01424 and NSA grant MDA 904-92-H-3035.
* Corresponding author.

SSDI 0012-365X(93)E0073-D

some other related computations it was shown that if: $m \geqslant p > 2$ then $A_m \in \pi_A(L_k)$, and if: $m \geqslant p = 2$ then $S_m \in \pi_A(L_k)$; for other results in support of the said conjecture see Abhyankar [2,4,5] and Serre [15]. Here A_m is the alternating group and S_m is the symmetric group for any positive integer m. Continuing this computation, in [6] it was shown that

$$\text{if } q < t \text{ and } p > 2 \text{ then } \bar{G}_{n,q} = A_n \tag{1.0}$$

whereas

$$\text{if } q < t \text{ and } p = 2 \text{ then } \bar{G}_{n,q} = A_n \text{ or } S_n. \tag{1.1}$$

In the present paper we shall show that

$$\textit{if } p = 2 < q \textit{ and } 2 < t \textit{ then } \bar{G}_{n,q} \subset A_n. \tag{1.1'}$$

In view of (1.1) and (1.1′) we shall have shown that

$$\text{if } p = 2 < q < t \text{ then } \bar{G}_{n,q} = A_n. \tag{1.1*}$$

In [3] we also computed the Galois groups $\tilde{G}_{n,t,s,a}$ of the equation $Y^n - aY^t + X^s = 0$ which gives an unramified covering of L_k, where a is a nonzero element of k and n, t, s are positive integers with $t < n \equiv 0(p)$ and $\mathrm{GCD}(n,t) = 1$ and $s \equiv 0(t)$. In particular we showed that

$$\text{if } p = 2 \text{ and either } 1 < t < 4 < n \text{ or } 1 < t < n-3, \text{ then } \tilde{G}_{n,t,s,a} = A_n \text{ or } S_n. \tag{1.2}$$

In the present paper we shall show that

$$\textit{if } p = 2 < n \textit{ then } \tilde{G}_{n,t,s,a} \subset A_n. \tag{1.2'}$$

In view of (1.2) and (1.2′) we shall have shown that

$$\text{if } p = 2 \text{ and either } 1 < t < 4 < n \text{ or } 1 < t < n-3, \text{ then } \tilde{G}_{n,t,s,a} = A_n. \tag{1.2*}$$

The proofs of (1.1′) and (1.2′) will be based on Jacobson's criterion for the Galois group of an equation to be contained in the alternating group which is valid for any characteristic; this may be compared to the more classical criterion which requires the modified discriminant to be a square and which is not valid in characteristic two. In Section 2, we shall review Jacobson's criterion and deduce from it a general result on trinomials of which (1.1′) and (1.2′) are special cases; see (2.27). Although Jacobson's criterion became more popular as Exercise 3 of Section 4.8 of Volume I of his 1974 book on Basic Algebra [13], it actually appeared as Exercise 1 of Section 1 of Chapter II of his 1964 Abstract Algebra III [12]. In Sections 3 and 4, which are independent of each other, we shall give several variations of Jacobson's criterion and deduce several different proofs of the general trinomial result (2.27). In Section 5 we shall relate these variations to the invariant of Arf [8] and the discriminants of Berlekamp [10] and Revoy [14] which were collated by Wadsworth [16], and we

shall also indicate that the basic function used in Jacobson's criterion was rediscovered by Bertin [11].

(1.3) Recall that $n=q+t$ where q is any positive power of p, and t is any integer with $t\not\equiv 0(p)$. Also let s be any positive integer, and let a be any nonzero element of k. By considering the polynomial $\bar{F}_{n,q,s,a}=Y^n-aX^sY^t+1$ and its Galois group $\bar{G}_{n,q,s,a}=\mathrm{Gal}(\bar{F}_{n,q,s,a}k(X))$, in Theorem 4 of [6] it is shown that if $2=p<q<t$ and if we know that $\bar{G}_{n,q}\subset A_n$ then the equation $\bar{F}_{n,q,s,a}=0$ gives an unramified covering of L_k with $\bar{G}_{n,q,s,a}=A_n$. Therefore by (1.1*) we see that:

(1.3.1) if $2=p<q<t$ then $\bar{F}_{n,q,s,a}=0$ gives an unramified covering of L_k and for its Galois group we have $\bar{G}_{n,q,s,a}=A_n$.

Likewise, by considering the monic polynomial of degree $n-1$ with coefficients in $k[X]$ given by

$$\bar{F}'_{n,q,s,a}=t^{-2}[(Y+t)^t-Y^t](Y+t)^q-aX^{-rs}Y^t=0$$

with

$$r=(q+t)\,\mathrm{LCM}\left(t,\frac{q-1}{\mathrm{GCD}(q-1,q+t)}\right)$$

and by considering its Galois group $\bar{G}'_{n,q,s,a}=\mathrm{Gal}\,\bar{F}'_{n,q,s,a}k(X))$, in Theorem 6 of [6] it is shown that: if $2=p<q<t$ and if we know that $\bar{G}_{n,q}\subset A_n$ then the equation $\bar{F}'_{n,q,s,a}=0$ gives an unramified covering of L_k with $\bar{G}'_{n,q,s,a}=A_{n-1}$. Therefore by (1.1*) we see that:

(1.3.2) if $2=p<q<t$ then $\bar{F}'_{n,q,s,a}=0$ gives an unramified covering of L_k and for its Galois group we have $\bar{G}'_{n,q,s,a}=A_{n-1}$.

Thus we get the following.

(1.4) Theorem. *For $p=2$ and every positive integer m different from $3,4,6,7$ we have $A_m\in\pi_A(L_k)$.*

Namely, if $9\leqslant m\not\equiv 0(2)$ then use (1.1*) with $q=4$ and $m=n$, if $8\leqslant m\equiv 0(2)$ then use (1.3.2) with $q=4$ and $m=n-1$, and if $m=5$ then note that $A_5=\mathrm{PSL}(2,4)\in\pi_A(L_k)$ (see [2] for the fact that for any prime p we have $\mathrm{PSL}(2,q)\in\pi_A(L_k)$ for every positive power q of p). For $8\leqslant m\equiv 0(2)$, we may alternatively use (1.2*) with $m=n$ and with $t=(n/2)-1$ or $t=(n/2)-2$ according as $n/2$ is even or odd. It may be noted that all these proofs have been elementary in the sense of not using CT (=the classification theorem of finite simple groups). Since $A_1=A_2=1$ and since A_3 and A_4 are not quasi 2-groups, this only leaves us with A_6 and A_7. The story will be completed in a forthcoming paper of Abhyankar and Yie [7] by writing down simple equations to show that A_6 and A_7 also belong to $\pi_A(L_k)$ in case of $p=2$.

The possibility of (1.1*) when $q=4$ was first suggested to us by Serre. Then it was Leep who provided us with much information about the various discriminants which work in characteristic two. So to Serre and Leep, many thanks!

2. Jacobson's criterion

Let n be an integer with $n>1$, and consider the polynomials $D(R)$, $D^*(R)$, $\Delta(R)$ in indeterminates $R=(R_1, R_2, \ldots, R_n)$ with coefficients in $\mathbb{Z}$ given by

$$D(R)=\sum_{\pi\in A_n}\prod_{i=1}^{n} R_{\pi(i)}^{i-1} \quad \text{and} \quad D^*(R)=\sum_{\sigma\in S_n\setminus A_n}\prod_{i=1}^{n} R_{\sigma(i)}^{i-1} \tag{2.1}$$

and

$$\Delta(R)=\prod_{1\leqslant i<j\leqslant n}(R_j-R_i). \tag{2.2}$$

Consider the n by n (van der Monde) determinant whose ith row is $(1, R_i, R_i^2, \ldots, R_i^{n-1})$ for $1\leqslant i\leqslant n$; by calculating it in two different ways, and then equating the two values so obtained we see that

$$D(R)-D^*(R)=\Delta(R). \tag{2.3}$$

By squaring both sides of (2.3) and then adding $4D(R)D^*(R)$ to them we get

$$[D(R)+D^*(R)]^2=4D(R)D^*(R)+\Delta^2(R). \tag{2.4}$$

Let $B=(B_1, B_2, \ldots, B_n)$ be n indeterminates and, for $1\leqslant i\leqslant n$, let us assign weight i to B_i. Let $C(R)=(C_1(R), C_2(R), \ldots, C_n(R))$ where, for $1\leqslant i\leqslant n$, we have put $C_i(R)=(-1)^i$ times the ith elementary symmetric function of R; in other words, we have

$$Y^n+\sum_{i=1}^{n} C_i(R)\,Y^{n-i}=\prod_{i=1}^{n}(Y-R_i).$$

Now $D(R)+D^*(R)$ is a symmetric homogeneous polynomial of degree $n(n-1)/2$ in R with coefficients in $\mathbb{Z}$ and hence, by the fundamental theorem on symmetric functions, there exists a unique isobaric polynomial $U(B)$ of weight $n(n-1)/2$ in B with coefficients in $\mathbb{Z}$ such that

$$U(C(R))=D(R)+D^*(R). \tag{2.5}$$

Likewise $D(R)D^*(R)$ and $\Delta^2(R)$ are symmetric homogeneous polynomials of degree $n(n-1)$ in R with coefficients in $\mathbb{Z}$ and hence there exist unique isobaric polynomials $V(B)$ and $W(B)$ of weight $n(n-1)$ in B with coefficients in $\mathbb{Z}$ such that

$$V(C(R))=D(R)D^*(R) \quad \text{and} \quad W(C(R))=\Delta^2(R). \tag{2.6}$$

Since $C_1(R), C_2(R), \ldots, C_n(R)$ are algebraically independent over $\mathbb{Z}$, by (2.4)–(2.6) we get

$$U^2(B)=4V(B)+W(B) \tag{2.7}$$

as an identity in $\mathbb{Z}[B]$.

Let

$$f=f(Y)=Y^n+\sum_{i=1}^{n} b_i Y^{n-i} \tag{2.7*}$$

be a monic polynomial of degree n in Y with coefficients $b=(b_1, b_2, \ldots, b_n)$ in a field K, and let $r=(r_1, r_2, \ldots, r_n)$ be the roots of f in some overfield of K. By substituting b for B in (2.7) we get

$$U^2(b)=4V(b)+W(b). \tag{2.8}$$

Since $C(r)=b$, by substituting r for R in (2.2), (2.3), (2.5) and (2.6) we also get

$$U(b)=D(r)+D^*(r) \quad \text{and} \quad V(b)=D(r)D^*(r) \tag{2.9}$$

and

$$W(b)=\Delta^2(r)=\left[\prod_{1\le i<j\le n}(r_j-r_i)\right]^2=[D(r)-D^*(r)]^2. \tag{2.10}$$

As in Section 20 of [3], by $\mathrm{Disc}_Y^*(f)$ we shall denote the *modified Y-discriminant* of f which was *defined* by putting $\mathrm{Disc}_Y^*(f)=(-1)^{n(n-1)/2}\,\mathrm{Disc}_Y(f)$ where $\mathrm{Disc}_Y(f)$ is the *Y-discriminant* of f, i.e., $\mathrm{Disc}_Y(f)=\mathrm{Res}_Y(f, f_Y)$; thus now by (2.10) we have

$$\mathrm{Disc}_Y^*(f)=(-1)^{n(n-1)/2}\mathrm{Disc}_Y(f)=W(b). \tag{2.11}$$

For a moment assume that the roots of f are pairwise distinct. Then by (2.10) we have $D(r)\neq D^*(r)$. By (2.1) we also see that $\pi(D(r))=D(r)$ for all $\pi\in A_n$, and $\sigma(D(r))=D^*(r)$ for all $\sigma\in S_n\setminus A_n$. Consequently $\mathrm{Gal}(f, K)\subset A_n$ iff $D(r)$ and $D^*(r)$ both belong to K. Therefore by (2.9) we see that $\mathrm{Gal}(f, K)\subset A_n$ iff the polynomial $Z^2-U(b)Z+V(b)$ factors into linear factors in $K[Z]$. In case $U(b)\neq 0$, upon 'multiplying' the roots of the polynomial $Z^2-U(b)Z+V(b)$ by $-U(b)^{-1}$ we obtain the polynomial $Z^2+Z+V(b)U(b)^{-2}$, and hence one of them factors into linear factors in $K[Z]$ iff the other does. Thus we get the following.

(2.12) Jacobson's criterion. *Assume that f has no multiple roots*; [*in view of* (2.10) *this is equivalent to assuming that* $W(b)\neq 0$], *Then we have that* $\mathrm{Gal}(f, K)\subset A_n$ *iff the polynomial* $Z^2-U(b)Z+V(b)$ *factors into linear factors in* $K[Z]$. *Moreover, in case* $U(b)\neq 0$, *we have that* $\mathrm{Gal}(f, K)\subset A_n$ *iff the polynomial* $Z^2+Z+V(b)U(b)^{-2}$ *factors into linear factors in* $K[Z]$, *i.e. iff* $-V(b)U(b)^{-2}=z^2+z$ *for some* $z\in K$.

To apply this criterion to a trinomial, let d and e be integers with

$$0<e=n-d<d<n \quad \text{and} \quad \mathrm{GCD}(n,d)=1 \tag{2.12'}$$

and let $\bar{U}(B_d,B_n)$, $\bar{V}(B_d,B_n)$, $\bar{W}(B_d,B_n)$ to be the polynomials in B_d and B_n with coefficients $\mathbb{Z}$ obtained by putting zero for the remaining variables in $U(B)$, $V(B)$, $W(B)$ respectively. Now by (2.7) we get

$$\bar{U}^2(B_d,B_n)=4\bar{V}(B_d,B_n)+\bar{W}(B_d,B_n) \tag{2.13}$$

and, in view of (2.11), by applying the discriminant calculations of Section 20 of [3] to the polynomial $Y^n+B_dY^e+B_n$ we also get

$$\bar{W}(B_d,B_n)=(-1)^{n(n-1)/2}n^nB_n^{n-1}+(-1)^{(n+2)(n-1)/2}d^de^eB_n^{e-1}B_d^n. \tag{2.14}$$

Now B_n^{n-1} has weight $n(n-1)$ and hence, because $\mathrm{GCD}(n,d)=1$, the only other possible monomials of weight $n(n-1)$ in B_n and B_d are $B_n^{n-1-d}B_d^n$, $B_n^{n-1-2d}B_d^{2n}$, ...,; since $n-1-2d<0$ and $n-1-d=e-1$, we see that B_n^{n-1} and $B_n^{e-1}B_d^n$ are the only monomials of weight $n(n-1)$ in B_n and B_d; therefore $B_n^{(n-1)/2}$ and $B_n^{(e-1)/2}B_d^{n/2}$ are the only possible monomials of weight $n(n-1)/2$ in B_n and B_d; out of the last two monomials, only the first makes sense if n is odd, and only the second makes sense if n is even. Therefore, since $U(B)$ and $V(B)$ are isobaric of weight $n(n-1)/2$ and $n(n-1)$ respectively, we conclude that

$$\bar{U}(B_d,B_n)=\begin{cases}uB_n^{(n-1)/2} \text{ with } u\in\mathbb{Z} & \text{if } n\not\equiv 0(2),\\ u'B_n^{(e-1)/2}B_d^{n/2} \text{ with } u'\in\mathbb{Z} & \text{if } n\equiv 0(2),\end{cases} \tag{2.15}$$

and

$$\bar{V}(B_d,B_n)=vB_n^{n-1}+v'B_n^{e-1}B_d^n \quad \text{with } v,v'\in\mathbb{Z}. \tag{2.16}$$

By (2.13) to (2.16) we see that

$$v=\begin{cases}(1/4)[u^2-(-1)^{n(n-1)/2}n^n]\in\mathbb{Z} & \text{if } n\not\equiv 0(2),\\ (1/4)[-(-1)^{n(n-1)/2}n^n]\in 2\mathbb{Z} & \text{if } n\equiv 0(2),\end{cases} \tag{2.17}$$

and

$$v'=\begin{cases}(1/4)[-(-1)^{(n+2)(n-1)/2}d^de^e]\in 2\mathbb{Z} & \text{if } n\not\equiv 0(2) \text{ and } e>2;\\ (1/4)[-(-1)^{(n+2)(n-1)/2}d^de^e]\in 2\mathbb{Z} & \text{if } n\not\equiv 0(2) \text{ and } e=1<d-1;\\ (1/4)[-(-1)^{(n+2)(n-1)/2}d^de^e]\in\mathbb{Z}\setminus 2\mathbb{Z} & \text{if } n\not\equiv 0(2) \text{ and } e=1=d-1;\\ (1/4)[-(-1)^{(n+2)(n-1)/2}d^de^e]\in\mathbb{Z}\setminus 2\mathbb{Z} & \text{if } n\not\equiv 0(2) \text{ and } e=2;\\ (1/4)[u'^2-(-1)^{(n+2)(n-1)/2}d^de^e]\in\mathbb{Z} & \text{if } n\equiv 0(2).\end{cases} \tag{2.18}$$

Clearly an integer is odd iff its square is odd, and hence by (2.15)–(2.18) we get

$$\bar{U}(B_d,B_n)=\begin{cases}uB_n^{(n-1)/2} & \text{with } u\in\mathbb{Z}\setminus 2\mathbb{Z} \quad \text{if } n\not\equiv 0(2),\\ u'B_n^{(e-1)/2}B_d^{n/2} & \text{with } u'\in\mathbb{Z}\setminus 2\mathbb{Z} \quad \text{if } n\equiv 0(2).\end{cases} \tag{2.19}$$

For any odd integer w we have $w=1+2w^*$ for some integer w^* and this gives $w^2=1+4w^*(w^*+1)$ and hence $w^2\equiv 1(8)$ because $w^*(w^*+1)$ is always even; therefore, by (2.17)–(2.19) we see that

$$v'=\begin{cases}(1/4)[u^2-(-1)^{n(n-1)/2}n^n]\in 2\mathbb{Z} & \text{if } n\equiv 1(8),\\ (1/4)[u^2-(-1)^{n(n-1)/2}n^n]\in 2\mathbb{Z} & \text{if } n\equiv 7(8),\\ (1/4)[u^2-(-1)^{n(n-1)/2}n^n]\in \mathbb{Z}\setminus 2\mathbb{Z} & \text{if } n\equiv 3(8),\\ (1/4)[u^2-(-1)^{n(n-1)/2}n^n]\in \mathbb{Z}\setminus 2\mathbb{Z} & \text{if } n\equiv 5(8)\end{cases} \tag{2.20}$$

and

$$v'=\begin{cases}(1/4)[u'^2-(-1)^{(n+2)(n-1)/2}d^de^e]\in 2\mathbb{Z} & \text{if } n\equiv 0(8),\\ (1/4)[u'^2-(-1)^{(n+2)(n-1)/2}d^de^e]\in 2\mathbb{Z} & \text{if } n\equiv 2(8) \text{ and } e\equiv d(8),\\ (1/4)[u'^2-(-1)^{(n+2)(n-1)/2}d^de^e]\in 2\mathbb{Z} & \text{if } n\equiv 6(8) \text{ and } e\equiv d(8),\\ (1/4)[u'^2-(-1)^{(n+2)(n-1)/2}d^de^e]\in \mathbb{Z}\setminus 2\mathbb{Z} & \text{if } n\equiv 2(8) \text{ and } e\not\equiv d(8),\\ (1/4)[u'^2-(-1)^{(n+2)(n-1)/2}d^de^e]\in \mathbb{Z}\setminus 2\mathbb{Z} & \text{if } n\equiv 6(8) \text{ and } e\not\equiv d(8),\\ (1/4)[u'^2-(-1)^{(n+2)(n-1)/2}d^de^e]\in \mathbb{Z}\setminus 2\mathbb{Z} & \text{if } n\equiv 4(8).\end{cases} \tag{2.21}$$

Remembering that K is a field, and considering the trinomial

$$\bar f=\bar f(Y)=Y^n+\bar b_d Y^e+\bar b_n \text{ with } \bar b_d \text{ and } \bar b_n \text{ in } K \tag{2.21*}$$

by (2.12) we get the following.

(2.22) Special trinomial criterion. *Assume that $\bar f$ has no multiple roots; [in view of (2.10) this is equivalent to assuming that $\bar W(\bar b_d, \bar b_n)\neq 0$]. Then we have that $\mathrm{Gal}(\bar f, K)\subset A_n$ iff the polynomial $Z^2-\bar U(\bar b_d, \bar b_n)Z+\bar V(\bar b_d, \bar b_n)$ factors into linear factors in $K[Z]$. Moreover, in case $\bar U(\bar b_d, \bar b_n)\neq 0$, we have that $\mathrm{Gal}(\bar f, K)\subset A_n$ iff the polynomial $Z^2+Z+\bar V(\bar b_d, \bar b_n)\bar U(\bar b_d, \bar b_n)^{-2}$ factors into linear factors in $K[Z]$, i.e. iff $-\bar V(\bar b_d, \bar b_n)\bar U(\bar b_d, \bar b_n)^{-2}=z^2+z$ for some $z\in K$.*

Now Z^2+Z+1 is the only irreducible polynomial of degree two over the prime field GF(2) of characteristic two, and its splitting field in the field GF(4) of cardinality 4. Hence by (2.14)–(2.22) we get the following.

(2.23) Odd trinomial criterion. *Assume that the characteristic of K is two, and n is odd. Also assume that f has no multiple roots; [in view of (2.10) and (2.14), this is equivalent to assuming that $\bar b_n\neq 0$ which, in view of (2.19), is equivalent to assuming that $\bar U(\bar b_d, \bar b_n)\neq 0$]. Then, in case either $e=2$ or $e=1=d-1$, and either $n\equiv 1(8)$ or $n\equiv 7(8)$, we have that $\mathrm{Gal}(\bar f, K)\subset A_n$ iff $\bar b_n^{-d}\bar b_d^n=z^2+z$ for some $z\in K$. Likewise, in case either $e=2$ or $e=1=d-1$, and either $n\equiv 3(8)$ or $n\equiv 5(8)$, we have that $\mathrm{Gal}(\bar f, K)\subset A_n$ iff $1+\bar b_n^{-d}\bar b_d^n=z^2+z$ for some $z\in K$. Moreover, in case either $e>2$ or $e=1<d-1$, and either $n\equiv 1(8)$ or $n\equiv 7(8)$, we have $\mathrm{Gal}(\bar f, K)\subset A_n$. On the other hand, in case either $e>2$ or $e=1<d-1$, and either $n\equiv 3(8)$ or $n\equiv 5(8)$, we have that $\mathrm{Gal}(\bar f, K)\subset A_n$ iff $GF(4)\subset K$.*

Consequently, in case either $e>2$ *or* $e=1<d-1$, *we have that if* $\mathrm{GF}(4)\subset K$ *then* $\mathrm{Gal}(\bar{f}, K)\subset A_n$. *Hence, in case either* $e>2$ *or* $e=1<d-1$, *we have that if* K *contains an algebraic closure of its prime subfield, then* $\mathrm{Gal}(\bar{f}, K)\subset A_n$.

Similarly, by (2.14)–(2.22) we also get the following.

(2.24) Even trinomial criterion. *Assume that the characteristic of* K *is two, and* n *is even. Also assume that* $\bar{f}$ *has no multiple roots;* [*in view of* (2.10) *and* (2.14), *this is equivalent to assuming that* $\bar{b}_d\neq 0\neq \bar{b}_n^{e-1}$ *which, in view of* (2.19), *is equivalent to assuming that* $\bar{U}(\bar{b}_d, \bar{b}_n)\neq 0$]. *Then, in case* $n\equiv 0(8)$, *we have* $\mathrm{Gal}(\bar{f}, K)\subset A_n$. *Likewise, in case* $e\equiv d(8)$ *and either* $n\equiv 2(8)$ *or* $n\equiv 6(8)$, *we have*; $\mathrm{Gal}(\bar{f}, K)\subset A_n$. *On the other hand, in case* $n\equiv 4(8)$, *we have that* $\mathrm{Gal}(\bar{f}, K)\subset A_n$ *iff* $GF(4)\subset K$. *Likewise, in case* $e\not\equiv d(8)$ *and either* $n\equiv 2(8)$ *or* $n\equiv 6(8)$, *we have that* $\mathrm{Gal}(\bar{f}, K)\subset A_n$ *iff* $GF(4)\subset K$. *Consequently if* $GF(4)\subset K$ *then* $\mathrm{Gal}(\bar{f}, K)\subset A_n$. *Hence in particular if* K *contains an algebraic closure of its prime field then* $\mathrm{Gal}(\bar{f}, K)\subset A_n$.

By combining the odd and even trinomial criteria, we get the following.

(2.25) Characteristic two trinomial precriterion. *Assume that the characteristic of* K *is two. Also assume that* $\bar{f}$ *has no multiple roots;* [*in view of* (2.10) *and* (2.14), *for odd* n *this is equivalent to assuming that* $\bar{b}_n\neq 0$, *and for even* n *it is equivalent to assuming that* $\bar{b}_d\neq 0\neq \bar{b}_n^{e-1}$]. *Then firstly, in case either* $e=2$ *or* $d=2$, *and either* $n\equiv 1(8)$ *or* $n\equiv 7(8)$, *we have that* $\mathrm{Gal}(\bar{f}, K)\subset A_n$ *iff* $\bar{b}_n^{-d}\bar{b}_d^n=z^2+z$ *for some* $z\in K$. *Secondly, in case either* $e=2$ *or* $d=2$, *and either* $n\equiv 3(8)$ *or* $n\equiv 5(8)$, *we have that* $\mathrm{Gal}(\bar{f}, K)\subset A_n$ *iff* $1+\bar{b}_n^{-d}\bar{b}_d^n=z^2+z$ *for some* $z\in K$. *Thirdly, in case* $e\neq 2\neq d$, *and either* $n\equiv 1(8)$ *or* $n\equiv 7(8)$, *we have* $\mathrm{Gal}(\bar{f}, K)\subset A_n$. *Fourthly, in case* $e\neq 2\neq d$, *and either* $n\equiv 3(8)$ *or* $n\equiv 5(8)$, *we have that* $\mathrm{Gal}(\bar{f}, K)\subset A_n$ *iff* $\mathrm{GF}(4)\subset K$. *Fifthly, in case* $n\equiv 0(8)$, *we have* $\mathrm{Gal}(\bar{f}, K)\subset A_n$. *Sixthly, in case* $e\equiv d(8)$ *and either* $n\equiv 2(8)$ *or* $n\equiv 6(8)$, *we have*; $\mathrm{Gal}(\bar{f}, K)\subset A_n$. *Seventhly, in case* $n\equiv 4(8)$, *we have that* $\mathrm{Gal}(\bar{f}, K)\subset A_n$ *iff* $\mathrm{GF}(4)\subset K$. *Eighthly, in case* $e\not\equiv d(8)$ *and either* $n\equiv 2(8)$ *or* $n\equiv 6(8)$, *we have that* $\mathrm{Gal}(\bar{f}, K)\subset A_n$ *iff* $\mathrm{GF}(4)\subset K$. [*Note that, since* $\mathrm{GCD}(n,d)=1=\mathrm{GCD}(n,e)$, *these eight cases are exhaustive and mutually exclusive*]. *Consequently, in case* $e\neq 2\neq d$, *we have that if* $\mathrm{GF}(4)\subset K$ *then* $\mathrm{Gal}(\bar{f}, K)\subset A_n$. *Hence, in case* $e\neq 2\neq d$, *we have that if* K *contains an algebraic closure of its prime subfield, then* $\mathrm{Gal}(\bar{f}, K)\subset A_n$.

Now let t be an integer with

$$0<t<n \quad \text{and} \quad \mathrm{GCD}(n,t)=1 \tag{2.25'}$$

and consider the trinomial

$$f^*=f^*(Y)=Y^n+b^*_{n-t}Y^t+b^*_n \quad \text{with } b^*_{n-t} \text{ and } b^*_n \text{ in } K. \tag{2.25*}$$

Note that by Section 20 of [3] we have

$$\mathrm{Disc}_Y(f^*)=n^n b_n^{*n-1}+(-1)^{n-1}(n-t)^{n-t}t^t b_n^{*t-1}b_{n-t}^{*n}. \tag{2.26}$$

If $t<(n/2)$ then upon taking $\bar{f}=f^*$, whereas if $t>(n/2)$ and $b_n^*\neq 0$ then upon taking $\bar{f}$=the 'reciprocal' equation $Y^n+b_{n-t}^*b_n^{*-1}\,Y^{n-t}+b_n^{*-1}$, by (2.25) we get the following.

(2.27) Characteristic two trinomial criterion. *Assume that the characteristic of K is two, and $n>2$. Also assume that f^* has no multiple roots; [in view of (2.26), for odd n this is equivalent to assuming that $b_n^*\neq 0$, and for even n it is equivalent to assuming that $b_{n-t}^*\neq 0\neq b_n^{*t-1}$]. Then firstly, in case either $t=2$ or $n-t=2$, and either $n\equiv 1(8)$ or $n\equiv 7(8)$, we have that $\mathrm{Gal}(f^*,K)\subset A_n$ iff $b_n^{*t-n}b_{n-t}^{*n}=z^2+z$ for some $z\in K$. Secondly, in case either $t=2$ or $n-t=2$, and either $n\equiv 3(8)$ or $n\equiv 5(8)$, we have that $\mathrm{Gal}(f^*,K)\subset A_n$ iff $1+b_n^{*t-n}b_{n-t}^{*n}=z^2+z$ for some $z\in K$. Thirdly, in case $t\neq 2\neq n-t$, and either $n\equiv 1(8)$ or $n\equiv 7(8)$, we have $\mathrm{Gal}(f^*,K)\subset A_n$. Fourthly, in case $t\neq 2\neq n-t$, and either $n\equiv 3(8)$ or $n\equiv 5(8)$, we have that $\mathrm{Gal}(f^*,K)\subset A_n$ iff $\mathrm{GF}(4)\subset K$. Fifthly, in case $n\equiv 0(8)$, we have $\mathrm{Gal}(f^*,K)\subset A_n$. Sixthly, in case $t\equiv n-t(8)$ and either $n\equiv 2(8)$, or $n\equiv 6(8)$, we have $\mathrm{Gal}(f^*,K)\subset A_n$. Seventhly, in case $n\equiv 4(8)$, we have that $\mathrm{Gal}(f^*,K)\subset A_n$ iff $\mathrm{GF}(4)\subset K$. Eighthly, in case $t\not\equiv n-t(8)$ and either $n\equiv 2(8)$ or $n\equiv 6(8)$, we have $\mathrm{Gal}(f^*,K)\subset A_n$ iff $\mathrm{GF}(4)\subset K$. [Note that, since $\mathrm{GCD}(n,t)=1$ and $n>2$, these cases are exhaustive and mutually exclusive.]*

As an immediate consequence of (2.27) we have the following.

(2.28) Characteristic two trinomial corollary. *Assuming that the characteristic K is two, f^* has no multiple roots, $n>2$, and $t\neq 2\neq n-t$, we have the following. If $\mathrm{GF}(4)\subset K$ then $\mathrm{Gal}(f^*,K)\subset A_n$. Hence in particular, if K contains an algebraic closure of its prime subfield then $\mathrm{Gal}(f^*,K)\subset A_n$.*

Proof of (1.1'). Take $K=k(X)$ and $b_{n-t}^*=-X$ and $b_n^*=1$ in (2.28). □

Proof of (1.2'). Take $K=k(X)$ and $b_{n-t}^*=-a$ and $b_n^*=X^s$ in (2.28). □

3. Resultant criterion

In this section we shall describe a procedure for calculating the expression $-V(b)U(b)^{-2}$ occurring in Jacobson's criterion.

Continuing the notation of Section 2, let

$$\tilde{\Delta}(R)=\prod_{1\leq i<j\leq n}(R_j+R_i). \tag{3.1}$$

Since plus and minus coincide in characteristic two, for the images $D_0(R)$, $D_0^*(R)$, $\Delta_0(R)$, $\tilde{\Delta}_0(R)$ of $D(R)$, $D^*(R)$, $\Delta(R)$, $\tilde{\Delta}(R)$ in $(\mathbb{Z}/2\mathbb{Z})[R]$ we have

$$D_0(R)+D_0^*(R)=D_0(R)-D_0^*(R) \quad \text{and} \quad \tilde{\Delta}_0(R)=\Delta_0(R)$$

and hence by (2.3) we get

$$\tilde{\Delta}_0(R)=D_0(R)+D_0^*(R)$$

and therefore, because $\tilde{\Delta}(R)$ and $D(R)+D^*(R)$ are both symmetric in R, we must have

$$\tilde{\Delta}(R)=D(R)+D^*(R)+2H(C(R)) \quad \text{with } H(B)\in\mathbb{Z}[B] \tag{3.2}$$

and we note that this defines $H(B)$ uniquely. Let $\tilde{D}(R)\in\mathbb{Z}[R]$ and $\tilde{D}^*(R)\in\mathbb{Z}[R]$ be defined by putting

$$\tilde{D}(R)=D(R)+H(C(R)) \quad \text{and} \quad \tilde{D}^*(R)+H(C(R)) \tag{3.3}$$

and note that now by (3.2) we get

$$\tilde{\Delta}(R)=\tilde{D}(R)+\tilde{D}^*(R). \tag{3.4}$$

By (3.1) it is clear that $\tilde{\Delta}(R)$ is symmetric in R and hence there exists a unique $\tilde{U}(B)\in\mathbb{Z}[B]$ such that

$$\tilde{\Delta}(R)=\tilde{U}(C(R)). \tag{3.5}$$

By (2.1) and (3.3) we see that $\tilde{D}(R)\tilde{D}^*(R)$ is symmetric in R and hence there exists a unique $\tilde{V}(B)\in\mathbb{Z}[B]$ such that

$$\tilde{V}(C(R))=\tilde{D}(R)\tilde{D}^*(R). \tag{3.6}$$

By (2.3) and (3.3) we have

$$[\tilde{D}(R)+\tilde{D}^*(R)]^2=4\tilde{D}(R)\tilde{D}^*(R)+\Delta^2(R)$$

and

$$\tilde{D}(R)+\tilde{D}^*(R)=D(R)+D^*(R)+2H(C(R))$$

and hence by (2.5), (2.6), (3.4), (3.5) and (3.6) we get

$$\tilde{U}^2(B)=4\tilde{V}(B)+W(B) \quad \text{and} \quad \tilde{U}(B)=U(B)+2H(B). \tag{3.7}$$

By (2.7) and (3.7) we respectively have

$$4\tilde{V}(B)=[U^2(B)-W(B)]+4[H(B)U(B)+H^2(B)] \text{ and } U^2(B)-W(B)=4V(B)$$

and hence we get

$$\tilde{V}(B)=V(B)+H(B)U(B)+H^2(B). \tag{3.8}$$

For every $f(Y)$ as in (2.7*), we *define* $f^{\square}(Y)$ and $f^{\triangle}(Y)$ to be the unique polynomials in Y with coefficients in K such that

$$f(Y)=Yf^{\square}(Y^2)+f^{\triangle}(Y^2) \tag{3.9}$$

and we note that then the coefficients of $f^{\square}(Y)$ and $f^{\triangle}(Y)$ are amongst the coefficients of $f(Y)$. We claim that

$$\mathrm{Res}_Y(f(Y), f^{\square}(Y^2))=\tilde{U}^2(b) \tag{3.10}$$

with the understanding that $\mathrm{Res}_Y(f(Y), 0)=0$. Namely, for the polynomial

$$F(Y)=Y^n+\sum_{i=1}^{n} C_i(R)\,Y^{n-i}\in(\mathbb{Z}[R])[Y]$$

by (3.1) we have

$$\mathrm{Res}_Y(F(Y), F(-Y))=(-1)^n 2^n C_n(R)\tilde{\Delta}^2(R)$$

and clearly we have

$$\mathrm{Res}_Y(F(Y), F(-Y))=(-1)^n\mathrm{Res}_Y(F(Y), F(Y)-F(-Y))$$

and by (3.9) we have

$$F(Y)-F(-Y)=2YF^{\square}(Y^2)$$

and obviously we have

$$\mathrm{Res}_Y(F(Y), 2YF^{\square}(Y^2))=(-1)^n 2^n C_n(R)\,\mathrm{Res}_Y(F(Y), F^{\square}(Y^2))$$

and so conclude that

$$\mathrm{Res}_Y(F(Y), F^{\square}(Y^2))=\tilde{\Delta}(R)$$

and now, in view of (3.5), by substituting r for R in the above identity we get (3.10). By substituting b for B in (3.7) and (3.8), in view of (3.10) we get

$$\tilde{U}(b)=U(b)+2H(b) \tag{3.11}$$

and

$$\tilde{V}(b)=V(b)+H(b)U(b)+H^2(b) \tag{3.12}$$

and

$$\mathrm{Res}_Y(f(Y), f^{\square}(Y^2))=\tilde{U}^2(b)=4\tilde{V}(b)+W(b). \tag{3.13}$$

We introduce the *numerator Y-discriminant* of $f(Y)$, which we denote by $\mathrm{Num}_Y(f(Y))$ or $\mathrm{Num}_Y(f)$ or $\mathrm{Num}(f)$ and which we *define* by putting

$$\mathrm{Num}(f)=\tilde{V}(b). \tag{3.14}$$

Combining (2.11) and (3.14) we get

$$\mathrm{Num}(f)=\tilde{V}(b) \quad \text{and} \quad \mathrm{Disc}_Y^*(f)=(-1)^{n(n-1)/2}\mathrm{Disc}_Y(f)=W(b). \tag{3.15}$$

Finally, *in case f has no multiple roots*, we introduce the *rational Y-discriminant* of $f(Y)$, which we denote by $\mathrm{Rat}_Y(f(Y))$ or $\mathrm{Rat}_Y(f)$ or $\mathrm{Rat}(f)$, and which we *define* by putting

$$\mathrm{Rat}(f)=\mathrm{Num}(f)/\mathrm{Disc}_Y(f). \tag{3.16}$$

In case the characteristic of K is two and f has no multiple roots, by (3.11)–(3.16) we see that $\tilde{U}^2(b)=U^2(b)=W(b)=\mathrm{Disc}_Y^*(f)=\mathrm{Disc}_Y(f)\neq 0$ and $\mathrm{Rat}(f)=\tilde{V}(b)\tilde{U}^{-2}(b)=-V(b)U^{-2}(b)+\tilde{z}^2+\tilde{z}$ with $\tilde{z}=H(b)U^{-1}(b)\in K$, and clearly for every $z'\in K$ we have $z'+\tilde{z}\in K$ with $(z'+\tilde{z})^2+(z'+\tilde{z})=(z'^2+z')+(\tilde{z}^2+\tilde{z})$, and hence $\mathrm{Rat}(f)=z^2+z$ for some $z\in K$ iff $-V(b)U^{-2}(b)=z'^2+z'$ for some $z'\in K$; therefore by (2.12) we get the following.

(3.17) Resultant criterion. *Assume that the characteristic of K is two and f has no multiple roots. Then* $\mathrm{Gal}(f,K)\subset A_n$ *iff* $\mathrm{Rat}(f)=z^2+z$ *for some* $z\in K$.

Having expressed $-V(b)U^{-2}(b)$ in terms of $\mathrm{Rat}(f)$, let us give some methods of computing $\mathrm{Rat}(f)$.

So let $P=(P_1, P_2, \ldots, P_m)$ be indeterminates where m is a positive integer, let $E(P)=(E_1(P), E_2(P), \ldots, E_n(P))$ where $E_1(P), E_2(P), \ldots, E_n(P)$ are polynomials in P with coefficients in $\mathbb{Z}$, and consider the polynomial

$$F'(Y)=Y^n+\sum_{i=1}^{n} E_i(P)\,Y^{n-i}\in(\mathbb{Z}[P])[Y]. \tag{3.17*}$$

Now clearly there are unique polynomials $U'(P)$, $V'(P)$, $W'(P)$ in P with coefficients in $\mathbb{Z}$ such that

$$\tilde{U}(E(P))=U'(P), \qquad \tilde{V}(E(P))=V'(P), \qquad W(E(P))=W'(P) \tag{3.18}$$

and in view of (2.10), and (3.12)–(3.15) we get

$$\mathrm{Res}_Y(F'(Y), F'^{\square}(Y^2))=U'^2(P)=4V'(P)+W'(P) \tag{3.19}$$

and

$$\mathrm{Num}(F')=V'(P) \quad \text{and} \quad \mathrm{Disc}_Y^*(F')=W'(P) \tag{3.20}$$

and we have the following obvious.

(3.21) First computational principle. *If for some $r'=(r'_1, r'_2, \ldots, r'_m)$ with $r'_1, r'_2, \ldots, r'_m$ in K we have $b=E(r')$, then*

$$\tilde{U}(b)=U'(r') \quad \textit{and} \quad \mathrm{Res}_Y(f(Y), f^{\square}(Y))=\tilde{U}^2(b)=U'^2(r') \tag{3.21.1}$$

and

$$\mathrm{Num}(f)=\tilde{V}(b)=V'(r') \quad \textit{and} \quad \mathrm{Disc}^*_Y(f)=W(b)=W'(r'). \tag{3.21.2}$$

With positive integer t as in (2.25′) and the trinomial f^* as in (2.25*), by (2.26) we have $\mathrm{Disc}_Y(f^*)=u^*b_n^{*n-1}+u'^*b_n^{*t-1}b_{n-t}^{*n}$ with

$$u^*=\begin{cases} n^n\in\mathbb{Z}\setminus 2\mathbb{Z} & \text{if } n\not\equiv 0(2),\\ n^n\in 2\mathbb{Z} & \text{if } n\equiv 0(2)\end{cases}$$

and

$$u'^*=\begin{cases} (-1)^{n-1}(n-t)^{n-t}t^t\in 2\mathbb{Z} & \text{if } n\not\equiv 0(2),\\ (-1)^{n-1}(n-t)^{n-t}t^t\in\mathbb{Z}\setminus 2\mathbb{Z} & \text{if } n\equiv 0(2)\end{cases}$$

and hence

$$\mathrm{Disc}_Y(f^*)=u^*b_n^{*n-1}+u'^*b_n^{*t-1}b_{n-t}^{*n} \quad \text{with } u^*,\ u'^*\in\mathbb{Z} \text{ as above.} \tag{3.22}$$

Alternatively, we can deduce (3.22) by noting that, for any $c, c'\in K$, an easy calculation (similar to the discriminant calculation of Section 20 of [3]) shows that

$$\mathrm{Res}_Y(f^*(Y),\ cY^{n-1}+c'b_{n-t}^*Y^{t-1})=c^nb_n^{*n-1}+(-1)^{n-1}\times(c-c')^{n-t}c'^tb_n^{*t-1}b_{n-t}^{*n}. \tag{3.23}$$

To find $\mathrm{Num}(f^*)$, consider the trinomial

$$F^*(Y)=Y^n+B_{n-t}^*Y^t+B_n^*\in(\mathbb{Z}[B_{n-t}^*,B_n^*])[Y] \tag{3.23*}$$

with indeterminates B_{n-t}^* and B_n^*. Now by (3.15) and (3.22) we have

$$\mathrm{Disc}^*_Y(F^*)=(-1)^{n(n-1)/2}n^nB_n^{*n-1}+(-1)^{(n+2)(n-1)/2}(n-t)^{n-t}t^tB_n^{*t-1}B_{n-t}^{*n}$$

and clearly

$$F^{*\square}(Y^2)=\begin{cases} Y^{n-1}+B_{n-t}^*Y^{t-1} & \text{if } n\not\equiv 0(2) \text{ and } t\not\equiv 0(2),\\ Y^{n-1} & \text{if } n\not\equiv 0(2) \text{ and } t\equiv 0(2),\\ B_{n-t}^*Y^{t-1} & \text{if } n\equiv 0(2) \text{ and } t\not\equiv 0(2),\end{cases}$$

and hence, say by (3.23), we have

$$\mathrm{Res}_Y(F^*(Y),F^{*\square}(Y^2))=\begin{cases} B_n^{*n-1} & \text{if } n\not\equiv 0(2)\\ B_n^{*t-1}B_{n-t}^{*n} & \text{if } n\equiv 0(2) \text{ and } t\not\equiv 0(2)\end{cases}$$

and therefore, *assuming* $n>2$, by (3.11)–(3.15) we get

$$\mathrm{Num}(F^*)=v^*B_n^{*n-1}+v'^*B_n^{*t-1}B_{n-t}^{*n} \quad \text{with } v^*,\ v'^*\in\mathbb{Z}$$

where

$$v^*=\begin{cases}(1/4)[1-(-1)^{n(n-1)/2}n^n]\in 2\mathbb{Z} & \text{if } n\equiv 1(8),\\ (1/4)[1-(-1)^{n(n-1)/2}n^n]\in 2\mathbb{Z} & \text{if } n\equiv 7(8),\\ (1/4)[1-(-1)^{n(n-1)/2}n^n]\in \mathbb{Z}\setminus 2\mathbb{Z} & \text{if } n\equiv 3(8),\\ (1/4)[1-(-1)^{n(n-1)/2}n^n]\in \mathbb{Z}\setminus 2\mathbb{Z} & \text{if } n\equiv 5(8),\\ (1/4)[-(-1)^{n(n-1)/2}n^n]\in 2\mathbb{Z} & \text{if } n\equiv 0(2)\end{cases}$$

and

$$v'^*=\begin{cases}(1/4)[-(-1)^{(n+2)(n-1)/2}(n-t)^{n-t}t^t]\in 2\mathbb{Z} & \text{if } n\not\equiv 0(2) \text{ and } 2\notin\{t,n-t\},\\ (1/4)[-(-1)^{(n+2)(n-1)/2}(n-t)^{n-t}t^t]\in \mathbb{Z}\setminus 2\mathbb{Z} & \text{if } n\not\equiv 0(2) \text{ and } 2\in\{t,n-t\},\\ (1/4)[1-(-1)^{(n+2)(n-1)/2}(n-t)^{n-t}t^t]\in 2\mathbb{Z} & \text{if } n\equiv 0(8),\\ (1/4)[1-(-1)^{(n+2)(n-1)/2}(n-t)^{n-t}t^t]\in 2\mathbb{Z} & \text{if } n\equiv 2(8) \text{ and } t\equiv n-t(8),\\ (1/4)[1-(-1)^{(n+2)(n-1)/2}(n-t)^{n-t}t^t]\in 2\mathbb{Z} & \text{if } n\equiv 6(8) \text{ and } t\equiv n-t(8),\\ (1/4)[1-(-1)^{(n+2)(n-1)/2}(n-t)^{n-t}t^t]\in \mathbb{Z}\setminus 2\mathbb{Z} & \text{if } n\equiv 2(8) \text{ and } t\not\equiv n-t(8),\\ (1/4)[1-(-1)^{(n+2)(n-1)/2}(n-t)^{n-t}t^t]\in \mathbb{Z}\setminus 2\mathbb{Z} & \text{if } n\equiv 6(8) \text{ and } 2\not\equiv n-t(8),\\ (1/4)[1-(-1)^{(n+2)(n-1)/2}(n-t)^{n-t}t^t]\in \mathbb{Z}\setminus 2\mathbb{Z} & \text{if } n\equiv 4(8)\end{cases}$$

and hence, by taking F^* for F' in (3.18) to (3.21), we conclude that

$$\text{Num}(f^*)=v^*b_n^{*n-1}+v'^*b_n^{*t-1}b_{n-t}^{*n} \quad \text{with } v^*, v'^*\in\mathbb{Z} \text{ as above.} \tag{3.24}$$

Thus we have the following.

Second proof of (2.27). In view of (3.16) and (3.17), this follows from (3.22) and (3.24).

To give a more general method of computing $\text{Num}(f)$, for every f as in (2.7*), we *define* $f^\bullet(Y)\in K[Y]$ by putting

$$f^\bullet(Y)=Y^2f_Y^\square(Y^2)+Yf_Y^\triangle(Y^2) \tag{3.25}$$

and we note that then

$$f_Y^\square(Y^2)=f_Y(Y)-2f^\bullet(Y) \tag{3.26}$$

where $f_Y(Y), f_Y^\square(Y), f_Y^\triangle(Y)$ are the Y-derivatives of $f(Y), f^\square(Y), f^\triangle(Y)$ respectively. Let T be an indeterminate. Then, say be looking at the determinantal expression of the resultant, we see that $\text{Res}_Y(f(Y), Tf_Y(Y)-f^\bullet(Y))$ is a polynomial of degree $\leqslant n$ in T with coefficients in the ring generated by the coefficients of f over the prime subring of K. So, for $0\leqslant i\leqslant n$, we may introduce the ith *numerator Y-discriminant* of f as an element of the said ring, which we denote by $\text{Num}_Y^{(i)}(f(Y))$ or $\text{Num}_Y^{(i)}(f)$ or $\text{Num}^{(i)}(f)$, and which we *define* by putting

$$\text{Res}_Y(f(Y), Tf_Y(Y)-f^\bullet(Y))=\sum_{i=0}^{n}\text{Num}^{(i)}(f)\,T^{n-i} \tag{3.27}$$

and we note that then there exist unique polynomials $U_0(B)$, $U_1(B)$, ..., $U_n(B)$ in B with coefficients in $\mathbb{Z}$ such that

$$\mathrm{Num}^{(i)}(F)=U_i(C(R)) \quad \text{for } 0\leqslant i\leqslant n \tag{3.28}$$

and for these polynomials we clearly have

$$\mathrm{Num}^{(i)}(f)=U_i(b) \quad \text{for } 0\leqslant i\leqslant n. \tag{3.29}$$

Let

$$\hat{H}(B)=\sum_{i=3}^{n} 2^{i-3}U_i(B)\in\mathbb{Z}[B] \tag{3.30}$$

and for every rational number w let

$$\mathrm{Int}(w)=\text{the largest integer not exceeding } w. \tag{3.31}$$

Now we are ready to prove the following.

(3.32) Second computational principle. *We have*

$$\mathrm{Disc}_Y(f)=\mathrm{Num}^{(0)}(f) \quad \textit{and} \quad -\mathrm{Int}(n/2)\mathrm{Disc}_Y(f)=\mathrm{Num}^{(1)}(f) \tag{3.32.1}$$

and

$$\mathrm{Num}(f)=-\mathrm{Int}(n/4)\mathrm{Disc}_Y(f)+\mathrm{Num}^{(2)}(f)+2\hat{H}(b) \tag{3.32.2}$$

and if the characteristic of K is two and f has no multiple roots then we also have

$$\mathrm{Rat}(f)=\mathrm{Int}(n/4)+[\mathrm{Num}^{(2)}(f)/\mathrm{Disc}_Y(f)]. \tag{3.32.3}$$

To see this, first note that by (3.27) and (3.28) we have

$$\mathrm{Res}_Y(F(Y),\, TF_Y(Y)-F^{\bullet}(Y))=\sum_{i=0}^{n} U_i(C(R))\,T^{n-i} \tag{3.33}$$

which we regard as a polynomial identity in T over $\mathbb{Q}[R]$. Given any $0\neq Q\in\mathbb{Q}$, by substituting $Q^{-1}T$ for T in the above identity we get

$$\mathrm{Res}_Y(F(Y),\, Q^{-1}TF_Y(Y)-F^{\bullet}(Y))=\sum_{i=0}^{n} Q^{i-n}U_i(C(R))\,T^{n-i}.$$

The LHS of the above equation equals $\mathrm{Res}_Y(F(Y),\, Q^{-1}[TF(Y)-QF^{\bullet}(Y)])$ which in turn equals $Q^{-n}\mathrm{Res}_Y(F(Y),\, TF(Y)-QF^{\bullet}(Y))$, and hence by multiplying both sides by Q^n we get

$$\mathrm{Res}_Y(F(Y),\, TF_Y(Y)-QF^{\bullet}(Y))=\sum_{i=0}^{n} Q^{i}U_i(C(R))\,T^{n-i}$$

and now by taking (2, 1) for (Q, T), in view of (3.26), we get

$$\mathrm{Res}_Y(F(Y), F^{\square}(Y)) = \sum_{i=0}^{n} 2^i U_i(C(R))$$

and hence, in view of (3.13) and (3.30), we conclude that

$$4\tilde{V}(C(R)) + W(C(R)) = U_0(C(R)) + 2U_1(C(R)) + 4U_2(C(R)) + 8\hat{H}(C(R)). \quad (3.34)$$

By the expansion of the resultant in terms of roots, we see that the LHS of (3.33) equals the product $\prod_{i=1}^{n}[TF_Y(R_i) - F^{\bullet}(R_i)]$ and, since $\prod_{i=1}^{n} F_Y(R_i) = \mathrm{Disc}_Y(F)$, the said product equals

$$\mathrm{Disc}(F)\left[T^n - \left(\sum_{i=1}^{n} \frac{F^{\bullet}(R_i)}{F_Y(R)}\right) T^{n-1} + \text{terms of degree less than } n-1 \text{ in } T\right]$$

and hence by (3.33) we get

$$\mathrm{Disc}_Y(F) = U_0(C(R)) \quad (3.35)$$

and

$$-\mathrm{Disc}_Y(F) \sum_{i=1}^{n} \frac{F^{\bullet}(R_i)}{F_Y(R_i)} = U_1(C(R)). \quad (3.36)$$

By Lagrange interpolation, i.e., by noting that both sides of the following proposed equation are polynomials of degree less than n in Y and their values coincide for the n distinct values $R_1, R_2, \ldots, R_n$ of Y, we see that

$$F^{\bullet}(Y) = \sum_{i=1}^{n} \frac{F^{\bullet}(R_i) F(Y)}{(Y - R_i) F_Y(R_i)}$$

and, since clearly the coefficient of Y^{n-1} in the LHS equals $\mathrm{Int}(n/2)$ and the coefficient of Y^{n-1} in the RHS equals $\sum_{i=1}^{n} F^{\bullet}(R_i)/F_Y(R_i)$, we conclude that $\mathrm{Int}(n/2) = \sum_{i=1}^{n} F^{\bullet}(R_i)/F_Y(R_i)$ and therefore by (3.36) we get

$$-\mathrm{Int}(n/2)\,\mathrm{Disc}_Y(F) = U_1(C(R)). \quad (3.37)$$

By (3.15) we have $W(C(R)) = (-1)^{n(n-1)/2}\mathrm{Disc}_Y(F)$ and hence by (3.34), (3.35) and (3.37) we conclude that

$$\tilde{V}(C(R)) = -\mathrm{Int}(n/4)\mathrm{Disc}_Y(F) + U_2(C(R)) + 2\hat{H}(C(R)). \quad (3.38)$$

In view of (3.15) and (3.29), upon substituting r for R in (3.35), (3.37) and (3.38), we get (3.32.1) and (3.32.2). In view of (3.16), by (3.32.2) we get (3.32.3).

Returning to t and f^* as in (2.25′) and (2.25*), *upon letting* $v = (n-1)/2$ or $n/2$ according as n is odd or even, and $\tau = (t-1)/2$ according as t is odd or even, we clearly have

$$Tf_Y^*(Y) - f^{**}(Y) = (nT - v)\,Y^{n-1} + (tT - \tau)\,b_{n-t}^* Y^{t-1}$$

and hence by (3.23) and (3.27) we get

$$\sum_{i=0}^{n} \mathrm{Num}^{(i)}(f^*)\,T^{n-i} = (nT-v)^n b_n^{*n-1} + (-1)^{n-1} \times [(n-t)\,T-(v-\tau)]^{n-t}(tT-\tau)^t b_n^{*t-1} b_{n-t}^{*n}.$$

and therefore

$$\mathrm{Num}^{(2)}(f^*) = \hat{v} b_n^{*n-1} + (-1)^{n-1} \hat{v}' b_n^{*t-1} b_{n-t}^{*n} \tag{3.39}$$

where

$$\hat{v} = v^2 n^{n-1}(n-1)/2 \tag{3.40}$$

and

$$\begin{aligned} \hat{v}' = {} & [(n-t)^{n-t}\tau^2 t^{t-1}(t-1)/2] \\ & + [(n-t)^{n-t-1}(v-\tau)(n-t)\tau t^t] \\ & + [(n-t)^{n-t-2}(v-\tau)^2(n-t)(n-t-1)t^t/2]. \end{aligned} \tag{3.41}$$

Thus we have the following.

Third proof of (2.27). In view of (3.17) and (3.32.3), this follows from (3.22) and (3.39) to (3.41).

4. Mod eight criterion

Continuing the notation of Section 2, as another consequence and variation of Jacobson's Criterion, let us now prove the following.

(4.1) Mod eight criterion. *Assume that the characteristic of K is two and f has no multiple roots. Let $\phi: K' \to K$ be a ring homomorphism of a domain K' of characteristic zero into the field K such that $\ker(\phi) = 2K'$ and such that for some $b' = (b'_1, b'_2, \ldots, b'_n)$ with $b'_1, b'_2, \ldots, b'_n$ in K' we have $\phi(b'_i) = b_i$ for $1 \leqslant i \leqslant n$. Now considering the polynomial $f'(Y) = Y^n + \sum_{i=1}^{n} b'_i Y^{n-i}$ we have that:*

(4.1.1) *if* $\mathrm{Disc}_Y^*(f') = x^2 + 8y$ *for some* $x, y \in K'$ *then* $\mathrm{Gal}(f, K) \subset A_n$,

and conversely:

(4.1.2) *if* $\mathrm{Im}(\phi) = K$ *and* $\mathrm{Gal}(f, K) \subset A_n$ *then* $\mathrm{Disc}_Y^*(f') = x^2 + 8y$ *for some* $x, y \in K'$.

Proof. To prove (4.1.1) suppose that $\mathrm{Disc}_Y^*(f') = x^2 + 8y$ for some $x, y \in K'$. Then by applying (2.8) and (2.11) to f' we get

$$U^2(b') - 4V(b') = W(b') = x^2 + 8y.$$

Consequently $\phi(x^2)=\phi(U^2(b'))$, and hence $\phi(x)=\phi(U(b'))$, and therefore $x=U(b')+2h'$ for some $h'\in K'$. Substituting this value of x in the above displayed equation we get

$$U^2(b')-4V(b')=U^2(b')+4h'U(b')+4h'^2+8y$$

and substracting $U^2(b')$ from both sides and then dividing them by 4 we obtain $-V(b')=h'U(b')+h'^2+2y$, and now by applying ϕ to the last equation we get

$$-V(b)=hU(b)+h^2 \quad \text{with } h=\phi(h')\in K.$$

Therefore $-V(b)U^{-2}(b)=z^2+z$ with $z=hU^{-1}(b)\in K$, and hence by (2.12) we get $\mathrm{Gal}(f, K)\subset A_n$.

To prove (4.1.2) assume that $\mathrm{Im}(\phi)=K$ and $\mathrm{Gal}(f, K)\subset A_n$. Now by (2.12) we see that $-V(b)=\phi(x'^2)U^2(b)+\phi(x')U^2(b)$ for some $x'\in K'$. It follows that $-V(b')=x'^2U^2(b')+x'U^2(b')+2y$ for some $y\in K'$. Multiplying both sides by 4 we get $-4V(b')=4x'^2U^2(b')+4x'U^2(b')+8y$. Now by applying (2.8) and (2.11) to f' we get

$$\mathrm{Disc}_Y^*(f')=U^2(b')-4V(b')=U^2(b')+4x'^2U^2(b')+4x'U^2(b')+8y$$

and hence $\mathrm{Disc}_Y^*(f')=x^2+8y$ with $x=U(b')+2x'U(b')\in K'$. □

As an application of (4.1.1), let us give the following.

Fourth proof of (2.27). Note that now t and f^* are as in (2.25′) and (2.25*), and we are assuming that K is a field of characteristic two, f^* has no multiple factors, and $n>2$. Let us start by recalling the well-known fact that given any field K of characteristic 2, there exists a ring epimorphism $\phi: K'\to K$ of a domain K' of characteristic zero with $\mathrm{Ker}(\phi)=2K'$; (although we shall not use the stronger fact that moreover K' can be chosen to be a Henselian discrete valuation ring, for a proof of the weaker and stronger facts see (1.4) of Wadsworth's paper [16]). Now we can take $f'(Y)=Y^n+b'_{n-t}Y^t+b'_n$ with $b'_{n-t}\in\phi^{-1}(b^*_{n-t})$ and $b'_n\in\phi^{-1}(b^*_n)$, and then by applying (2.11) and (2.26) to f' we get

$$\mathrm{Disc}_Y^*(f')=(-1)^{n(n-1)/2}n^nb_n'^{n-1}+(-1)^{(n+2)(n-1)/2}(n-t)^{n-t}t^tb_n'^{t-1}b'^n_{n-t}.$$

Now upon letting

$$g=\begin{cases}0 & \text{if either } n\equiv 1(8) \text{ or } n\equiv 7(8) \text{ or } n\equiv 0(8),\\ 0 & \text{if } t\equiv n-t(8) \text{ and either } n\equiv 2(8) \text{ or } n\equiv 6(8),\\ 1 & \text{if either } n\equiv 3(8) \text{ or } n\equiv 5(8) \text{ or } n\equiv 4(8),\\ 1 & \text{if } t\not\equiv n-t(8) \text{ and either } n\equiv 2(8) \text{ or } n\equiv 6(8)\end{cases}$$

and

$$x'=\begin{cases}b_n'^{(n-1)/2} & \text{if } n\not\equiv 0(2),\\ b_n'^{(t-1)/2}b_{n-t}'^{n/2} & \text{if } n\equiv 0(2)\end{cases}$$

and

$$y^* = \begin{cases} 0 & \text{if } t=2\neq n-t, \\ b_n'^{t-1} b'_{n-t} & \text{if either } t=2 \text{ or } n-t=2 \end{cases}$$

and

$$y' = (1/8)[\mathrm{Disc}^*_Y(f') - (1+4g)x'^2 - 4y^*]$$

we see that $g\in\{0,1\}$ and $x', y^*, y'\in K'$ with $\mathrm{Disc}^*_Y(f') = (1+4g)x'^2 + 4y^* + 8y'$.

As in the statement of (2.27), let us divide the situation into eight cases according as: (i) $2\in\{t, n-t\}$ and either $n\equiv 1(8)$ or $n\equiv 7(8)$, (ii) $2\in\{t, n-t\}$ and either $n\equiv 3(8)$ or $n\equiv 5(8)$, (iii) $t\neq 2\neq n-t$ and either $n\equiv 1(8)$ or $n\equiv 7(8)$, (iv) $t\neq 2\neq n-t$ and either $n\equiv 3(8)$ or $n\equiv 5(8)$, (v) $n\equiv 0(8)$, (vi) $t\equiv n-t(8)$ and either $n\equiv 2(8)$, or $n\equiv 6(8)$, (vii) $n\equiv 4(8)$, and (viii) $t\not\equiv n-t(8)$ and either $n\equiv 2(8)$ or $n\equiv 6(8)$.

Now in cases (iii), (v) and (vi) we have $g=0=y^*$ and hence (2.7) follows from (4.1.2).

In cases (iv), (vii) and (viii), we have $g=1$ and $y^*=0$, and hence assuming $\mathrm{GF}(4)\subset K$, we can find $z', g'\in K'$ such that $z'^2+z'-g=2g'$, and now have $\mathrm{Disc}^*_Y(f') = x^2+8y$ with $x=(2z'+1)x'\in K'$ and $y=y'-g'x'^2\in K'$, and hence again by (4.1.1) we get $\mathrm{Gal}(f^*, K)\subset A_n$. To complete the proof of (2.7) in cases (iv), (vii) and (viii), conversely assuming $\mathrm{Gal}(f^*, K)\subset A_n$, by (4.1.2) we have $\mathrm{Disc}^*_Y(f') = x^2+8y$ for some $x, y\in K'$, and equating the two evaluations of $\mathrm{Disc}^*_Y(f')$ we get $x^2+8y=(1+4)x'^2+8y'$, and hence we must have $x=x'+2l$ for some $l\in K'$, and substituting this value of x in the previous equation we get $x'^2+4lx'+4l^2+8y=(1+4)x'^2+8y'$, and subtracting x'^2 from both sides and then dividing by 4 and afterwords applying ϕ we obtain $\phi(l^2)+\phi(lx')+\phi(x'^2)=0$, and since by the defining equation of x' we clearly have $\phi(x')\neq 0$, we conclude that $z^2+z+1=0$ with $z=\phi(l)\in K$, and hence $\mathrm{GF}(4)\subset K$.

In cases (i) and (ii), assuming $g+b_n^{*t-n}b_{n-t}^{*n} = z^2+z$ for some $z\in K$, multiplying by b_n^{*n-1} we obtain $gb_n^{*n-1}+b_n^{*t-1}b_{n-t}^{*n} = z^2b_n^{*n-1}+zb_n^{*n-1}$ and we can find some $l\in K'$ with $\phi(l)=zb_n^{*(n-1)/2}$, and then we get $gx'^2+y^*=l^2+lx'+2\lambda$ for some $\lambda\in K'$, and now multiplying by 4 and substituting in the equation $\mathrm{Disc}^*_Y(f') = (1+4g)x'^2+4y^*+8y'$ we get $\mathrm{Disc}^*_Y(f') = x^2+8y$ with $x=x'+2l\in K'$ and $y=\lambda+y'\in K'$, and hence by (4.1.1) we conclude that $\mathrm{Gal}(f^*, K)\subset A_n$. Finally, in cases (i) and (ii), conversely assuming $\mathrm{Gal}(f^*, K)\subset A_n$, by (4.1.2) we have $\mathrm{Disc}^*_Y(f') = x^2+8y$ for some $x, y\in K'$, and equating the two evaluations of $\mathrm{Disc}^*_Y(f')$ we get $x^2+8y=(1+4g)x'^2+4y^*+8y'$, and hence we must have $x=x'+2l$ for some $l\in K'$, and substituting this value of x in the previous equation we get $x'^2+4lx'+4l^2+8y=(1+4g)x'^2+4y^*+8y'$, and subtracting x'^2 from both sides and then dividing by 4 and afterwords applying ϕ we obtain $\phi(l^2)+\phi(lx')+\phi(gx'^2)+\phi(y^*)=0$, and since by the defining equation of x' we clearly have $\phi(x')\neq 0$, we conclude that $g+b_n^{*t-n}b_{n-t}^{*n} = z^2+z$ with $z=\phi(l)/\phi(x')\in K$. □

The above proofs suggest yet another variation of Jacobson's Criterion, namely the following.

(4.2) Mod four criterion. *In the notation of* (4.1), *without the condition* $\mathrm{Im}(\phi)=K$, *but assuming that* $\mathrm{Disc}^*_Y(f')=(1+4\zeta)\xi^2+4\eta$ *with* $\zeta, \xi, \eta\in K'$, *we have* $\mathrm{Gal}(f, K)\subset A_n$ *iff* $z^2+\phi(\xi)z+\phi(\zeta\xi^2+\eta)=0$ *for some* $z\in K$.

Proof. Applying (2.8) and (2.11) to f' we get

$$\mathrm{Disc}^*_Y(f')=U^2(b')-4V(b')$$

and hence, because of the assumed equation for $\mathrm{Disc}^*_Y(f')$, we must have $U(b')=\xi+2\theta$ for some $\theta\in K'$, and substituting this value of $U(b')$ in the above displayed equation we get

$$\mathrm{Disc}^*_Y(f')=\xi^2+4\theta\xi+4\theta^2-4V(b')$$

and now equating the RHS of the last equation with the RHS of the assumed equation for $\mathrm{Disc}^*_Y(f')$ and subtracting ξ^2 from both and then dividing everything by 4 we conclude that

$$\theta\xi+\theta^2-V(b')=\zeta\xi^2+\eta.$$

By (2.12) we know that $\mathrm{Gal}(f, K)\subset A_n$ iff $z^{*2}-U(b)z^*+V(b)=0$ for some $z^*\in K$. Now $-U(b)=\phi(U(b'))=\phi(\xi+2\theta)=\phi(\xi)$ and $V(b)=\phi(V(b'))=\phi(\theta\xi+\theta^2)+\phi(\zeta\xi^2+\eta)$, and hence $\mathrm{Gal}(f, K)\subset A_n$ iff $z^{*2}+\phi(\xi)z^*+\phi(\theta\xi+\theta^2)+\phi(\zeta\xi^2+\eta)=0$ for some $z^*\in K$. Upon letting $z=z^*+\phi(\theta)$ we see that: $z^{*2}+\phi(\xi)z^*+\phi(\theta\xi+\theta^2)+\phi(\zeta\xi^2+\eta)=0$ for some $z^*\in K$ iff $z^2+\phi(\xi)z+\phi(\zeta\xi^2+\eta)=0$ for some $z\in K$. □

Finally, as an application of (4.2) here is the following.

Fifth proof of (2.27). In the above Fourth Proof, by taking $(\zeta, \xi, \eta)=(g, x', y^*+2y')$ we get $\mathrm{Disc}^*_Y(f')=(1+4\zeta)\xi^2+4\eta$ with $\zeta, \xi, \eta\in K'$. Now apply (4.2). □

5. Arf invariant of Jacobson's quadratic and discriminants of Berlekamp and Revoy

In Section 2 we considered a monic polynomial $f(Y)=Y^n+\sum_{i=1}^n b_i Y^{n-i}$ of degree n in Y with coefficients $b=(b_1, b_2, \ldots, b_n)$ in a field K, and we defined $U(b)$, $V(b)\in K$. Now we may denote $U(b)$ and $V(b)$ by $\mathrm{Jen}(f)$ and $\mathrm{Jum}(f)$ and call them *Jacobson's denominator Y-discriminant of* f and *Jacobson's numerator Y-discriminant* of f respectively, and if $U(b)\neq 0$ then we may denote $V(b)U^{-2}(b)$ by $\mathrm{Jat}(f)$ and call it *Jacobson's rational Y-discriminant* of f. Moreover, the quadratic polynomial $Z^2-\mathrm{Jen}(f)Z+\mathrm{Jum}(f)$ may be denoted by $J(f)$ and called *Jacobson's quadratic* of f. Assuming f to have no multiple roots, we may thus restate Jacobson's Criterion (2.12) by saying that:

The Galois group of f *over* K *is contained in the alternating group* (*of degree* n) *if Jacobson's quadratic of* f *has a root in* K.

The philosophy behind the criterion is standard in Galois theory. We start with a general polynomial

$$\prod_{i=1}^{n}(Y-R_i).$$

We find a function of the roots $R=(R_1, R_2, \ldots, R_n)$ which is invariant under the action of the alternating group and has exactly two orbits under the action of the symmetric group. If such a function is found, then the condition for the Galois group to be contained in the alternating group is exactly that the function evaluated for the roots of the given polynomial gives an element of the ground field.

In case of Jacobson's criterion, the said function is precisely $D(R)$ and its conjugate is precisely $D^*(R)$ and defined in (2.1). Since this is somewhat difficult to evaluate, or perhaps because people were unaware of it, other functions have been suggested and used which we now describe.

Bertin [11] has the same function as Jacobson's, except it is defined by induction on n and she derives the result that the function $D(R)$ ($I^{(n)}$ in her notation) generates the field of invariants of the alternating group in characteristic two.

Berlekamp [10] used a different function, namely

$$\delta=\sum_{1\leqslant i<j\leqslant n}\frac{R_j}{R_i+R_j}$$

and deduces that δ has conjugate $\delta+1$ in characteristic two. His quadratic equation is then

$$Z^2+Z+\beta=0$$

where

$$\beta=\sum_{1\leqslant i<j\leqslant n}\frac{R_iR_j}{(R_i+R_j)^2}.$$

He observes that there are problems in evaluating β in terms of the polynomial directly and refers to his tricks in his earlier book [9]. His earlier calculations are similar to our resultant criterion and indeed his β is equal to our $\mathrm{Rat}(f)$ in characteristic two. To see this, start with

$$(R_i+R_j)^2=(R_i-R_j)^2+4R_iR_j.$$

Multiply the above over all $1\leqslant i<j\leqslant n$. Then expanding the RHS we have

$$\left[\prod(R_i-R_j)^2\right]+4\left[\prod(R_i-R_j)^2\right]\left[\sum\frac{R_iR_j}{(R_i-R_j)^2}+4(\cdots)\right].$$

Hence, in view of (3.13), we get the desired result in characteristic two.

Revoy [14] gives an explicit formula for β in terms of the elementary symmetric functions of the quantities $R_j/(R_i+R_j)$ where $1\leqslant i<j\leqslant n$. There are no formulas, to compute the symmetric functions in terms of original equation, though.

In case the characteristic of K is two, $\wp(K)$ denotes the additive subgroup of K consisting of all elements of the form z^2+z with $z\in K$, and for a quadratic $g=Z^2+g_1Z+g_2$ with $0\neq g_1\in K$ and $g_2\in K$, following Wadsworth [16], we let $\alpha(g)$ denote the Arf invariant of g as introduced by Arf [8], i.e., $\alpha(g)$ is the image of $g_2g_1^{-2}$ under the residue class homomorphism $\omega: K\to K/\wp(K)$.

Now we may rephrase the characteristic two case of Jacobson's Criterion by saying that:

In case the characteristic of K is two, the Galois group of f over K is contained in the alternating group (of degree n), iff $\alpha(J(f))=0$, i.e., iff the Arf invariant of Jacobson's quadratic of f is zero.

Without any restriction on the characteristic of K, in Section 3 we have introduced the rational Y-discriminant of f and we have denoted it by $\mathrm{Rat}(f)$. Note that in case the characteristic of K is two, we clearly have $\alpha(J(f))=\omega(\mathrm{Jat}(f))=\omega(\mathrm{Rat}(f))$.

In view of Wadsworth's theory ([16]) we may simply say that all these discriminants are the same when viewed as residue classes modulo $\wp(K)$.

To avoid confusion, let us note that Wadsworth refers to a different discriminant introduced by Revoy, which is related to Berlekamp's but is not always equal.

References

[1] S.S. Abhyankar, Coverings of algebraic curves, Amer. J. Math. 79 (1957) 825–856.
[2] S.S. Abhyankar, Group enlargements, C.R. Acad. Sci. Paris 312 (1991) 763–768.
[3] S.S. Abhyankar, Galois theory on the line in nonzero characteristic, Bull. Amer. Math. Soc. 27 (1992) 68–133.
[4] S.S. Abhyankar, Linear disjointness of polynomials, Proc. Amer. Math. Soc. 116 (1992) 7–12.
[5] S.S. Abhyankar, Wreath products and enlargements of groups, Discrete Math. 120 (1993) 1–12.
[6] S.S. Abhyankar, Alternating group coverings of the affine line in characteristic greater than two, Math. Ann. 296 (1993) 63–68.
[7] S.S. Abhyankar and I. Yie, Small degree coverings of the affine line in characteristic two, Discrete Math. 133 (this Vol.) (1994) 1–23.
[8] C. Arf, Untersuchungen über quadratische Formen in Körper der Characteristic 2 (Teil I), Crelle J. 183 (1941) 148–167.
[9] E. Berlekamp, Algebraic Coding Theory (McGraw-Hill, New York, 1968).
[10] E. Berlekamp, An analog to the discriminant over fields of characteristic 2, Algebra 38 (1976) 315–317.
[11] M.-J. Bertin, Anneau des Invariants du Groupe Alterné, Bull. Sc. math. 2e série 94 (1970) 65–72.
[12] N. Jacobson, Lectures in Abstract Algebra, Vol. 3 (Van Nostrand Princeton, NJ, 1964).
[13] N. Jacobson, Basic Algebra, Vol. 1 (Freeman, San Francisco, CA, 1974).
[14] P. Revoy, Anneau des Invariants du Groupe Alterné, Bull. Sc. math. 2e série 106 (1982) 427–431.
[15] J.-P. Serre, Construction de revêtements étales de la droite affine en caractéristique p, C.R. Acad. Sci. Paris 311 (1990) 341–346.
[16] A.R. Wadsworth, Discriminants in characteristic two, Linear and Multilinear Algebra 17 (1985) 235–263.