ARTICLES

Some properties and uses of the discriminant of a polynomial

R. Gow

Let K be a field and let $K[x]$ denote the ring of polynomials over K. Let $f = f(x)$ be a monic polynomial in $K[x]$ of degree $n \geq 1$ and let the roots of f in some splitting field L over K be $\alpha_1, \ldots, \alpha_n$. Put

$$\delta = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j),$$

so that δ is an element of L. Clearly, if f has a repeated root, $\delta = 0$. Otherwise, $\delta \neq 0$ and then $L : K$ is a normal separable extension of finite degree. Recall that the Galois group G of f over K is the group of all automorphisms of L that fix K elementwise. The elements of G permute the roots of f and G may naturally be considered as a subgroup of the symmetric group of degree n. The following basic result is proved in any standard text on Galois theory.

1.1 Lemma. *Let $\sigma \in G$. Consider σ as a permutation on the n roots of f. Then*

$$\sigma(\delta) = \epsilon_\sigma \delta$$

where ϵ_σ is the sign of the permutation determined by σ.

We now set $D = \delta^2$ and call D the *discriminant* of the polynomial f. It follows from Lemma 1.1 that D is fixed by all elements of G and thus, by the Galois correspondence, $D \in K$. Indeed, using the notation just introduced, the following result holds.

1.2 Theorem. *Suppose that K has characteristic different from 2 and let D be the discriminant of f. Let G be the Galois group of f over K.*

(i) If $D = 0$, f has a repeated root.

(ii) If $D \neq 0$ and D has a square root in K, G is naturally a subgroup of A_n, the alternating group of degree n.

(iii) If $D \neq 0$ and D has no square root in K, $G \cap A_n$ has index 2 in G and $K(\sqrt{D})$ is a quadratic extension of K contained in the splitting field of f over K.

It should be clear that the restriction on the characteristic of K is not required for part (i) above. We will discuss substitutes for parts (ii) and (iii) when the characteristic of K is 2 later in the paper.

It is the purpose of this paper to discuss some properties of the discriminant of a polynomial. While the discriminant may seem to be rather a weak invariant, we hope to show how it may be used quite effectively when investigating a number of problems. Our results are drawn from various parts of the literature and contain nothing new.

The discriminant of a polynomial f is expressible as a polynomial in the coefficients of f. However, the number of terms involved tends to be ineffably large. For example, the discriminant of the quartic $x^4 + ax^3 + bx^2 + cx + d$ is

$$256(I^3 - 27J^2)$$

where

$$I = d - \frac{ac}{4} + \frac{b^2}{12}, \quad J = \frac{bd}{6} - \frac{c^2}{16} - \frac{a^2 d}{16} + \frac{abc}{48} - \frac{b^3}{216}.$$

This involves 16 terms. The discriminant of a quintic involves 59 terms. The interested reader should consult the article by J. McKay, [2], to see some explicit formulae and references on this topic.

One of the most useful formulae for calculating the discriminant involves the formal derivative of a polynomial.

1.3 Lemma. *Let $f \in K[x]$ be a monic polynomial of degree $n \geq 1$ and let the roots of f in some splitting field over K be $\alpha_1, \ldots, \alpha_n$. Then the discriminant of f is*

$$(-1)^{n(n-1)/2} \prod_{i=1}^{n} f'(\alpha_i).$$

If we take $f = x^m - 1$, we find from this formula that the discriminant D of f is $(-1)^{\epsilon(m)} m^m$, where $\epsilon(m) = m(m-1)/2 + (m-1)^2$. Taking m equal to an odd prime p, we obtain $D = p^p$ if $p \equiv 1 (\mathrm{mod} 4)$ and $D = -p^p$ if $p \equiv 3 (\mathrm{mod} 4)$. This provides us with a convenient proof of the fact that if ϵ is a primitive p–th root of unity in $\mathbb{C}$, $\sqrt{p} \in \mathbb{Q}(\epsilon)$ if $p \equiv 1 (\mathrm{mod} 4)$ and $\sqrt{-p} \in \mathbb{Q}(\epsilon)$ if $p \equiv 3 (\mathrm{mod} 4)$.

There is a formula, due to R. G. Swan, [4], for the discriminant of a trinomial, that is, a polynomial having only three non–zero terms. Let $f = x^n + ax^k + b$, where $0 < k < n$. The discriminant D of f is given by

$$D = (-1)^{n(n-1)/2} b^{k-1} (n^N b^{N-K} - (-1)^N (n-k)^{N-K} k^K a^N)^d$$

where $d = \gcd(n,k), N = n/d, K = k/d$. This formula is quite useful, as trinomials are frequently employed for various field–theoretic constructions. We remark that when $k = 1$, the result above is easily proved using Lemma 1.3.

As an example of the use of this formula, let $f = x^n + ax + b$, with a and b both non–zero and let D be the discriminant of f. If $n \equiv 1 (\mathrm{mod}\, 4)$, it is not hard to see that D is a non–zero square in K if and only if

$$a = \lambda^2 - n^n \mu^{n-1}, \quad b = (n-1)a\mu,$$

for non–zero elements λ and μ in K. If $n \equiv 3 (\mathrm{mod}\, 4)$, the general solution for square D is

$$a = -\lambda^2 - n^n \mu^{n-1}, \quad b = (n-1)a\mu.$$

Suppose now that n is a prime p with $p \equiv 3 (\mathrm{mod}\, 4)$. Take

$$a = -1 - p^p \mu, \quad b = (p-1)a\mu,$$

where μ is an integer not divisible by p. Then we have

$$f = x^p - (1 + p^p \mu)x - (p-1)(1 + p^p \mu)\mu.$$

As the reduction of f modulo p is well known to be irreducible in $\mathbf{F}_p[x]$, f is irreducible in $\mathbf{Q}[x]$. The classification of finite simple groups now implies that the Galois group of f over $\mathbf{Q}$ is the alternating group A_p for $p > 23$ (and presumably this holds good for $p = 7, 11, 19, 23$). See, for example, Corollary 4.4 of [5]. Perhaps this can be proved purely by field–theoretic methods.

Consider now a polynomial f of degree $n \geq 1$ with real coefficients. Suppose that f has exactly r real roots. The Galois group of f over $\mathbf{R}$ is generated by the complex conjugation involutory mapping, σ, say. In its action on the roots of f, σ is represented by the product of $(n-r)/2$ transpositions and hence the sign of σ is $(-1)^{(n-r)/2}$. Since the discriminant of f is a non–zero square in $\mathbf{R}$ if and only if it is positive, we obtain the following result from Lemma 1.1.

1.4 Theorem. *Let $f \in \mathbf{R}[x]$ have degree n and exactly r real roots. Suppose that the discriminant of f is positive. Then $n \equiv r (\mathrm{mod}\, 4)$.*

The discriminant of a monic integral polynomial has an interesting congruence property modulo 4, as the next result indicates.

1.5 Theorem. *Let $f \in \mathbf{Z}[x]$ be a monic integral polynomial of degree $n \geq 1$. Let D be the discriminant of f. Then $D \equiv 0$ or $1 (\mathrm{mod}\, 4)$.*

Proof. Let the roots of f be $\alpha_1, \ldots, \alpha_n$. As f is monic, the α_i are algebraic integers. Put

$$\Delta = \prod_{1 \leq i < j \leq n} (\alpha_i + \alpha_j).$$

It should be clear that Δ is fixed by all elements of the Galois group of f and hence it is a rational number. However, Δ is also an algebraic integer and thus it is a rational integer. We have now

$$D = \prod \left((\alpha_i + \alpha_j)^2 - 4\alpha_i \alpha_j \right) = \Delta^2 + 4E,$$

where E is an algebraic integer. As E is clearly rational, E is a rational integer. Finally, the square of a rational integer is congruent mod 4 to 0 or 1 and since $D \equiv \Delta^2 (\mathrm{mod}\, 4)$, the result follows.

This result is a special case of a result of Stickelberger, [3], on the discriminant of an algebraic number field.

One of the nicest applications of the discriminant concerns irreducibility questions for polynomials over finite fields. Let q be a power of a prime p and let $\mathbf{F}_q$ denote the finite field of order q. For the sake of simplicity, we first prove a special case of another result of Stickelberger, [3].

1.6 Theorem. *Suppose that q is odd and let f be a polynomial in $\mathbf{F}_q[x]$. If f has even degree ≥ 2 and the discriminant of f is a square in $\mathbf{F}_q$, f is reducible in $\mathbf{F}_q[x]$. If f has odd degree and the discriminant of f is a non– square in $\mathbf{F}_q$, f is also reducible.*

Proof. Suppose that f is irreducible of even degree $2m$. Then it is known from the theory of finite fields that $\mathbf{F}_{q^{2m}}$ is a splitting field for f over $\mathbf{F}_q$ and the Galois group of f is cyclic of order $2m$, being generated by the Frobenius mapping σ that sends a root α to α^q. Thus, as a permutation of the roots, σ is represented by the cycle

$$(\alpha, \sigma(\alpha), \ldots, \sigma^{2m-1}(\alpha)).$$

But it is well known that a cycle of even length has sign -1 and thus we deduce from Theorem 1.2 that the discriminant of f must be a non–square in $\mathbf{F}_q$. Similar reasoning gives the corresponding result when f has odd degree.

Before giving the generalization of this result, we mention an application that is occasionally useful. Let $f \in K[x]$ be a monic polynomial of degree $n \geq 1$ and let $g = f(x^2)$. It is quite straightforward to show that if D and D_1 are the discriminants of f and g, respectively, then

$$D_1 = (-1)^n f(0) 2^{2n} D^2.$$

Now we can prove a simple irreducibility criterion for g when K is a finite field.

1.7 Theorem. *Let $f \in \mathbf{F}_q[x]$ be a monic irreducible polynomial of degree $n \geq 1$ and suppose that q is odd. Let $g = f(x^2)$. Then g is irreducible if and only if $(-1)^n f(0)$ is a non–square in $\mathbf{F}_q$.*

Proof. Suppose that g is irreducible over $\mathbf{F}_q$. As g has even degree it follows from Theorem 1.6 that the discriminant of g must be a non–square in $\mathbf{F}_q$. The formula above for D_1 implies that $(-1)^n f(0)$ is a non–square.

We consider the converse part of the theorem. Given a polynomial h of degree $r \geq 1$, define h^* by

$$h^* = (-1)^r h(-x).$$

It should be clear that $(hh_1)^* = h^* h_1^*$ for polynomials h and h_1 and that $h^{**} = h$. Moreover, suppose that $h = h^*$. Then if r is even, h is a polynomial in x^2, whereas, if r is odd, x divides h and $x^{-1}h$ is a polynomial in x^2. Let h be a monic irreducible factor of g. Then we have $g = hw$ for some polynomial w. As g is a polynomial in x^2, we have $g = g^*$ and thus by our remarks above, $g = h^* w^*$. We see that h^* is a monic irreducible factor of g. Thus we either have $h = h^*$ or else h and h^* are relatively prime, in which case hh^* divides g.

Suppose that $h = h^*$. We can obviously assume that x does not divide f by the irreducibility of f (this only excludes the possibility that $f = x$, for which the result is obvious) and it follows that x does not divide h. We conclude that h is a polynomial in x^2, say $h = a(x^2)$, for some irreducible monic polynomial a. But we see that w above must also be a polynomial in x^2, say $w = b(x^2)$ and thus

$$g = f(x^2) = a(x^2)b(x^2).$$

But this entails a factorization $f = ab$ and it follows that as f is irreducible, $f = a$. Hence g is irreducible in this case.

Suppose now that $h \neq h^*$. Then hh^* divides g and as hh^* is fixed by *, it is a polynomial in x^2, say $hh^* = a(x^2)$. Repeating the argument above we must have $f = a$ and hence $g = hh^*$. We obtain

$$g(0) = f(0) = h(0)h^*(0) = (-1)^n h(0)^2.$$

It follows that if g is reducible, $(-1)^n f(0)$ is a square and thus the converse statement is proved.

We note that the second part of this argument applies to any field of characteristic not equal to 2. Either g is irreducible or else $g = hh^*$ for some monic irreducible polynomial h. If the characteristic of K is 2, we can argue that g is either irreducible or else $g = h^2$ for some irreducible h. This latter condition holds if and only if each coefficient of f is a square in K. The first part of the argument applies only to finite fields.

We now give the generalization of Theorem 1.6, due to Stickelberger.

1.8 Theorem. *Let q be a power of an odd prime and let f be a polynomial of degree $n \geq 1$ in $\mathbf{F}_q[x]$ without repeated roots. Let r be the number of irreducible factors of f in $\mathbf{F}_q[x]$ and let D be the discriminant of f. Then we have $n \equiv r \pmod 2$ if D is a square in $\mathbf{F}_q$ and $n \equiv r + 1 \pmod 2$ if D is a non–square in $\mathbf{F}_q$.*

Proof. Let $f_1, \ldots, f_r$ be the irreducible factors of f in $\mathbf{F}_q[x]$ and let $D_1, \ldots, D_r$ be the discriminants of the f_i. Elementary properties of the discriminant show that $D = D_1 \ldots D_r$ modulo squares in $\mathbf{F}_q$. Let s be the number of irreducible factors of even degree. If D is a square, Theorem 1.6 implies that s must be even. Thus if t is the number of factors of odd degree, $r \equiv t \pmod 2$. But we clearly have $n \equiv t \pmod 2$ and the result follows in this case. The corresponding result when D is a non–square is proved similarly.

There remains the problem of finding an analogue of these results for fields of characteristic 2. We begin by discussing Swan's approach to this problem. For the sake of simplicity, we restrict our attention to the field $\mathbf{F}_2$. Let f be a polynomial in $\mathbf{F}_2[x]$ without repeated roots. We can find a monic polynomial g in $\mathbf{Z}[x]$ such that $\overline{g} = f$, where the bar denotes reduction modulo 2. The discriminant of g is then an odd integer. For the discriminant of f must be 1 in $\mathbf{F}_2$, since f has no repeated roots, and it is easily proved that the discriminant of f is the reduction modulo 2 of that of g (because the discriminants are given

by the same integral polynomial in the coefficients of the polynomials). We now consider g as a polynomial in $\mathbf{Z}_2[x]$, where $\mathbf{Z}_2$ denotes the ring of 2–adic integers. Hensel's Lemma shows that as the discriminant of g is a 2–adic unit, if f has r irreducible factors in $\mathbf{F}_2[x]$, g has r irreducible factors in $\mathbf{Z}_2[x]$ having the same degree as those of f. Furthermore, the splitting field of g over the field of 2–adic numbers is an unramified extension (uniquely determined up to isomorphism by its degree) whose Galois group is cyclic. Thus g has a cyclic Galois group when considered as a 2–adic polynomial. Finally, it is well known that a 2–adic unit u is a 2–adic square if and only if $u \equiv 1(\mathrm{mod}8)$. Thus, the Galois group of g over the 2–adic numbers is contained in A_n if and only if $D \equiv 1(\mathrm{mod}8)$, where D is the discriminant of g, and it follows from Theorem 1.8 that $n - r$ is even if and only if $D \equiv 1(\mathrm{mod}8)$. (Notice that we already know that $D \equiv 1(\mathrm{mod}4)$, by Theorem 1.5.) Taking into account the correspondence discussed above between the factorizations into irreducibles of f and g, we obtain a result of Swan, [4].

1.9 Theorem. *Let $f \in \mathbf{F}_2[x]$ be a polynomial of degree $n \geq 1$ without repeated roots and suppose that f has exactly r irreducible factors in $\mathbf{F}_2[x]$. Let $g \in \mathbf{Z}[x]$ be a monic polynomial such that $\overline{g} = f$. Then $n - r$ is even if and only if $D \equiv 1(\mathrm{mod}8)$, where D is the discriminant of g.*

This result is quite useful, as we are able to obtain a factorization criterion again by means of the discriminant. Swan applied his discriminant formula for trinomials and Theorem 1.9 to obtain information about the factorization of trinomials over $\mathbf{F}_2$. This information was helpful in the compilation of tables of data about such trinomials. See, for example, [1]. It is apparently possible to obtain Theorem 1.9 without the intermediary of the 2–adic numbers but it seems to us that this provides a good conceptual framework. If we replace $\mathbf{F}_2$ by $\mathbf{F}_q$, where q is a power of 2, we must work in the ring of integers of an appropriate unramified extension of the field of 2–adic numbers to obtain an analogue of Theorem 1.9.

Finally, we describe an intrinsic invariant of a polynomial over a field of characteristic 2 that plays the role of the discriminant over fields of characteristic different from 2. Let K be a field of characteristic 2 and let $f \in K[x]$ be a non–constant polynomial of degree n without repeated roots. Let the roots of f be $\alpha_1, \ldots, \alpha_n$ in a splitting field over K. Define $\beta = \beta(f)$ by

$$\beta = \sum_{i<j} \frac{\alpha_i}{\alpha_i + \alpha_j}.$$

Then we find that $\beta + \beta^2 = C$, where

$$C = \sum_{i<j} \frac{\alpha_i \alpha_j}{\alpha_i^2 + \alpha_j^2}.$$

It is found that for a transposition σ permuting the roots, $\sigma(\beta) = \beta + 1$. Thus, β is invariant under A_n but not S_n. The quantity C is invariant under all permutations of the roots and hence lies in K. Moreover, the Galois group of f is contained in A_n if and only if $C = \lambda + \lambda^2$ for some λ in K. If K is the finite field $\mathbf{F}_{2^m}$, C is expressible in the form above if and only if $\mathrm{Tr}(C) = 0$, where Tr is the trace function, defined by

$$\mathrm{Tr}(C) = \sum_{i=0}^{m-1} C^{2^i}.$$

Of course, if $K = \mathbf{F}_2$, C satisfies this condition if and only if $C = 0$. This provides an alternative approach to Theorem 1.9. We could say that C is a second discriminant of f, which is used once we know that the original discriminant of f is non–zero. The introduction of C and discussion of its properties are due to Berlekamp, [1]. We remark that we have not seen any formula for calculating C from, say, the coefficients of f.

References

[1] E. R. Berlekamp, An analog of the discriminant over fields of characteristic two, J. Algebra 38 (1976), 315–317.

[2] J. McKay, On computing discriminants, Amer. Math. Monthly 94 (1987), 523–527.

[3] L. Stickelberger, Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper, Verhandl. Ersten Intern. Math. Kongresses, Zürich 1897, Leipzig 1898, 182–193.

[4] R. G. Swan, Factorization of polynomials over finite fields, Pac. J. Math. 12 (1962), 1099–1106.

[5] W. Feit, Some consequences of the classification of finite simple groups, Proc. Symp. Pure Math. 37 (1980), 175–181.

Department of Mathematics,
University College,
Belfield,
Dublin 4.