Discriminants in Algebra and Arithmetic

Sudhir R. Ghorpade[1]
Department of Mathematics, Indian Institute of Technology, Bombay
Powai, Mumbai 400 076, India.
E-mail: srg@math.iitb.ernet.in

We begin with the familiar notion of the discriminant of a quadratic and discuss how it can be extended to more general situations. We also outline some important applications of the notion of discriminant in Algebra and Arithmetic.

1 Discriminant in High School Algebra

Usually, we first come across discriminants in High School when we study the quadratic equation

$$aX^2 + bX + c = 0. \tag{1}$$

The quantity $\Delta = b^2 - 4ac$ is called the discriminant of (1) and it has the quintessential property:

$$\Delta = 0 \Longleftrightarrow \text{ the equation (1) has a repeated root.} \tag{2}$$

Strictly speaking, (2) holds if (1) is a genuine quadratic, i.e., if $a \neq 0$. Indeed, if $a \neq 0$ and if α, β are the roots of (1), then we have

$$aX^2 + bX + c = a(X - \alpha)(X - \beta) \tag{3}$$

or equivalently

$$\alpha + \beta = \frac{-b}{a} \quad \text{and} \quad \alpha\beta = \frac{c}{a}.$$

Thus from the simple identity $(\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta$, it follows that

$$\Delta = a^2(\alpha - \beta)^2. \tag{4}$$

Note that the above expression makes it obvious that the property (2) holds.

[1]Partially supported by a ‘Career Award’ grant from AICTE, New Delhi and an IRCC grant from IIT Bombay.

We now consider the problem of suitably defining the discriminant of a general equation

$$f(X) = 0$$

where f is a polynomial of degree n, i.e.,

$$f(X) = a_0X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n, \quad \text{with } a_0 \neq 0. \tag{5}$$

Let us assume that f is a nonconstant polynomial, i.e., $n \geq 1$. What should the discriminant of f be? Burnside and Panton (1892) answer this nicely by saying that the *discriminant* ought to be the *simplest function of the coefficients in a rational and integral form, whose vanishing expresses the condition for equal roots.* Let $\alpha_1, \ldots, \alpha_n$ denote the roots[2] of f so that

$$f(X) = a_0(X - \alpha_1) \ldots (X - \alpha_n). \tag{6}$$

As a first guess for the discriminant of f, it seems natural to consider an expression such as

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

This is certainly a simple function whose vanishing expresses the condition for repeated roots. But it isn't really a function of the coefficients, even in the case of a quadratic. So we take a cue from (4), and consider

$$V_f^2 = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Now this is a *symmetric* polynomial function in $\alpha_1, \ldots, \alpha_n$, in the sense that it is unchanged if we permute $\alpha_1, \ldots, \alpha_n$. We have a fundamental result

[2]It may be worthwhile to digress here a bit to discuss the idea of *roots* of a polynomial. If our polynomial $f(X)$ has complex coefficients (in particular, integral, rational or real coefficients), then the Fundamental Theorem of Algebra assures us that it has exactly n roots in $\mathbb{C}$, when counted with multiplicities. Recall that α is said to be a root of *multiplicity* m if $f(X) = (X - \alpha)^m g(X)$ for some polynomial $g(X)$ with $g(\alpha) \neq 0$. In case $m > 1$, we say that α is a *multiple root* or a *repeated root* of f. In general, if A is an integral domain and $f \in A[X]$ (i.e., f is a polynomial in X with coefficients in A), then for any integral domain B containing A as a subring, f has at most n roots in B. Moreover, there exists a field L containing A as a subring such that f has exactly n roots in L when counted with multiplicities. Thus abstractly speaking, by suitably enlarging the domain, if necessary, we can always consider n elements $\alpha_1, \ldots, \alpha_n$ which are the roots of f. Here each root is repeated as many times as its multiplicity.

going back to Newton which says that every symmetric polynomial can be expressed as a polynomial in the ‘elementary symmetric functions’. The *elementary symmetric functions* in $\alpha_1, \ldots, \alpha_n$ are as follows.

$$\begin{aligned} e_1 &= \alpha_1 + \ldots + \alpha_n = \sum_{1 \le i \le n} \alpha_i \\ e_2 &= \alpha_1\alpha_2 + \ldots + \alpha_{n-1}\alpha_n = \sum_{1 \le i < j \le n} \alpha_i\alpha_i \\ &\vdots \\ e_n &= \alpha_1 \ldots \alpha_n. \end{aligned}$$

From (5) and (6), we see that

$$e_1 = \frac{-a_1}{a_0}, \ e_2 = \frac{a_2}{a_0}, \ \ldots, \ e_n = \frac{(-1)^n a_n}{a_0}. \tag{7}$$

Thus it follows from Newton’s Theorem on symmetric functions, that any symmetric polynomial in $\alpha_1, \ldots, \alpha_n$ is a polynomial in $e_1, \ldots, e_n$, and hence it equals a polynomial in the coefficients $a_0, a_1, \ldots, a_n$ divided by some power of a_0. In the case of V_f^2, the degree in α_1 is $2(n-1)$, and since each e_i is of degree 1 in α_1, we see that the degree of V_f^2 in $e_1, \ldots, e_n$ is at most $2(n-1)$. Thus $a_0^{2n-2} V_f^2$ would be a polynomial in $a_0, a_1, \ldots, a_n$ with integral coefficients. We are now ready to make a formal definition.

Definition 1.1 The *discriminant* of f, denoted by $\mathrm{Disc}(f)$, is defined by

$$\mathrm{Disc}(f) = a_0^{2n-2} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2.$$

From the definition of $\mathrm{Disc}(f)$, the following result is evident.

Theorem 1.2 $\mathrm{Disc}(f) = 0 \iff f$ *has a repeated root.* $\square$

Although our definition of $\mathrm{Disc}(f)$ meets all the basic requirements, the situation is still unsatisfactory because for any practical use of the above theorem, we should not have to find the $\mathrm{Disc}(f)$ by first finding the roots of f. In other words, it is highly desirable to have a concrete expression for $\mathrm{Disc}(f)$ purely in terms of the coefficients $a_0, a_1, \ldots, a_n$ of f. This is not so easy (try the case of $n = 3$)! But we can give a nice expression for $\mathrm{Disc}(f)$ if we know the classical notion of resultant. Let us quickly recall some basics concerning resultants. We refer to [21] for more on this topic.

Definition 1.3 Given any two polynomials

$$f(X) = a_0 X^n + \cdots + a_n \quad \text{and} \quad g(X) = b_0 X^m + \cdots + b_m, \tag{8}$$

the *resultant* of $f(X)$ and $g(X)$ is defined to be the $(m+n) \times (m+n)$ determinant

$$\begin{vmatrix} a_0 & a_1 & & \cdots\cdots & & a_n & & & \\ & a_0 & a_1 & \cdots\cdots & & a_{n-1} & a_n & & \\ & & & \cdots\cdots\cdots & \cdots\cdots & & & & \\ & & & & a_0 & a_1 & & \cdots\cdots & a_n \\ b_0 & b_1 & & \cdots\cdots & & b_m & & & \\ & b_0 & b_1 & \cdots\cdots & & b_{m-1} & b_m & & \\ & & & \cdots\cdots\cdots & \cdots\cdots & & & & \\ & & & & b_0 & b_1 & & \cdots\cdots & b_m \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} m \text{ rows} \\ \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} n \text{ rows} \end{matrix}$$

where the blanks before a_0, b_0 and after a_n, b_m are to be filled with zeros. It is denoted by $\mathrm{Res}_X(f, g; n, m)$ or simply by $\mathrm{Res}(f, g)$.

An important fact about resultants is the following.

Theorem 1.4 (Product Formula) *Let $f(X)$ and $\alpha_1, \ldots, \alpha_n$ be as in (5) and (6). Also let $g(X) = b_0 X^m + b_1 X^{m-1} + \ldots + b_m$ be a polynomial in X. Then*

$$\mathrm{Res}(f, g) = a_0^m \prod_{i=1}^{n} g(\alpha_i).$$

Moreover, if $b_0 \neq 0$ and if $\beta_1, \ldots, \beta_n$ are the roots of g so that $g(X) = b_0 \prod_{j=1}^{m} (X - \beta_j)$, then

$$\mathrm{Res}(f, g) = (-1)^{mn} b_0^n \prod_{j=1}^{m} f(\beta_j) = a_0^m b_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j).$$

In particular, $\mathrm{Res}(f, g) = 0$ *if and only if f and g have a common root.*

We are now ready to relate resultants to discriminants and thereby get a concrete formula for $\mathrm{Disc}(f)$ in terms of the coefficients of f.

Theorem 1.5 *Let $f(X) = a_0X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n$ be a non-constant polynomial of degree n. Let $f'(X)$ be the derivative of $f(X)$, i.e., $f'(X) = na_0X^{n-1} + (n-1)a_1X^{n-2} + \ldots + a_{n-1}$. Then*

$$\operatorname{Res}(f, f') \;=\; (-1)^{\frac{n(n-1)}{2}}\, a_0 \operatorname{Disc}(f).$$

Proof: Let $\alpha_1, \ldots, \alpha_n$ be the roots of f. Then we have

$$f(X) \;=\; a_0 \prod_{i=1}^{n}(X - \alpha_i), \quad \text{and therefore} \quad f'(X) \;=\; a_0 \sum_{i=1}^{n} \prod_{\substack{j=1 \\ j\neq i}}^{n}(X - \alpha_j).$$

Hence, using Theorem 1.4, we see that $\operatorname{Res}(f, f')$ equals

$$a_0^{n-1} \prod_{i=1}^{n} f'(\alpha_i) \;=\; a_0^{n-1} \prod_{i=1}^{n} a_0 \prod_{\substack{j=1 \\ j\neq i}}^{n}(\alpha_i - \alpha_j) \;=\; a_0^{2n-1} \prod_{i=1}^{n} \prod_{\substack{j=1 \\ j\neq i}}^{n}(\alpha_i - \alpha_j).$$

Now if in the last product, we collate together the terms of the form $(\alpha_i - \alpha_j)$ and $(\alpha_j - \alpha_i)$ so as to get the corresponding term in the expression for $\operatorname{Disc}(f)$, then the number of sign changes required would be

$$\sum_{1\leq i<j\leq n} 1 \;=\; \sum_{i=1}^{n} \sum_{j=i+1}^{n} 1 \;=\; \sum_{i=1}^{n}(n-i) \;=\; \frac{n(n-1)}{2}.$$

(Alternatively, the number of sign-changes is the number of 2-element subsets $\{\alpha_i, \alpha_j\}_{i<j}$ of the n-element set $\{\alpha_1, \ldots, \alpha_n\}$, and so it is $\binom{n}{2} = \frac{n(n-1)}{2}$.) Therefore, we conclude that

$$\operatorname{Res}(f, f') \;=\; a_0^{2n-1}(-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} \prod_{\substack{j=1 \\ i<j}}^{n}(\alpha_i - \alpha_j)^2 \;=\; (-1)^{\frac{n(n-1)}{2}}\, a_0 \operatorname{Disc}(f). \quad \square$$

Remark. The sign factor $(-1)^{\frac{n(n-1)}{2}}$ in the above result has, curiously, been missed by several mathematicians. For example, this error occurred in the first edition of Lang's *Algebra*. In the second edition [13, p. 211], Lang mentions that Serre has pointed out to him this error and also that it occurs in van der Waerden, Samuel, and Hilbert but not in Weber. Indeed, the error occurs in van der Waerden's *Algebra* [23, p. 82], the original French edition of Samuel's *Algebraic Theory of Numbers* [17, p. 49] although not in its English translation. In the case of Hilbert, one might expect that the reference is to Hilbert's famous *Zahlbericht* (see [8, pp. 63–363] or the recent English translation [9]), but we have not been able to spot any error there. This may be because Hilbert's collected works were revised and corrected by Olga Taussky et al. On the other hand, Weber's *Textbook of Algebra*, written more than a century ago, is quite careful about the sign during the discussion of the discriminant (cf. [24, §50]).

Corollary 1.6 *Let $f(X)$ and $\alpha_1, \ldots, \alpha_n$ be as in (5) and (6). Assume that $f'(X)$ is of degree $n-1$*[3] *and let $\beta_1, \ldots, \beta_{n-1}$ be the roots of $f'(X)$. Then*

$$\mathrm{Disc}(f) = (-1)^{\frac{n(n-1)}{2}} a_0^{n-2} \prod_{i=1}^{n} f'(\alpha_i) = (-1)^{\frac{n(n-1)}{2}} n^n a_0^{n-1} \prod_{j=1}^{n-1} f(\beta_j).$$

Proof: Follows easily from Theorem 1.4 and Theorem 1.5 by noting that $(-1)^{n(n-1)} = 1$. □

Example: Consider a cubic polynomial of the form $f(X) = X^3 + pX + q$. To find $\mathrm{Disc}(f)$, we note that the roots of $f'(X) = 3X^2 + p$ are $\pm(-p/3)^{1/2}$. Therefore, by the second formula in the Corollary above, $\mathrm{Disc}(f)$ equals

$$\begin{aligned}
& (-1)^{\frac{3(2)}{2}} 3^3 \left[(-p/3)^{3/2} + p(-p/3)^{1/2} + q\right] \left[-(-p/3)^{3/2} - p(-p/3)^{1/2} + q\right] \\
= \; & -27 \left[q^2 - \left[(-p/3) + p\right]^2 (-p/3)\right] \\
= \; & -27 \left[q^2 + (4p^2/9)(p/3)\right] \\
= \; & -4p^3 - 27q^2.
\end{aligned}$$

More generally, if $f(X) = X^3 + aX^2 + bX + c$, then using the above method or by directly computing the resultant, it can be seen that

$$\mathrm{Disc}(f) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

We leave it to the reader to verify this formula.

Exercise: Let $f(X)$ and $\alpha_1, \ldots, \alpha_n$ be as in the definition of the Discriminant. Assume that $f(X)$ is monic, i.e., $a_0 = 1$. Prove that $\mathrm{Disc}(f)$ equals

[3] This is always the case if the coefficients are complex numbers or more generally, if n is not divisible by the characteristic.

the square of the Vandermonde determinant $\det\left(\alpha_i^{j-1}\right)$ corresponding to $\alpha_1, \ldots, \alpha_n$. Deduce that $\mathrm{Disc}(f)$ is also given by the determinant of the $n \times n$ matrix whose $(i,j)^{\text{th}}$ entry is the power sum symmetric function p_{i+j-2}. In other words, if for $k \geq 0$, $p_k = \alpha_1^k + \ldots + \alpha_n^k$, then show that

$$\mathrm{Disc}(f) = \begin{vmatrix} 1 & \alpha_1 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \ldots & \alpha_2^{n-1} \\ \vdots & & \ddots & \\ 1 & \alpha_n & \ldots & \alpha_n^{n-1} \end{vmatrix}^2 = \begin{vmatrix} p_0 & p_1 & \ldots & p_{n-1} \\ p_1 & p_2 & \ldots & p_n \\ \vdots & & \ddots & \\ p_{n-1} & p_n & \ldots & p_{2n-2} \end{vmatrix}.$$

2 Discriminant in College Algebra

In the B.Sc. and M.Sc. level courses in Algebra, where one mainly studies groups, rings, fields, etc., the notion of discriminant is encountered once again. Here, at least initially, it appears far removed from the classical or the high school algebra notion of discriminant. We will try to narrow this gap by first recalling the relevant definitions and then describing how the two seemingly different notions of discriminant are related to one another. In what follows, we will assume mild familiarity with the concepts such as rings, fields, vector spaces, and basic facts concerning them. We begin with a brief discussion of the notion of trace, and some of its properties, which are needed later. For proofs of these auxiliary results, one may refer to [6] or standard texts such as [13].

Let K be a field and L be a ring containing K as a subring. Then L is a vector space over K. We will assume that the vector space dimension of L over K is finite and denote it by $[L : K]$. A nice passage from L to K is provided by the *trace* map

$$\mathrm{Tr}_{L/K} : L \to K$$

which is defined as follows. Let $n = [L : K]$. Given any $\alpha \in L$, let t_α denote the linear transformation of $L \to L$ defined by $t_\alpha(x) = \alpha x$ for $x \in L$. Then we define $\mathrm{Tr}_{L/K}(\alpha)$, to be the trace of t_α. In other words, if $\{u_1, \ldots, u_n\}$ is a K-basis of L, and if $t_\alpha(u_j) = \sum_{i=1}^n a_{ij} u_i$ for some $a_{ij} \in K$ $(1 \leq j \leq n)$, then $\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^n a_{ii}$. The latter is easily seen to be independent of the choice of a basis. Some basic properties of the trace map Tr (we often drop the subscript L/K when it is clear from the context) are as follows.

(i) $\mathrm{Tr}_{L/K}$ is a K–linear map, i.e., $\mathrm{Tr}(au+bv) = a\mathrm{Tr}(u) + b\mathrm{Tr}(v)$ for all $a, b \in K$ and $u, v \in L$. Moreover, the restriction of $\mathrm{Tr}_{L/K}$ to K equals $[L:K]$ times the identity map, that is, $\mathrm{Tr}(a) = na$ for $a \in K$.

(ii) Suppose L is a field such that $L = K(\alpha)$ for some $\alpha \in L$.[4] Let $f(X)$ be the *minimal polynomial*[5] of α over K. Assume that $f(X)$ has distinct roots, say $\alpha_1, \ldots, \alpha_n$. Then $\mathrm{Tr}(\alpha) = \alpha_1 + \ldots + \alpha_n$.

Remarks. 1. Suppose L is a field. Then K is a subfield of L and the finiteness of $[L:K] = \dim_K L$ implies that for each $\alpha \in L$, the minimal polynomial of α over K exists.[6] The roots $\alpha_1, \ldots, \alpha_d$ of this minimal polynomial are called the *conjugates* of α over K.

2. Suppose L is a field. If every $u \in L$ has distinct conjugates over K, then we say that L/K is *separable*. It can be shown that if K is any field containing rationals, then L/K is always separable. If L/K is separable (and $\dim_K L$ is finite), then the so called Primitive Element Theorem assures us that there exists some $\alpha \in L$ such that $L = K(\alpha)$; such an element α is called a *primitive element* in L.

3. Suppose L is a field such that L/K is a separable and u is any element of L. If we let d denote the degree of the minimal polynomial of u over K and $u_1, \ldots, u_d$ denote the roots of the minimal polynomial, then $n = de$, where $e = \dim_{K(u)} L$, and the n elements $u^{(1)}, \ldots, u^{(n)}$ obtained by taking each of $u_1, \ldots, u_d$ exactly e times, are called the *conjugates of* u *w.r.t.* L/K. We have $\mathrm{Tr}(u) = u^{(1)} + \ldots + u^{(n)}$.

Example. Consider $L = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. This is a field and a 2-dimensional vector space over $K = \mathbb{Q}$ with $\{1, \sqrt{2}\}$ as a basis. Given any $u = a + b\sqrt{2} \in L$, the matrix of the linear transformation t_u w.r.t. the

[4]By $K(\alpha)$ one denotes the smallest subfield of L containing K and α; it consists of all 'rational functions' $p(\alpha)/q(\alpha)$, where $p(X), q(X) \in K[X]$ with $q(\alpha) \neq 0$.

[5]A monic polynomial (i.e., a polynomial whose leading coefficient is 1) in $K[X]$ satisfied by α and of least possible degree is unique and is called the *minimal polynomial* of α over K. Its degree equals $[K(\alpha):K]$. See [6], [11], [13] or [26] for more on this.

[6]Indeed, since $n = \dim_K L$, the set $\{1, \alpha, \ldots, \alpha^n\}$ of $n+1$ elements must be linearly dependent over K, and thus α satisfies a nonzero polynomial of degree $\leq n$ over K. This, or any nonzero polynomial satisfied by α, can easily be made monic upon dividing by its leading coefficient.

above basis is easily seen to be

$$\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$$

and therefore $\mathrm{Tr}(u) = 2a$. Alternately, u satisfies the polynomial

$$X^2 - 2aX + (a^2 - 2b^2) = \left(X - (a + b\sqrt{2})\right)\left(X - (a - b\sqrt{2})\right)$$

and this is the minimal polynomial of u if $b \neq 0$. Therefore $a+b\sqrt{2},\ a-b\sqrt{2}$ are the conjugates of u w.r.t. L/K and the last equality in the Remark above is verified.

We are now ready to define the notion of discriminant in the set-up of the ring L containing a field K as a subring and such that $\dim_K L = n$ is finite.

Definition 2.1 Given any n elements $u_1, \ldots, u_n \in L$, the *discriminant* $D_{L/K}(u_1, \ldots, u_n)$ of $u_1, \ldots, u_n$ w.r.t. L/K is defined to be the determinant of the $n \times n$ matrix $\left(\mathrm{Tr}_{L/K}(u_i u_j)\right)$.

Note that $D_{L/K}(u_1, \ldots, u_n)$ is an element of K.

Lemma 2.2 *If $u_1, \ldots, u_n \in L$ are such that $D_{L/K}(u_1, \ldots, u_n) \neq 0$, then $\{u_1, \ldots, u_n\}$ is a K–basis of L.*

Proof: It suffices to show that $u_1, \ldots, u_n$ are linearly independent over K. Suppose $\sum_{i=1}^n c_i u_i = 0$ for some $c_1, \ldots, c_n \in K$. Multiplying the equation by u_j and taking the trace, we find that $\sum_{i=1}^n c_i \mathrm{Tr}(u_i u_j) = 0$. By hypothesis, the matrix $\left(\mathrm{Tr}_{L/K}(u_i u_j)\right)$ is nonsingular. Hence it follows that $c_j = 0$ for $j = 1, \ldots, n$. $\square$

Lemma 2.3 *If $\{u_1, \ldots, u_n\}$ and $\{v_1, \ldots, v_n\}$ are two K–bases of L and $u_i = \sum_{j=1}^n a_{ij} v_j,\ \ a_{ij} \in K$, then we have*

$$D_{L/K}(u_1, \ldots, u_n) = [\det(a_{ij})]^2 D_{L/K}(v_1, \ldots, v_n).$$

In particular, since (a_{ij}) is nonsingular, we have

$$D_{L/K}(u_1, \ldots, u_n) = 0 \Longleftrightarrow D_{L/K}(v_1, \ldots, v_n) = 0.$$

Proof: For any $i, j \in \{1, \ldots, n\}$, we have

$$u_i u_j = \left(\sum_{k=1}^{n} a_{ik} v_k \right) u_j = \sum_{k=1}^{n} a_{ik} v_k \left(\sum_{l=1}^{n} a_{jl} v_l \right) = \sum_{k=1}^{n} \sum_{l=1}^{n} a_{ik} a_{jl} v_k v_l.$$

Taking trace of both sides, and letting A denote the matrix (a_{ij}), we see that

$$(\mathrm{Tr}(u_i u_j)) = A^{\mathrm{t}} \, (\mathrm{Tr}(v_i v_j)) \, A$$

and so the result follows. $\square$

Remark: We shall say that the discriminant of L/K is zero (or nonzero) and write $D_{L/K} = 0$ (or $D_{L/K} \neq 0$) if for some K–basis $\{u_1, \ldots, u_n\}$ of L, the quantity $D_{L/K}(u_1, \ldots, u_n)$ is zero (or nonzero). The last lemma justifies this terminology.

We are now ready to describe the link between the two notions of discriminant considered in this and the previous section.

Theorem 2.4 *Suppose L is a field and L/K is a separable. Then the discriminant of L/K is nonzero. In fact, if α is a primitive element (so that $L = K(\alpha)$ and $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a K–basis of L) and $f(X)$ is its minimal polynomial, then we have*

$$D_{L/K}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) \;=\; \prod_{i>j} (\alpha_i - \alpha_j)^2 \;=\; \mathrm{Disc}(f)$$

where $\alpha_1, \alpha_2, \ldots, \alpha_n$ denote the conjugates of α.

Proof: Since L/K is separable, the trace of any element of L equals the sum of its conjugates w.r.t. L/K. Thus if $\{u_1, \ldots, u_n\}$ is a K–basis of L and ${u_i}^{(1)}, {u_i}^{(2)}, \ldots, {u_i}^{(n)}$ denote the conjugates of u_i w.r.t. L/K, then we have $\mathrm{Tr}(u_i u_j) = \sum_{k=1}^{n} u_i^{(k)} u_j^{(k)}$. In other words, the matrix $(\mathrm{Tr}(u_i u_j))$ equals the product of the matrix $\left(u_i^{(j)} \right)$ with its transpose. Therefore

$$D_{L/K}(u_1, \ldots, u_n) \;=\; \begin{vmatrix} u_1^{(1)} & u_1^{(2)} & \ldots & u_1^{(n)} \\ u_2^{(1)} & u_2^{(2)} & \ldots & u_2^{(n)} \\ \vdots & \vdots & \ddots & \vdots \\ u_n^{(1)} & u_n^{(2)} & \ldots & u_n^{(n)} \end{vmatrix}^2 .$$

In case $u_1, u_2, \ldots, u_n$ are $1, \alpha, \ldots, \alpha^{(n-1)}$ respectively, then the determinant above is a Vandermonde determinant and the RHS becomes

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ {\alpha_1}^{n-1} & {\alpha_2}^{n-1} & \ldots & {\alpha_n}^{n-1} \end{vmatrix}^2 = \prod_{i>j} (\alpha_i - \alpha_j)^2 = \prod_{i<j} (\alpha_i - \alpha_j)^2 .$$

Therefore, we obtain the desired formulae. Our first assertion follows from the fact that if $L = K(\alpha)$ is separable over K, then the conjugates $\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}$ of α w.r.t. L/K are distinct. □

Remark: The converse of the above Theorem, viz., if $D_{L/K} \neq 0$ then L/K is separable, is also true. For a proof, see [26].

3 Discriminant in Arithmetic

In Arithmetic, which we start learning even before entering high school, we mainly deal with numbers and their divisibility properties. A basic result is the

Fundamental Theorem of Arithmetic *Every nonzero integer can be factored as* ± 1 *times a finite product of prime numbers. Moreover, this decomposition is unique up to rearrangement of terms.*

In higher arithmetic, we are interested in knowing if such a result holds in domains more general than $\mathbb{Z}$, the ring of integers. An example of such a domain is

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

This is a subring of $\mathbb{C}$, and is called the ring of *Gaussian integers.* Here i is the usual complex number whose square is -1. The notion of divisibility is easily defined in $\mathbb{Z}[i]$ or for that matter, in any ring.

Given a ring[7] A and elements $a, b \in A$, we say that b *divides* a, and write $b|a$, if $a = bc$ for some $c \in A$.

The analogue of a prime number is the so called irreducible element.

[7] By a ring we shall always mean a commutative ring with identity.

An element p in a ring A is said to be *irreducible* if $p \neq 0$, p is not a unit[8], and whenever $p = bc$ for some $b, c \in A$, either b is a unit or c is a unit.

For example, 5 is irreducible in $\mathbb{Z}$ but not in $\mathbb{Z}[i]$ since it decomposes as $5 = (2+i)(2-i)$. Further, the factors $2+i$ and $2-i$ can be shown to be irreducible elements which are distinct; in fact, they do not even differ by a unit. On the other hand, 3 remains prime in $\mathbb{Z}[i]$. Indeed, if $u = a+bi$ and $v = c+di$ are elements of $\mathbb{Z}[i]$ such that $3 = uv$, then by taking modulus (as complex numbers) and squaring, we have $9 = (a^2+b^2)(c^2+d^2)$. But the square of an integer is always $\equiv 0$ or $1 \pmod 4$, and so the sum of two squares is never $\equiv 3 \pmod 4$. Hence $a^2+b^2 = 1$ or $c^2+d^2 = 1$. This implies that either u or v is in $\{1, -1, i, -i\}$, i.e., either u is a unit or v is a unit. The prime 2 of $\mathbb{Z}$ is special. It splits in $\mathbb{Z}[i]$ as $2 = (1+i)(1-i)$ and the factors $1 \pm i$ are irreducible, but they aren't really distinct because they differ simply by a unit [indeed, $1+i = i(1-i)$ and so $2 = i(1-i)^2$]. In general, a prime number p, when extended to $\mathbb{Z}[i]$

$$\begin{cases} \text{splits as a product of two distinct irreducibles} & \text{if } p \equiv 1 (\text{mod } 4) \\ \text{remains irreducible} & \text{if } p \equiv 3 (\text{mod } 4) \\ \text{equals unit times the square of an irreducible} & \text{if } p = 2. \end{cases}$$

Incidentally, for $p \equiv 1 (\text{mod } 4)$, the two irreducible factors in $\mathbb{Z}[i]$ must be (complex) conjugates of each other (prove!), and thus the result about the decomposition of such primes in $\mathbb{Z}[i]$ is equivalent to Fermat's Two Squares Theorem (viz., primes $\equiv 1 (\text{mod } 4)$ are sums of two squares).

The ring $\mathbb{Z}[i]$ is an example of the ring of algebraic integers (in a number field). The latter are defined as follows. A subfield K of $\mathbb{C}$, which is finite dimensional as a vector space over $\mathbb{Q}$ is called an *algebraic number field* or simply a *number field*. We call $\dim_{\mathbb{Q}} K$ the *degree* of $K/\mathbb{Q}$ and denote it by $[K : \mathbb{Q}]$. If K is a number field, then every element of K satisfies a nonzero polynomial with integer coefficients (check!). Those elements of K which satisfy a monic polynomial with integer coefficients are called (*algebraic*) *integers* in K. The set of all algebraic integers in K form a subring of K, called the ring of integers of K and denoted by $\mathcal{O}_K$.

Exercises. Let K be a number field of degree n and $\mathcal{O}_K$ be its ring of integers.

[8]Units in a ring A are defined to be the elements which divide 1. For example, 1, -1 are the only units in $\mathbb{Z}$.

1. Show that given any $u \in K$, there exists $d \in \mathbb{Z}$ such that $d \neq 0$ and $du \in \mathcal{O}_K$. Deduce that the quotient field of $\mathcal{O}_K$ is K and moreover, there exist a $\mathbb{Q}$-basis $\{u_1, \ldots, u_n\}$ of K such that $u_i \in \mathcal{O}_K$ for all $i = 1, \ldots, n$.

2. Show that $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. In other words, if a rational number satisfies a monic polynomial with integer coefficients, then it must be an integer.

If $\{u_1, \ldots, u_n\}$ is a $\mathbb{Q}$-basis of K such that $\{u_1, \ldots, u_n\} \subseteq \mathcal{O}_K$, then from Exercise 2 above, we see that $D_{K/\mathbb{Q}}(u_1, \ldots, u_n)$ is an integer. Moreover, by Theorem 2.4, it is a nonzero integer.

Lemma 3.1 *Let $\{u_1, \ldots, u_n\} \subseteq \mathcal{O}_K$ be a $\mathbb{Q}$-basis of K with the property that $|D_{K/\mathbb{Q}}(u_1, \ldots, u_n)|$ is minimal. Then $\mathcal{O}_K = \mathbb{Z}u_1 + \ldots + \mathbb{Z}u_n$, i.e., $u \in \mathcal{O}_K$ if and only if $u = c_1u_1 + \ldots + c_nu_n$ for some $c_1, \ldots, c_n \in \mathbb{Z}$.*

Proof: It is clear that $\mathbb{Z}u_1 + \ldots + \mathbb{Z}u_n \subseteq \mathcal{O}_K$. If $u \in \mathcal{O}_K$, then we can write $u = r_1u_1 + \ldots + r_nu_n$ for some $r_1, \ldots, r_n \in \mathbb{Q}$. If $r_k \notin \mathbb{Z}$ for some k $(1 \leq k \leq n)$, then $r_k = m_k + \lambda$, where $m_k \in \mathbb{Z}$ and λ is a rational number with $0 < \lambda < 1$. Define $v_1, \ldots, v_n$ by $v_j = u_j$ if $j \neq k$ and $v_k = u - m_ku_k$. Then it is clear that $\{v_1, \ldots, v_n\} \subseteq \mathcal{O}_K$ and $\{v_1, \ldots, v_n\}$ is a $\mathbb{Q}$-basis of K. Moreover the matrix (a_{ij}) of rationals for which $v_i = \sum_{j=1}^n a_{ij}u_j$ for $i = 1, \ldots, n$, is the identity matrix except for the k–th row, which is given by $(r_1, \ldots, r_{k-1}, \lambda, r_{k+1}, \ldots, r_n)$. Thus in view of Lemma 2.3, we see that

$$D_{K/\mathbb{Q}}(v_1, \ldots, v_n) = [\det(a_{ij})]^2 D_{K/\mathbb{Q}}(u_1, \ldots, u_n) = \lambda^2 D_{K/\mathbb{Q}}(u_1, \ldots, u_n).$$

Since $\lambda < 1$, the minimality of $|D_{K/\mathbb{Q}}(u_1, \ldots, u_n)|$ is contradicted. This proves the lemma. $\square$

Definition 3.2 A $\mathbb{Q}$-basis $u_1, \ldots, u_n$ of a number field K such that $\mathcal{O}_K = \mathbb{Z}u_1 + \ldots + \mathbb{Z}u_n$ is called an *integral basis* of K.

The above Lemma shows that every number field has an integral basis. Also, it is clear that if $\{u_1, \ldots, u_n\}$ and $\{v_1, \ldots, v_n\}$ are any two integral bases of K, then $v_i = \sum_{j=1}^n a_{ij}u_j$ for $j = 1, \ldots, n$, for some $n \times n$ matrix (a_{ij}) with integral entries. Moreover the inverse of (a_{ij}) is also a matrix with integral entries. Therefore, $\det(a_{ij}) = \pm 1$. Hence from Lemma 2.3, it follows that any two integral bases of K have the same discriminant; it is called the *(absolute) discriminant of* K and is denoted by d_K.

The following example illustrates the computation of discriminant and determination of integral bases.

Example: Let K be a quadratic field [that is, a subfield of $\mathbb{C}$ such that $[K : \mathbb{Q}] = 2$] and $\mathcal{O}$ be its ring of integers. If α is any element of K which is not in $\mathbb{Q}$, then $1 < [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq [K : \mathbb{Q}] = 2$, and hence $K = \mathbb{Q}(\alpha)$. Moreover, α satisfies a quadratic polynomial with integer coefficients, and thus $\alpha = a + b\sqrt{\Delta}$ for some $a, b \in \mathbb{Q}$ and $\Delta \in \mathbb{Z}$. Since $\alpha \notin \mathbb{Q}$, we must have $b \neq 0$ and Δ not a square. It follows that $K = \mathbb{Q}\left(\sqrt{\Delta}\right)$. Removing the extraneous square factors from Δ, if any, we can write $K = \mathbb{Q}(\sqrt{m})$, where m is a squarefree integer. We now attempt to give a more concrete description of $\mathcal{O}$. First, note that $\mathbb{Z}[\sqrt{m}] = \{r + s\sqrt{m} : r, s \in \mathbb{Z}\} \subseteq \mathcal{O}$. Let $x = a + b\sqrt{m} \in \mathcal{O}$ for some $a, b \in \mathbb{Q}$. Then the other conjugate $a - b\sqrt{m}$ of x must also be in $\mathcal{O}$. Therefore the sum of these two, i.e., $\mathrm{Tr}(x) = 2a$ and the product $a^2 - mb^2$ are both in $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. Since m is squarefree and $a^2 - mb^2 \in \mathbb{Z}$, we see that $a \in \mathbb{Z}$ if and only if $b \in \mathbb{Z}$. Thus if $a \notin \mathbb{Z}$, then we can find an odd integer a_1 such that $2a = a_1$, and relatively prime integers b_1 and c_1 with $c_1 > 1$ such that $b = \frac{b_1}{c_1}$. Now

$$\left(a_1 = 2a \in \mathbb{Z} \text{ and } a^2 - mb^2 \in \mathbb{Z}\right) \Rightarrow \left(4|c_1^2 a_1^2 \text{ and } c_1^2|4mb_1^2\right) \Rightarrow c_1 = 2.$$

Hence b_1 is odd and $a_1^2 - mb_1^2 \equiv 0 (\mathrm{mod}\ 4)$. Also a_1 is odd, and therefore, $m \equiv 1 (\mathrm{mod}\ 4)$. It follows that if $m \not\equiv 1 (\mathrm{mod}\ 4)$, then $a, b \in \mathbb{Z}$, and so in this case,

$$\mathcal{O} = \mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\} \text{ and } \{1, \sqrt{m}\} \text{ is an integral basis.}$$

In the case $m \equiv 1 (\mathrm{mod}\ 4)$, the preceding observations imply that

$$\mathcal{O} \subseteq \left\{\frac{a_1 + b_1\sqrt{m}}{2} : a_1, b_1 \in \mathbb{Z} \text{ with } a_1 \equiv b_1 (\mathrm{mod}\ 2)\right\}$$

and, moreover, $\frac{1+\sqrt{m}}{2} \in \mathcal{O}$ since it is a root of $X^2 - X - \frac{m-1}{4}$; therefore

$$\mathcal{O} = \mathbb{Z}[\frac{1 + \sqrt{m}}{2}] = \{\frac{a + b\sqrt{m}}{2} : a, b \in \mathbb{Z} \text{ with } a \equiv b (\mathrm{mod}\ 2)\}$$

and consequently,

$$\{1, \frac{1 + \sqrt{m}}{2}\} \text{ is an integral basis.}$$

We can now compute the discriminant of K as follows.

$$d_K = \begin{cases} \det\begin{pmatrix} 2 & 0 \\ 0 & 2m \end{pmatrix} & = \ 4m \qquad \text{if } m \equiv 2, 3 (\bmod 4) \\ \det\begin{pmatrix} 2 & 1 \\ 1 & (1+m)/2 \end{pmatrix} & = \ m \qquad \text{if } m \equiv 1 (\bmod 4). \end{cases}$$

It may be remarked that the integer $d = d_K$ determines the quadratic field K completely, and the set $\{1, \frac{d+\sqrt{d}}{2}\}$ is always an integral basis of K. (Verify!)

In general, the unique factorization property is not true in the ring of integers of a number field; in other words, the Fundamental Theorem of Arithmetic may not hold there. For example, if $K = \mathbb{Q}(\sqrt{-5})$, then from the example above, we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, and for the number 6, we have two different factorizations:

$$6 = 3 \cdot 2 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

It is not difficult to see that the factors $2, 3, 1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are irreducible and genuinely distinct (i.e., no two differ by a unit) in $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Around 1844, the German mathematician E. Kummer was studying arithmetic in the ring $\mathbb{Z}[\zeta]$ of cyclotomic integers[9] while trying to prove Fermat's Last Theorem[10]. Kummer realised that the unique factorization may not always hold in rings of cyclotomic integers. Instead of giving up the problem, he continued to delve deeper and made a remarkable discovery! He showed that the unique factorization property can be salvaged if we replace numbers by what he called ideal numbers. Another German mathematician R. Dedekind simplified and extended Kummer's work by using

[9] If $\zeta = \zeta_n$ is a primitive n–th root of unity (e.g., $\zeta = e^{2\pi i/n} = \cos(2\pi/n) + i\sin(2\pi/n)$), then $\mathbb{Q}(\zeta)$ is a number field, called a *cyclotomic field* and its ring of integers is $\mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + \ldots + a_{n-1}\zeta^{n-1} : a_0, a_1, \ldots, a_n \in \mathbb{Z}\}$, which is called the ring of cyclotomic integers.

[10] Fermat's Last Theorem (FLT) is the famous assertion of P. Fermat that the equation $x^n + y^n = z^n$ has no solution in nonzero integers, if $n \geq 3$. It is natural to consider the ring of cyclotomic integers here because the existence of a solution (x, y, z) yields a factorization $x^n = (y - z)(y - \zeta z) \ldots (y - \zeta^{n-1} z)$ in $\mathbb{Z}[\zeta]$ and to proceed further, it would be useful to know if the unique factorization property is valid in $\mathbb{Z}[\zeta]$. In a sense, Kummer didn't succeed in proving FLT (though he settled it for several values of n) because of the failure of unique factorization in $\mathbb{Z}[\zeta]$. Recently, in 1994, FLT has been proved by A. Wiles partly in collaboration with R. Taylor.

ideals in place of ideal numbers.[11] Dedekind's results were first published in 1871.[12] In effect, Dedekind showed that if K is a number field, then every nonzero ideal of $\mathcal{O}_K$ factors as a finite product of prime ideals, and this factorization is unique up to rearrangement of terms. Integral domains with this property are now known as *Dedekind domains.*

At any rate, if K is a number field and p is a prime number, then, thanks to the abovementioned result of Kummer-Dedekind-Kronecker, the extended ideal $p\mathcal{O}_K$ can be factored uniquely as

$$p\mathcal{O}_K = P_1^{e_1} P_2^{e_2} \cdots P_h^{e_h}$$

where $P_1, \ldots, P_h$ are distinct prime ideals of $\mathcal{O}_K$ and $e_1, \ldots, e_h$ are positive integers. The prime p is said to be *ramified* in K if $e_i > 1$ for some i.

Example: If $K = \mathbb{Q}(i)$, then 2 is the only ramified prime.

In general, to understand the phenomenon of ramification, the discriminant is an indispensable tool. This may be clear from the following basic result.

Theorem 3.3 (Dedekind's Discriminant Theorem) *Let K be a number field and d_K be its discriminant. Then for any prime number p, we have*

$$p \textit{ is ramified in } K \Longleftrightarrow p | d_K.$$

Example: If $K = \mathbb{Q}(\sqrt{m})$, where m is a squarefree integer, then we have calculated the discriminant d_K of K. Thus, for any prime number p, we have:

$$p \text{ is ramified in } K \Longleftrightarrow \begin{cases} p|m & \text{if } m \equiv 1 (\text{mod } 4) \\ p|m \text{ or } p = 2 & \text{if } m \not\equiv 1 (\text{mod } 4). \end{cases}$$

[11] In fact, the concept of an ideal of a ring was thus born in the work of Kummer and Dedekind. Note that these historical origins justify the nomenclature "ideal", which may otherwise seem obscure. Indeed, by considering ideals, the ideal situation (of unique factorization) is restored!

[12] Incidentally, another approach towards understanding and extending Kummer's work was developed by his student L. Kronecker, whose work was apparently completed in 1859 but was not published until 1882.

In the case of the cyclotomic field $K = \mathbb{Q}(\zeta_n)$, where n is any integer > 2 and ζ_n is a primitive n–the root of unity, the discriminant turns out[13] to be

$$d_K = (-1)^{\varphi(n)/2} \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}$$

where the product in the denominator is over all prime numbers dividing n, and $\varphi(n)$ denotes the number of positive integers $\leq n$ and relatively prime to n. Therefore,

$$p \text{ is ramified in } \mathbb{Q}(\zeta_n) \Longleftrightarrow p|n.$$

Remarks. 1. For a proof of Dedekind's discriminant Theorem, see [7] or the books of Lang [14] or Serre [19].
2. The notions of discriminant and resultant are no doubt classical and date back more than a century. However, extensions and generalisations (to 'higher dimensions') of these notions are of much current interest. For an introduction, see the expository article [22] by Sturmfels and the references therein. At a more advanced level, there is a book [5] by Gelfand, Kapranov and Zelevinsky, and the recently published review [3] by Catanese may be a good starting point for this.
3. It may be remarked that the phenomenon of ramification or rather the absence of ramification, is closely related to certain basic notions in Topology. Briefly speaking, unramified field extensions (i.e., extensions for which no prime 'below' is ramified 'above') correspond to (topological or unbranched) coverings. Thus, saying that a field has no unramified extensions, is analogous to the condition that the corresponding topological space is simply connected. Unfortunately, in the compartmentalized courses at College and University level, such analogies are rarely highlighted. Thus we might take this opportunity to mention the following brief and rough dictionary of some basic concepts from Algebra and Topology.

$$\text{Algebraic Field Extensions} \longleftrightarrow \text{Branched Coverings;}$$
$$\text{Galois extensions} \longleftrightarrow \text{Regular Coverings;}$$
$$\text{Galois Groups} \longleftrightarrow \text{Groups of Deck transformations.}$$

For more on Coverings Spaces in particular, and Topology, in general, we recommend the classic text of Seifert and Threlfall [18] or the more recent

[13] For a proof of the discriminant formula for cyclotomic fields, one may refer to [25].

book of Massey [15]. The first appendix in [16] also gives a nice and quick summary of the basics of covering spaces.
4. It is a nontrivial result of Minkowski that for any number field K other than $\mathbb{Q}$, we have $|d_K| > 1$. This means that there exists at least one prime number p which is ramified in K. Thus, we might say that $\mathbb{Q}$ is simply connected! Analogous result holds when $\mathbb{Q}$ is replaced by the field $\mathbb{C}(X)$ of rational functions in one variable with complex coefficients. This time, the topological analogue is the more familiar result that the Riemann sphere or the extended complex plane is simply connected.

5. The study of ramification (and hence of discriminants) is of basic importance in some advanced developments in Algebraic Number Theory, which go under the name of Class Field Theory. This is a fascinating topic, and to learn more about it, see [2] or [14]. It may also be worthwhile and interesting to see Hilbert's *Zahlbericht*, which was meant as a report to the German Mathematical Society on the status of Algebraic Number Theory in 1895. This report contained several original contributions by Hilbert and perhaps started the subject of Class Field Theory. The *Zahlbericht* is now available in English [9].

6. The relation with ramification is perhaps the most important application of discriminant in Number Theory. However, the classical discriminant $\Delta = b^2 - 4ac$ of a quadratic also comes up in the following important and classical question.

Given an integer Δ, what are the possible binary quadratic forms $ax^2 + bxy + cy^2$ with integer coefficients a, b, c, for which $\Delta = b^2 - 4ac$? Can we classify them?

This was studied by Legendre and Gauss, and the notions of class number and genera were developed by Gauss for classifying binary quadratic forms with a given discriminant. For an exposition of the basics of this theory, one may consult the texts of Baker [1] or Flath [4]. For a beautiful introduction to some modern developments motivated by this problem, we refer to Serre's Singapore lecture [20].

7. The discriminant also makes an unexpected appearance in questions related to the generalization of the so called Waring's problem. For example, it is shown in [12] that if K is a number field and n, k are integers with $n \geq k \geq 2$, then every $n \times n$ matrix over $\mathcal{O}_K$ is a sum of k-th powers of matrices over $\mathcal{O}_K$ if and only if the discriminant d_K of K is coprime to k. Moreover, when this condition is met, seven powers always suffice.

Acknowledgments

This article is an expanded version of a lecture delivered at S. P. College, Pune on February 19, 2000. This formed a sequel to a lecture by Prof. Balwant Singh on Resultants (cf. [21]). The author would like to thank the S. P. College for its invitation, and also thank Prof. S. A. Katre for a number of useful suggestions on a preliminary version of this article.

References

[1] A. Baker, A Concise Introduction to the Theory of Numbers, Cambridge University Press, 1984.

[2] J. W. S. Cassels and A. Fröhlich (eds.), Algebraic Number Theory, Academic Press, 1967.

[3] F. Catanese, Review of [5], *Bull. Amer. Math. Soc.*, Vol. 37 (2000), 183–198.

[4] D. E. Flath, Introduction to Number Theory, John Wiley & Sons, 1989.

[5] I. M. Gelfand, M. M. Kapranov and A. V. Zelevinsky, Discriminants, Resultants and Multidimensional Determinants, Birkhäuser, 1994.

[6] S. R. Ghorpade, Notes on Galois Theory, IIT Bombay, Oct. 1994.

[7] S. R. Ghorpade, Field Theory and Ramification Theory, Instructional School on Algebraic Number Theory, Bombay Univ., Dec. 1994.

The lecture notes [6] and [7] are unpublished but can be downloaded from: `http://www.math.iitb.ernet.in/~srg/Lecnotes.html`

[8] D. Hilbert, Gesammelte Abhandlungen, Band I: Zahlentheorie, 2nd Ed., Springer– Verlag, 1970.

[9] D. Hilbert, The Theory of Algebraic Number Fields, Springer-Verlag, 1998.

[10] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, Springer–Verlag, 1982.

[11] N. Jacobson, Basic Algebra I, 2nd Ed., W. H. Freeman, 1985.

[12] S. A. Katre and S. A. Khule, Matrices over orders in algebraic number fields as sums of k-th powers, *Proc. Amer. Math. Soc.*, Vol. 128, No. 3 (2000), 671–675.

[13] S. Lang, Algebra, 2nd ed., Addison-Wesley, 1984.

[14] S. Lang, Algebraic Number Theory, Springer–Verlag, 1986.

[15] W. S. Massey, A Basic Course in Algebraic Topology, Springer-Verlag, 1991.

[16] D. Rolfsen, Knots and Links, Publish or Perish Inc., 1990.

[17] P. Samuel, Theorie Algebrique des Nombres, Hermann, 1967. [An English translation was published by Houghton Miffin in 1970, while a corrected French edition was published by Hermann in 1971.]

[18] H. Seifert and W. Threlfall, A Textbook of Algebraic Topology, Academic Press, 1980.

[19] J.-P. Serre, Local Fields, Springer–Verlag, 1979.

[20] J.-P. Serre, $\Delta = b^2 - 4ac$, *Math. Medley*, Singapore Math. Society, Vol. 13 (1985), 1–13. (See also: Œuvres, Collected Papers, Vol. IV: 1985–1998, Springer–Verlag, 2000; or the appendix of [4].)

[21] B. Singh, Resultants, *Bona Mathematica*, Vol. 11, No. 1 (2000), 11–21.

[22] B. Sturmfels, Introduction to resultants, Proc. Symp. Appl. Math., Vol. 53, pp. 25–39, American Math. Society, 1998.

[23] B. L. van der Waerden, Algebra, Vol. 1, F. Ungar, 1949. [Reprinted by Springer-Verlag in 1991.]

[24] H. Weber, Lehrbuch der Algebra, Band I, Viehweg, 1895.

[25] L. C. Washington, Introduction to Cyclotomic Fields, Springer–Verlag, 1982. [Second Ed., Springer-Verlag, 1997.]

[26] O. Zariski and P. Samuel, Commutative Algebra, Vol. 1, D. Van Nostrand, 1958. [Reprinted by Springer–Verlag in 1975.]