Determining the Discriminant

Fernando Q. Gouvêa and Jonathan Webster

Two "discriminants":

1. discriminant of a polynomial
2. discriminant of an algebraic number field

We are primarily interested in the latter one, but there are interesting things to say about the other and about how the two notions are connected. That is the focus of this talk.

Dedekind and Algebraic Number Theory

> The Tenth Supplement, which first appeared in the second edition of 1871, created, at a single hammer-blow, modern algebraic number theory...

(William Ewald, *From Kant to Hilbert*, vol II, p. 762.)

Perhaps we can find a little more about the process behind that hammer-blow.

The discriminant of a polynomial

Let

$$f(x) = (x - r_1)(x - r_2)\dots(x - r_n)$$

$$= x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n.$$

The *discriminant* of f is

$$\operatorname{disc}(f) = \prod_{i<j} (r_i - r_j)^2.$$

(If $f(x)$ is not monic, multiply by the $(2n-2)$th power of the leading coefficient.)

Some authors define $\operatorname{disc}(f) = \prod_{i \neq j} (r_i - r_j)$, which differs by a sign.

Since permuting the roots does not change $\mathrm{disc}(f)$, it is possible to express it as a polynomial in the elementary symmetric functions s_i.

So we really want to think of $\mathrm{disc}(f)$ as the polynomial in $s_1, s_2, \ldots, s_n$ which equals (one of) the product(s) above.

For example, suppose $f(x) = x^2 + bx + c$. Then we know the roots are

$$r_1 = \frac{-b + \sqrt{b^2 - 4c}}{2} \qquad r_2 = \frac{-b - \sqrt{b^2 - 4c}}{2}$$

so

$$r_1 - r_2 = \sqrt{b^2 - 4c}$$

and

$$\text{disc}(f) = b^2 - 4c.$$

This quantity appears, without a name, in several bits of 18th century mathematics.

For example, Lagrange looked at the polynomial whose roots are $(r_i - r_j)^2$ to study the number of "imaginary" roots of a polynomial. The independent term of that polynomial is the discriminant.

Several similar examples, but nothing systematic until Gauss, who introduced what he called the *determinant* of a polynomial.

Gauss

1. Determinant of a quadratic form $ax^2 + 2bxy + cy^2$ is $b^2 - ac$. (*Disquisitiones Arithmeticae*, 1801)

2. Determinant of a ternary quadratic form

$$ax^2 + a'x'x' + a''x''x'' + 2bx'x'' + 2b'xx'' + 2b''xx'$$

   is

$$ab^2 + a'b'b' + a''b''b'' - aa'a'' - 2bb'b''.$$

   (Also in the *D.A.*)

3. Determinant of a (monic) polynomial in general. (*Demonstratione Nova Altera Theorematis Omnem Functionem Algebraicam Rationalem Integram Unius Variabilis in Factores Reales Primi vel Secondi Gradus Resolvi Posse*, 1815)

More Gauss

In the 1815 paper:

- Proof that symmetric functions of the roots can be expressed as polynomials in the coefficients.
- Definition of the "determinant."
- Distinction between the function of the roots and the polynomial in the coefficients.
- Proof of the main properties *without* assuming the polynomial has roots.

With the development of the theory of determinants (of $n \times n$ arrays), it became clear that $\mathrm{disc}(f)$ is (up to sign and a power of the leading coefficient) the square of the Vandermonde determinant

$$\det \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ r_1 & r_2 & r_3 & \dots & r_n \\ r_1^2 & r_2^2 & r_3^2 & \dots & r_n^2 \\ \dots & \dots & \dots & \dots & \dots \\ r_1^{n-1} & r_2^{n-1} & r_3^{n-1} & \dots & r_n^{n-1} \end{bmatrix}$$

Enter Elimination Theory

Beginning with Bézout's work in the late 1700s, much effort was put into systematizing the process of eliminating a variable in a system of several equations.

In the mid-1800s, J. J. Sylvester formalized the process, defining the *resultant* of two polynomials.

If applied to two polynomials in one variable, the resultant is a number (the variable is "eliminated"); it is zero if and only if the polynomials have a common root.

From the point of view of Elimination Theory, $\mathrm{disc}(f)$ can also be interpreted as the resultant of $f(x)$ and $f'(x)$, which yields a determinant formula for $\mathrm{disc}(f)$

$$\begin{vmatrix}
1 & -s_1 & s_2 & \dots & \pm s_{n-1} & \pm s_n & 0 & \dots & 0 \\
0 & 1 & -s_1 & \dots & \pm s_{n-2} & \pm s_{n-1} & \pm s_n & \dots & 0 \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
0 & 0 & 0 & \dots & 1 & -s_1 & s_2 & \dots & \pm s_n \\
n & -(n-1)s_1 & (n-2)s_2 & \dots & \pm s_{n-1} & 0 & 0 & \dots & 0 \\
0 & n & -(n-1)s_1 & \dots & \pm 2s_{n-2} & \pm s_{n-1} & 0 & \dots & 0 \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
0 & 0 & 0 & \dots & n & -(n-1)s_1 & (n-2)s_2 & \dots & \pm s_{n-1}
\end{vmatrix}$$

(I hope that is right!)

The new name "discriminant" was proposed by Sylvester in 1851:

> . . . where *I* denotes the determinant, or, as I shall in the future call such function (in order the avoid the obscurity and confusion arising from employing the same word in two different senses) the Discriminant. . .

(*On a Remarkable Discovery in the Theory of Canonical Forms and Hyperdeterminants*, 1851; *Mathematical Papers*, vol. 1, p. 280.)

He adds a footnote.

"Discriminant," because it affords the *discrimen* or test for ascertaining whether or not equal factors enter into a function of two variables, or more generally of the existence or otherwise of multiple points in the locus represented or characterized by any algebraical function, the most obvious and first observed species of singularity in such function or locus. Progress in these researches is impossible without the aid of clear expression; and the first condition of a good nomenclature is that different things shall be called by different names. The innovations in mathematical language here and elsewhere (not without high sanction) introduced by the author, have been never adopted except under actual experience of the embarrassment arising from the want of them, and will require no vindication to those who have reached that point, where the necessity of some such additions becomes felt.

A later comment:

> The truth of the remark is not appreciably diminished by the occurrence of the word “meso-catalecticism” in another footnote two pages on.

Thomas Muir, *The Theory of Determinants in the Historical Order of Development*, vol. 2, p. 63 (1911)

Hermite was already using the new term in 1854, attributing it to "les Géomètres anglais." (*Crelle* **47**; *Œvres*, vol. 1, p. 225.)

In 1857, we see Hermite saying "...le discriminant (déterminant de Gauss)..." (*Crelle* **53**; *Œvres*, vol. 1, p. 416.) So the term was not yet in wide use.

When was it adopted in German? Dedekind used "discriminant" in 1871.

Francesco Brioschi used the new term in his *La teorica dei determinanti e le sue principali applicazioni* (1854). Brioschi is clearly following Sylvester. Brioschi's book was translated to German in 1856.

George Salmon's book on algebra was translated to German in 1863; Salmon, of course, used "discriminant."

Both terms seem to coexist in German for a long time. Kronecker was using "determinant" of a quadratic form well into the 1870s.

One way to trace the acceptance of the new term in German: Richard Baltzer, *Theorie und Anwendung der Determinanten*

- "determinant": First edition (1857) to third edition (1870).
- "discriminant": Fourth edition (1875) and after.

  Bei dem jetzigen Sprachgebrauch ist der von Sylvester (Philos. Mag, 1851. II p. 406) gebildete Name "Discriminante" bezeichnender.

  (Baltzer, 4th ed., footnote on p. 123)

The discriminant matters

Kronecker, 1854: Let n be a positive integer, let $\Phi_n(x)$ be the nth cyclotomic polynomial, and let α be a root of a monic polynomial $f(x)$ with integer coefficients. If $\gcd(n, \mathrm{disc}(f)) = 1$, then $\Phi_n(x)$ remains irreducible over $\mathbb{Q}(\alpha)$. (Notation and terminology modernized—Kronecker uses "determinant.")

Dedekind points to this result in 1871 as offering the "first hint" (erste Spur) that discriminants played a role in understanding the relationships between different number fields.

Algebraic Numbers

Let θ be a root of an irreducible monic polynomial $f(x)$ of degree n with *integer* coefficients. Gauss, Dirichlet, Eisenstein, and Kummer all studied the field $\mathbb{Q}(\theta)$ consisting of all rational functions of θ.

Any element ω of $\mathbb{Q}(\theta)$ can be written as

$$\omega = a_1 + a_2\theta + a_3\theta^2 + \cdots + a_n\theta^{n-1}$$

with $a_i \in \mathbb{Q}$.

The natural choice of "integers" will then be $\mathbb{Z}[\theta]$, namely (the set of) those ω for which all a_i are integers. The desire is to study the "arithmetic" of such "integers."

Problem 1: Many different θ will define the same field. For example $\mathbb{Q}(2\theta)$ is the same as $\mathbb{Q}(\theta)$, but $\mathbb{Z}[2\theta]$ is much smaller than $\mathbb{Z}[\theta]$. What's worse, the choice affects the arithmetic we want to study.

Problem 2: While one can factor elements of $\mathbb{Z}[\theta]$ as products of non-factorable elements (and units), these factorizations are usually not unique.

Prototype Example: take $\theta_1 = \sqrt{-3}$ to be a root of $x^2 + 3$ and $\theta_2 = (-1 + \sqrt{-3})/2$ to be a root of $x^2 + x + 1$. Then $\mathbb{Q}(\theta_1) = \mathbb{Q}(\theta_2)$.

Eisenstein studied the arithmetic of $\mathbb{Z}[\theta_2]$, which has unique factorization.

On the other hand, $\mathbb{Z}[\theta_1] = \mathbb{Z}[\sqrt{-3}]$ is a real mess:

$$(1 + \sqrt{-3})^3 = -8 = -2^3$$

so no good factorization theory is possible!

The equation

$$(1 + \sqrt{-3})^3 = -8 = -2^3$$

contradicts any prime factorization theory for $\mathbb{Z}[\sqrt{-3}]$:

Let π be a prime, and write $v_\pi(a)$ for the multiplicity of π in the factorization of a. Then we gave $3v_\pi(1 + \sqrt{-3}) = 3v_\pi(2)$ and hence $v_\pi(1 + \sqrt{-3}) = v_\pi(2)$.

Since this holds for any π there must be an invertible element $u + v\sqrt{-3}$ such that $1 + \sqrt{-3} = 2(u + v\sqrt{-3}) = 2u + 2v\sqrt{-3}$, which is impossible because $2u$ and $2v$ are even.

Key definition: an element $\omega \in \mathbb{Q}(\theta)$ is an *algebraic integer* if it is the root of a monic polynomial with *integer* coefficients. (Seems to be due independently to Dedekind and Kronecker.)

We can always take our field to be $\mathbb{Q}(\theta)$, where θ is an algebraic integer. Then every element of $\mathbb{Z}[\theta]$ is an algebraic integer as well, but there may be other algebraic integers in $\mathbb{Q}(\theta)$.

Basic question: how bad can it be? Suppose ω is an algebraic integer and

$$\omega = a_1 + a_2\theta + a_3\theta^2 + \cdots + a_n\theta^{n-1}$$

with $a_i \in \mathbb{Q}$. Can we control the size of the denominators of the a_i?

Theorem: Suppose ω is an algebraic integer. Write

$$\omega = \frac{1}{d}\left(a_1 + a_2\theta + a_3\theta^2 + \cdots + a_n\theta^{n-1}\right)$$

with $a_i \in \mathbb{Z}$, $\gcd(a_1, \ldots, a_n) = 1$. Then d^2 is a divisor of $\operatorname{disc}(f)$.

(First published by Dedekind, 1871.)

This seems to have been the key result. The proof given by Dedekind also suggest how to generalize the notion of the discriminant.

Suppose θ is a root of an irreducible monic polynomial $f(x)$ with integer coefficients. Then we write $\theta^{(1)} = \theta, \theta^{(2)}, \ldots, \theta^{(n)}$ for the roots of $f(x)$.

Define the i-th conjugate of

$$\omega = a_1 + a_2\theta + a_3\theta^2 + \cdots + a_n\theta^{n-1}$$

to be

$$\omega^{(i)} = a_1 + a_2\theta^{(i)} + a_3{\theta^{(i)}}^2 + \cdots + a_n{\theta^{(i)}}^{n-1}$$

It's easy to check that conjugation respects field operations, and in particular that the conjugate of an algebraic integer is also an algebraic integer.

Dedekind's proof shows: if ω is an algebraic integer, then there exists a basis $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ of the field $\mathbb{Q}(\theta)$, with all α_i algebraic integers, such that

$$\operatorname{disc}(f) = \pm d^2 \left(\det \begin{bmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^{(2)} & \alpha_2^{(2)} & \ldots & \alpha_n^{(2)} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_1^{(n)} & \alpha_2^{(n)} & \ldots & \alpha_n^{(n)} \end{bmatrix} \right)^2 .$$

This leads to defining the quantity on the left to be the *discriminant of the system of algebraic numbers* $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$.

$$\operatorname{disc}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \left(\det \begin{bmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^{(2)} & \alpha_2^{(2)} & \ldots & \alpha_n^{(2)} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_1^{(n)} & \alpha_2^{(n)} & \ldots & \alpha_n^{(n)} \end{bmatrix} \right)^2$$

It is easy to see that it is a rational integer when the α_i are algebraic integers.

Notice that

$$\operatorname{disc}(f) = \pm \operatorname{disc}(1, \theta, \theta^2, \ldots, \theta^{n-1}).$$

To do this Dedekind had to understand enough linear algebra to be able to explain what a basis is, and also enough about "modules" (in modern terms, torsion-free finitely-generated $\mathbb{Z}$-modules) to prove the desired result.

It's possible to give a theory-free proof applying Cramer's rule to the system of equations giving ω and its conjugates in terms of θ and its conjugates. Kronecker went that way in his 1881 *Grundzüge*.

Look at the formula again: if ω is an algebraic integer whose expression in terms of powers of θ has denominator d, then there exists a basis $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ of the field $\mathbb{Q}(\theta)$, with all α_i algebraic integers, such that

$$\operatorname{disc}(f) = \pm d^2 \operatorname{disc}(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

More generally, given any two bases of K, their discriminants differ by a square factor ℓ^2.

It then follows that

- There exists a basis of $K = \mathbb{Q}(\theta)$ consisting of algebraic integers whose discriminant has smallest possible absolute value.
- An element $\omega \in \mathbb{Q}(\theta)$ is an algebraic integer if and only if it is a $\mathbb{Z}$-linear combination of such a basis.

Dedekind calls this an *integral basis* of $\mathbb{Q}(\theta)$ and calls its discriminant the *fundamental number* (Grundzahl) or the *discriminant* of the algebraic number field. We'll use the modern notation d_K for this number.

To summarize: if $K = \mathbb{Q}(\theta)$ is a number field and $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is an integral basis, then

$$d_K = \left(\det \begin{bmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^{(2)} & \alpha_2^{(2)} & \ldots & \alpha_n^{(2)} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_1^{(n)} & \alpha_2^{(n)} & \ldots & \alpha_n^{(n)} \end{bmatrix} \right)^2 .$$

We have $d_K \in \mathbb{Z}$. Notice that the determinant itself is *not* an integer, so it is possible that $d < 0$.

Kronecker gave a different, but equivalent, definition.

After the publication of the second edition of Dirichlet-Dedekind in 1871, Dedekind wrote an "Anziege", a kind of book notice. The description of ideals and factorization he gives there has already evolved a little. In particular, he says that he had proved a connection to "higher congruences" that did not appear in Supplement X.

Suppose p is a rational prime, K is a number field of discriminant $\mathrm{disc}(K)$. The question is to determine the factorization of p as an algebraic integer in K.

Let $f(x)$ be a monic polynomial with integer coefficients whose root θ is a primitive element for K, i.e., $K = \mathbb{Q}(\theta)$. Then, as above, $\text{disc}(f) = \pm \ell^2 d_K$ for some integer k.

Suppose p does not divide ℓ and

$$f(x) \equiv P_1(x) P_2(x) \dots P_m(x) \pmod{p}$$

with $P_i(x)$ irreducible modulo p.

Then there exist primes $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_m$ (explicitly given in terms of the polynomials $P_i(x)$) such that

$$(p) = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_m.$$

In other words, if $\text{disc}(f) = \pm\ell^2 d_K$ and p does not divide ℓ, we can determine the factorization of p in K by factoring $f(x)$ modulo p.

The natural question, then, is whether this suffices to determine the factorizations of all rational primes. We could if this were true:

Let K be a number field. For each prime p one can find an algebraic integer θ with irreducible polynomial $f(x)$ such that $K = \mathbb{Q}(\theta)$, $\text{disc}(f) = \pm\ell^2 d_K$, and p does not divide ℓ.

Conjecture: Let K be a number field. For each prime p one can find an algebraic integer θ with irreducible polynomial $f(x)$ such that $K = \mathbb{Q}(\theta)$, $\text{disc}(f) = \pm \ell^2 d_K$, and p does not divide ℓ.

Dedekind quickly realized that this is cannot be true!

Dedekind's Observation

Suppose we have a number field K of degree 3 in which 2 factors as a product of three different primes: $(2) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$.

If we can find an algebraic integer θ with irreducible polynomial $f(x)$ (necessarily of degree 3) such that $K = \mathbb{Q}(\theta)$, $\operatorname{disc}(f) = \pm\ell^2 \operatorname{disc}(K)$, and ℓ is odd (i.e., not divisible by 2), then we must have

$$f(x) = F_1(x)F_2(x)F_3(x) \pmod 2$$

with F_1, F_2 and F_3 *distinct* irreducible polynomials of degree one in $\mathbb{F}_2[x]$.

Dedekind's Observation

Suppose we have a number field K of degree 3 in which 2 factors as a product of three different primes: $(2) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$.

If we can find an algebraic integer θ with irreducible polynomial $f(x)$ (necessarily of degree 3) such that $K = \mathbb{Q}(\theta)$, $\operatorname{disc}(f) = \pm\ell^2 \operatorname{disc}(K)$, and ℓ is odd (i.e., not divisible by 2), then we must have

$$f(x) = F_1(x)F_2(x)F_3(x) \pmod 2$$

with F_1, F_2 and F_3 *distinct* irreducible polynomials of degree one in $\mathbb{F}_2[x]$.

But there are only two such polynomials!

Dedekind found an explicit example, a cubic field K of discriminant -503 in which 2 is a product of three distinct primes. Then for any α with $K = \mathbb{Q}(\alpha)$ and minimal polynomial $f(x)$, we must have $\mathrm{disc}(f)$ divisible by 4.

For this field, the prime 2 is a *common inessential discriminant divisor*: it divides the discriminants of all minimal polynomials of generators of K, but it does not actually divide d_K.

Natural question: when do CIDDs occur? This question was considered by both Dedekind and Hensel, independently of each other.

Is it a Good Question?

It certainly has theoretical significance: Zolotarev's first attempt at a theory of algebraic numbers would have worked if CIDDs did not exist. (This seems to have been Dedekind's motivation for writing the 1878 paper.)

The factorization theorem is very easy to use, so it is somewhat frustrating when it cannot be used.

It would help us to compute d_K.

Dedekind's observation is a sufficient condition: if in a field K we know that

$$(p) = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\ldots\mathfrak{p}_m^{e_m}$$

with distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_m$ of degrees $f_1, f_2, \ldots, f_m$ and there do *not* exist m incongruent mod p monic irreducible polynomials P_i of degree f_i, then p is a common inessential discriminant divisor.

This is very likely to happen when p is small enough!

So CIDDs are not uncommon.

Is this the only reason? In other words, are CIDDs entirely a small primes phenomenon?

Or might there be situations where CIDDs occur for a deeper, more mysterious reason?

Dedekind's Answer

In 1878, Dedekind published *Über der Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen*, in the *Abhandlungen der Königschen Gesellschaft der Wissenschaften zu Göttingen*, volume 23, 1878, pages 1–23.

The first section gives a proof of the theorem giving the factorization of p when it is not an index divisor.

The second and third sections give an explicit constructive way to test whether a prime p divides the index of an algebraic integer θ.

Dedekind's Answer

In the fourth section, Dedekind shows that his initial observation is in fact a necessary and sufficient condition:

Theorem: Let $f_1, f_2, \ldots, f_m$ be the (residual) degrees of the prime divisors $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_m$ dividing p. Suppose there exist m monic irreducible polynomials P_i, pairwise incongruent mod p, with $\deg(P_i) = f_i$. Then there exists an algebraic integer $\theta \in K$ whose index is not divisible by p.

Historiographical Note

In Hasse's *Number Theory*, chapter 25, section 6 (p. 456 of the English translation), this criterion is stated, and Hasse says:

"In deriving this criterion, Hensel gave the first demonstration of the power of his new foundation of algebraic number theory."

As we will see, Hensel did give such a proof, but 16 years after Dedekind. And the first proof did not use the "new foundation" at all!

Does Dedekind's Theorem Settle the Question?

In a way, yes. It shows that common inessential discriminant divisors are a "small primes" phenomenon, depending entirely on a combinatorial condition: are there sufficiently many irreducible polynomials mod p?

On the other hand, to apply Dedekind's criterion requires that we know the factorization of p. Our initial goal was precisely to determine that factorization!

Kronecker and CIDDs

In his famous *Grundzüge* (1882), Kronecker tells us that he had known about the problem of index divisors since 1858:

"I found a similar example in the thirteenth roots of unity when, in 1858, I was doing my first work on this theory. These examples show that the introduction of forms is necessary even in the more special theory of algebraic numbers. . . "

Like Dedekind, Kronecker is arguing that a more sophisticated approach was necessary.

Kronecker and Hensel

Hensel was Kronecker's student, and his first assignment (either from Kronecker or chosen by himself) seems to have been to recreate Kronecker's example "in the 13th roots of unity."

Since for the cyclotomic fields there is always a θ whose index is 1, this must mean that K is a subfield of $\mathbb{Q}(\mu_{13})$.

Hensel found that 3 was a CIDD in the (unique) quartic subfield.

Generalizing, Hensel found a sufficient criterion for a subfield of a cyclotomic $\mathbb{Q}(\mu_p)$, with p prime, to have CIDDs. (In his Ph.D. thesis, 1884.)

Hensel's criterion is not necessary, but he made a big effort to prove that it was. Knowing Dedekind's criterion and Kummer's work on cyclotomic fields, it is easy to construct an counterexample. Hensel cites Dedekind's paper, but apparently had not read it carefully!

Indeed, it seems that the only part of Dedekind's 1878 paper that Hensel really understood was the explicit example of a field where 2 was a CIDD.

Hensel's 1894 Paper

"Arithmetische Untersuchungen über die gemeinsamen ausserwesentlichen Discriminantentheiler einer Gattung" (*Journal für die Reine und Angewandte Mathematik*, 113 (1894), 128–160

This paper seems to contain results from Hensel's *Habilitation* (1886), which was never published. (For details, see Petri's *Perioden, Elementartheiler, Transzendenz: Kurt Hensels Weg zu den p-adischen Zahlen*.)

Hensel seems to have waited until after Kronecker's death (late 1891) because he was under the impression that a proof might be found among his teacher's papers.

Hensel's 1894 Paper

First part: gives a proof of Dedekind's condition. He cites Dedekind for the sufficiency but seems to think the converse is new. His proof is identical to Dedekind's.

§2 opens with: "The result from the previous section can also be expressed in another form that is remarkable in that to apply it we do not need to know the decomposition of p..."

To give that criterion, we have to review some Kroneckerian ideas.

Given a number field K, first find an integral basis $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. Now look at the "generic integer"

$$\omega = u_1\alpha_1 + u_2\alpha_2 + \cdots + u_n\alpha_n$$

where the u_i are variables.

As before, let $\omega^{(1)} = \omega$ and write $\omega^{i)}$ for the conjugates. The *fundamental equation* of the field K is

$$F(t, u_1, u_2, \ldots, u_n) = (t - \omega^{(1)})(t - \omega^{(2)}) \ldots (t - \omega^{(n)}).$$

This is a polynomial in $n + 1$ variables with integer coefficients.

Hensel's idea was to compute the discriminant of the fundamental equation as a polynomial in t. It is

$$\mathfrak{D}(u_1, u_2, \ldots, u_n) = \prod_{i<j} (\omega^{(i)} - \omega^{(j)})^2$$

which is a polynomial in n variables with integer coefficients.

Hensel's Theorem: the *content* of $\mathfrak{D}(u_1, u_2, \ldots, u_n)$ is exactly d_K. In other words,

$$\mathfrak{D}(u_1, u_2, \ldots, u_n) = d_K \Delta(u_1, u_2, \ldots, u_n)^2$$

where Δ is a polynomial with integer coefficients that do not have any common factors. It is sometimes called the *index form*.

Now suppose

$$\theta = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n \in K,$$

where the a_i are integers. Then the discriminant of θ can be computed by taking $\mathfrak{D}$ and plugging the a_is in for the u_is. So:

$$\mathrm{disc}(\theta) = d_K\Delta(a_1, a_2, \ldots, a_n)^2.$$

The upshot: if p is a CIDD for K, Δ will be a polynomial whose coefficients are not all divisible by p, but whose values when we plug in integers are *always* divisible by p.

Hensel then gave a constructive criterion for a polynomial to have that property.

Does that settle it?

Dedekind's criterion requires us to know how to factor p in K.

Hensel's criterion requires us to have an integral basis for K. (It is also quite heavy in terms of computation.)

The missing piece was supplied by Hensel after 1897: his p-adic numbers give us a way to find the factorization of p, and then one can use Dedekind's criterion. That story I will save for another time.

So was the problem interesting?

The verdict seems to be “no”!