Dedekind's 1871 version of the theory of ideals*

Translated by Jeremy Avigad

March 19, 2004

Translator's introduction

By the middle of the nineteenth century, it had become clear to mathematicians that the study of finite field extensions of the rational numbers is indispensable to number theory, even if one's ultimate goal is to understand properties of diophantine expressions and equations in the ordinary integers. It can happen, however, that the "integers" in such extensions fail to satisfy unique factorization, a property that is central to reasoning about the ordinary integers. In 1844, Ernst Kummer observed that unique factorization fails for the cyclotomic integers with exponent 23, i.e. the ring $\mathbb{Z}[\zeta]$ of integers of the field $\mathbb{Q}(\zeta)$, where ζ is a primitive twenty-third root of unity. In 1847, he published his theory of "ideal divisors" for cyclotomic integers with prime exponent. This was to remedy the situation by introducing, for each such ring of integers, an enlarged domain of divisors, and showing that each integer factors uniquely as a product of these. He did not actually *construct* these integers, but, rather, showed how one could characterize their behavior qua divisibility in terms of ordinary operations on the associated ring of integers.

Richard Dedekind and Leopold Kronecker later took up the task of extending the theory to the integers in *arbitrary* finite extensions of the rationals. Despite their common influences and goals, however, the theories they

*Work on this translation has been supported by a *New Directions* fellowship from the Andrew W. Mellon Foundation. As of March 2005, I have made a few minor corrections; the most notable occurs in footnote 19.

developed are strikingly different. Whereas Kronecker's is explicitly computational throughout, Dedekind's stated goal was to *avoid* computational reasoning:

> Even if there were such a theory, based on calculation, it still would not be of the highest degree of perfection, in my opinion. It is preferable, as in the modern theory of functions, to seek proofs based immediately on fundamental characteristics, rather than on calculation, and indeed to construct the theory in such a way that it is able to predict the results of calculation...[1]

Dedekind, in fact, published four versions of his theory of ideals. Three appeared in his "supplements," or appendices, to the second, third, and fourth editions of Dedekind's transcription of Dirichlet's *Vorlesungen über Zahlentheorie*, or *Lectures on Number Theory* [8]. These editions appeared in 1871, 1879, and 1894, respectively. The remaining version was written at the request of Lipschitz, translated into French, and published in the *Bulletin des Sciences Mathématiques et Astronomiques* in 1876-1877. It was also published as an independent monograph in 1877, and is, in essence, an expanded presentation of the version he published in 1879.

Whereas Dedekind's first version remained fairly close to Kummer's computational style of presentation, the later versions became increasingly abstract and algebraic. As a result, the development is an early and salient example of a transition to types of reasoning (set-theoretic, algebraic, structural, infinitary, nonconstructive, and so on) that are characteristic of modern mathematical thought. Thus, it is not surprising that Harold Edwards, who laments mathematics' departure from the explicitly computational styles of Gauss, Kummer, and Kronecker, judges Dedekind's first version of ideal theory to be his best [10, 12]. In contrast, Emmy Noether, who inherited the mantle of structuralism from Dedekind through Hilbert, expressed a clear preference for the last. Tracing the development of Dedekind's thinking can therefore help us gain a better understanding of how it is that modern mathematics, for better or for worse, has come to be the way it is.

Of the four versions of ideal theory, the long, second version of 1877 has been translated by John Stillwell [7], with a helpful introduction. What appears below is a translation of the first, 1871 version. This comprises

[1] Dedekind [4, §12], quoted by Stein [18, page 245].

§§159–163 from Supplement X, "On the composition of binary quadratic forms," from the second edition of the Dedekind-Dirichlet *Lectures*.[2]

A good deal has been written about Dedekind's work, from mathematical and historical perspectives.[3] Edwards' detailed survey [10] provides an excellent overview of the development of the theory of ideals from Kummer to Dedekind and Kronecker, and Stillwell's introductory notes to [7, 9] provide additional background.[4] Since these provide excellent historical and mathematical context for appreciating the material below, I will add only a few introductory remarks here.

From a methodological point of view, perhaps the most striking difference between Dedekind's theory and Kummer's is Dedekind's use of the set-theoretic notion of an *ideal*. Recall that Kummer reasoned about his ideal divisors only indirectly, in terms of explicitly given predicates that express what it means for an algebraic integer x of the field in question to be divisible by the ideal divisor α. In contrast, Dedekind chose to identify the ideal divisor α with the set, or "system," of all the integers x that it divides. It is clear that this set is closed under addition, and under multiplication by any integer. Thus, Dedekind, in fact, introduced the modern algebraic definition of an ideal, and ultimately showed that every such ideal arises from an ideal divisor in Kummer's sense.

Dedekind went out of his way to explain why this tack is to be preferred. At the end of §162 below, he notes that although Kummer's approach is perfectly rigorous, the fact that the indirect references to ideal divisors are not references to actual objects may cast doubt on the validity of proofs. In the introduction to the 1877 version, he is more emphatic in claiming that the approach can lead to "hasty conclusions and incomplete proofs."

[2]The German title of the supplement is *Über die Komposition der binären quadratischen Formen*. Sections §§159–163 are found on pages 423–462 of the original version, and on pages 223–261 of both [6] and [5]. Note that Dedekind's entire *Werke* is available online at [20]; a PDF version of the van der Waerden reprinting of this version of ideal theory is available on my web page, http://www.andrew.cmu.edu/∼avigad.

The preceding sections in Supplement X develop a Gaussian theory of binary quadratic forms, accounting for the title. The sections after the ones translated develop the theory further, treating ideal classes, more general results for orders and modules, and applications of the theory to the study of quadratic forms. More on these topics can be found in [7, 9] and Stillwell's introductory notes to these.

[3]See, for example, [2, 15] and the references there, or the online bibliography at [21].

[4]See also Edwards' discussion of Kummer's work in [13], and a modern presentation of Kronecker's theory in [11].

Replacing talk of predicates by talk of sets may seem to be nothing more than linguistic convenience, but this move has important methodological consequences: treating sets (or predicates) as "objects" in their own right allows one to define operations on them in a manner that is *independent of the way in which they are represented*.

Thus, for example, in §161, Dedekind defines the least common multiple of two modules to be their intersection, without worrying about how a finite set of *generators* for this intersection can be computed from finite sets of generators for the initial modules. We find a similar use of nonconstructivity in §162, where Dedekind characterizes integral bases as those bases of integers whose discriminants have the least absolute value; he does this without giving an algorithm for *finding* such a basis or determining this least discriminant. In fact, in both examples just cited, algorithms can be obtained. But Dedekind's presentation sends the strong message that such algorithms are not *necessary*, i.e. that one can have a fully satisfactory theory that fails to provide them. This paves the way to more dramatic uses of nonconstructive reasoning, in which one uses facts about infinitary functions, sets, and sequences that are *false* on an algorithmic interpretation. Such reasoning was used, for example, by Hilbert, in proving his *Basissatz* in 1890.

There are at least two significant differences between the 1871 and 1877 versions of Dedekind's ideal theory.[5] The first has to do with the use of "simple ideals" in 1871. In §163, Dedekind defines a simple ideal to be a prime ideal that can be represented as the set of all solutions π to a congruence $\nu\pi \equiv 0 \pmod{\mu}$. As was the case with Kummer's theory, this means that there is an effective test for divisibility by these ideal prime divisors: an algebraic integer π is divisible by the ideal divisor corresponding to μ and ν if and only if it satisfies the associated congruence. This can be extended to provide a test for divisibility by *powers* of these ideal divisors, cast in §163 as a definition of the powers of the simple ideals. Dedekind shows that the notion of divisibility by powers of the simple ideals has the requisite properties; in particular, every element of the ring of integers is determined (up to associates) by the powers of the simple ideals that divide it. This implies that *every* prime ideal is a simple ideal, and that, in turn, implies that every ideal (other than $\{0\}$) can be represented by an appropriate μ and ν. Thus, every ideal in the new sense arises as the set of integers divisible by

[5]In comparing the two theories, I have benefited a good deal from discussions with Steven Douglas White, who will expand on this analysis in an upcoming MS thesis.

one of Kummer's ideal divisors. This is what Dedekind has in mind when he writes, in the 1877 introduction:

> A fact of highest importance, which I was able to prove rigorously only after numerous vain attempts, and after surmounting the greatest difficulties, is that, conversely, each system enjoying [the new definition of an ideal] is also an ideal [in Kummer's sense]. That is, it is the set $\mathfrak{a}$ of all numbers α of the domain $\mathfrak{o}$ divisible by a particular number; either an actual number or an ideal number indispensable for the completion of the theory.

Relying on simple ideals, however, runs counter to Dedekind's goal of avoiding reasoning that is based on particular representations of ideals rather than their "fundamental characteristics." By 1877, he has therefore dropped the term. That is not to say that he has avoided the use of such representations in his arguments: the ν and π above become κ and λ in a key argument in §25, but they are deprived of the honored status that is accorded by a definition, and the associated calculations are relegated to a pair of "auxiliary propositions" in the preceding section.

Dedekind's exposition and the mathematical context make it clear why the calculations have been moved. Contemporary algebraic treatments of the theory of ideals tend to identify the most general classes of structures for which the various results of the theory hold; Dedekind's 1877 treatment is remarkably modern in this respect. Chapter 1 of that version, as well as §161 below, develop general theorems that are true of arbitrary *modules*.[6] In the 1877 version, he then, very self-consciously, develops the portion of the theory of ideals that only presupposes that one is dealing with a ring of integers whose rank as a module coincides with the degree of the extension. Following Dedekind, these structures are still called *orders* today. With a specific counterexample, Dedekind notes that not every order has a theory of

[6]In both presentations, Dedekind defines a module to be a system of complex numbers that is closed under sums and differences. But at the end of [4, Chapter 1], he notes that the "researches in this first chapter ... do not cease to be true when the Greek letters denote not only numbers, but any objects of study, any two of which α, β produce a determinate third element $\gamma = \alpha + \beta$ of the same type, under a commutative and uniformly invertible operation (composition), taking the place of addition. The module $\mathfrak{a}$ becomes a *group* of elements...." In other words, Dedekind observes that the results hold for any (torsion-free) abelian group, viewed (in modern terms) as a free module over $\mathbb{Z}$. Today we recognize that, in fact, they hold more generally for free modules over a principal ideal domain.

ideal divisors (see the discussion below and at the end of [10, Section 5]), and then identifies the auxiliary propositions as being precisely the point at which one needs to assume that the ring in question is integrally closed, that is, consists of *all* the integers of the ambient number field. These propositions are clearly *necessary* for the ring to have a theory of ideal divisors; the subsequent development in 1877 shows that they are also sufficient. By meticulously identifying the algebraic-axiomatic assumptions that are in play at each stage of the development, Dedekind is clearly anticipating twentieth-century structuralist thought.

The observations just described are also present in the 1871 version (see, for example, footnote 31); the 1877 version simply makes them more prominent. It is easy to sympathize with Edwards, who feels that the resulting reorganization makes the proof of unique factorization seem ad-hoc and unmotivated. But in localizing and minimizing the role of representations and calculations, and making them secondary to structural systematization, Dedekind is exhibiting tendencies that have become hallmarks of modern mathematics. In the 1871 version, after showing that every prime ideal is simple, he remarks, in passing, that "we will therefore speak only of prime ideals in the future, and no longer of simple ideals." In light of the methodological overtones, this remark takes on greater significance than Dedekind intended.

Another important difference between the 1871 and 1877 versions is the treatment of multiplication of ideals. In 1871, unique factorization is expressed by the fundamental theorem that every ideal is the least common multiple of all the powers of prime ideals that divide it, where the least common multiple of any finite set ideals is defined to be their intersection. *Multiplication of ideals* plays no role in the proof, and is, in fact, defined only afterwards. In contrast, in 1877, multiplication of ideals is defined much earlier, and plays a central role in the presentation of the theory.

Why the change? Dedekind's frequent methodological comments show that he is acutely aware of the role that definitions play in structuring a theory. One finds him concerned with such issues of systematization as early as 1854, in his *Habilitationsrede* [3]. There, he characterizes a process of extending operations like addition and multiplication to extended domains, whereby one identifies the laws they satisfy in a restricted domain, and stipulates that these laws are to maintain their general validity (see also the discussion in [17]). Now, it is natural to express the goal of the theory of ideal divisors as being that of constructing a semigroup satisfying unique

factorization, together with a suitable embedding of the integers of the field in question (up to associates). This is, for example, the characterization used in Weyl's Princeton lectures on algebraic number theory from 1938–39 [19], as well as in more recent presentations, like Borevich and Shafarevich's textbook [1]. On this view, the goal is to define the collection of ideals *with an associated multiplication*, and to show that the resulting structure meets the specification. From that perspective, multiplication is naturally prior.

One might object that one can equally well characterize the goal of a theory of divisors taking the notions of divisibility and "prime power" as primitive. Kummer himself stated the requisite properties of the theory in such a way (see [10, Section 3]), and Dedekind's 1871 version shows, directly, these these requirements are satisfied by the system of ideals. But this way of proceeding runs against another one of Dedekind's methodological dicta, namely, that definitions and methods of proof used in an extended domain should parallel the definitions and methods of proof that have been effective in more restricted domains. In the presentation of ideal theory, he is careful to point out where definitions, basic characteristics, theorems, and proofs with respect to algebraic integers and ideals agree with their counterparts for the ordinary integers, and he seems to enjoy citing parallel developments in the *Lectures* wherever he can. This insistence on preservation of properties as one passes from a restricted domain to a more general one accords well with the guidelines he set in his 1854 lecture. The methodological benefits are clear, since it is often easy and efficient to reuse, adapt, and extend familiar modes of reasoning. In textbook presentations of the ordinary integers, multiplication is almost always considered to be a basic operation, whereas exponentiation, divisibility, and primality are defined from that. Dedekind would likely have felt that the domain of ideals should be treated along similar lines, insofar as possible.

Unfortunately, the theory of ideals diverges from the theory of integers almost immediately. It would be natural to say that an ideal $\mathfrak{a}$ *divides* an ideal $\mathfrak{b}$ if there is an ideal $\mathfrak{c}$ such that $\mathfrak{ac} = \mathfrak{b}$. But, instead, Dedekind adapts Kummer's notion of divisibility, whereby "$\mathfrak{a}$ divides $\mathfrak{c}$" means that $\mathfrak{a}$ *includes* $\mathfrak{c}$, i.e. $\mathfrak{a} \supseteq \mathfrak{c}$. In Kummer's language of ideal divisors, this amounts to saying that every integer divisible by $\mathfrak{c}$ is divisible by $\mathfrak{a}$. The fact that there are two natural notions of divisibility at hand is confusing, but the good news is that, in the end, the two notions coincide. According to Dedekind's introduction to the 1877 version, this is something we come to see "only after we have vanquished the deep difficulties characteristic of the nature

of the subject." Indeed, establishing the equivalence is almost tantamount to establishing unique factorization itself. To see this, note that unique factorization for the integers follows from the fact that the notions of "prime" and "irreducible" coincide. Passing to the theory of ideals, it is easy to show that every prime ideal is irreducible, and, further, that every prime ideal is prime *with respect to the Dedekind-Kummer notion of divisibility*. Demonstrating that the two notions of divisibility coincide therefore shows that there is sufficient agreement with the theory of the integers to ensure that unique factorization holds for ideals as well.

To sum up, making multiplication central to the development provides a way of characterizing the goals of the theory of ideal divisors in a way that highlights parallels with the theory of the integers, and helps make it clear how one can attain these goals by resolving the apparent differences between the two.

Let me close by commenting on the part of the text below that is likely to cause the most difficulties for a contemporary audience, namely, Dedekind's analytic treatment of quadratic forms in §159. Given a choice of basis $\omega_1, \omega_2, \ldots, \omega_n$ for a field Ω, viewed as a vector space over $\mathbb{Q}$, one can specify the multiplicative structure of the field by specifying each product of basis elements in terms of that basis. In other words, it suffices to write each product $\omega_j \omega_k$ as a sum

$$\omega_j \omega_k = \sum_i a_{i,j,k} \omega_i,$$

where each $a_{i,j,k}$ is a rational number. Not every choice of elements $a_{i,j,k}$ arises in such a way, however. To get a handle on the ways they are constrained, Dedekind defines, for each i, the quadratic form

$$H_i = \frac{1}{2} \sum_{j,k} a_{i,j,k} \omega_j \omega_k,$$

where now ω_j and ω_k are viewed as *variables*. He then takes the surprising step of treating the H_i as functions on the *real numbers*, and proceeds to use various differential operators and Jacobian functional determinants to derive what are, implicitly, identities in the coefficients $a_{i,j,k}$. In other words, Dedekind uses analytic techniques as a device for encoding and studying arithmetic properties of the number field. This may strike the modern reader as bizarre, but in doing so, Dedekind shows the influence of Jacobi, for whom arithmetic determinants and functional determinants were flip-sides of the

same coin.[7] In any event, the reader may well wish to skip §159, and begin with §160. The definition of the algebraic integers found there, and the subsequent development of the theory, will be more reassuringly familiar.

My German reading ability is limited, so treat this translation with caution. I am grateful to Wilfried Sieg and Dirk Schlimm for help with the translation, and for comments on and corrections to these introductory notes. I am also grateful to Steve Douglas White for helpful discussions and numerous corrections.

All the footnotes below, except for the ones with text in square brackets, are from the original. Note, however, that the original footnotes were not numbered.

References

[1] A. I. Borevich and I. R. Shafarevich. *Number theory*. Translated from the 1964 Russian first edition by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20. Academic Press, New York, 1966.

[2] Leo Corry. *Modern algebra and the rise of mathematical structures*, volume 17 of *Science Networks. Historical Studies*. Birkhäuser Verlag, Basel, 1996.

[3] Richard Dedekind. Über die Einführung neuer Funktionen in der Mathematik. Delivered as a *Hablitationsvorlesung* in Göttingen on June 30, 1854. Translated by William Ewald as "On the introduction of new functions in mathematics" in [14], volume 2, pages 754–762.

[4] Richard Dedekind. *Sur la théorie des nombres entiers algébrique*. Gauthier-Villars, Paris, 1877. Also *Bulletin des sciences mathématiques et astronomiques (1)*, 11 (1876) 278–288, (2), 1 (1877) 17–41, 69–92, 144–164, 207–248; parts also on pages 263–296 of [6, volume 3] and [5]. Translated as [7].

[5] Richard Dedekind. *Über die Theorie der ganzen algebraischen Zahlen*. F. Vieweg, Braunschweig, 1964. Excerpts on ideal theory from [6], with a forword by B. van der Waerden.

[7] See [16]. Jacobi's *Werke* is available online at [22], and the three papers discussed in [16] can be found, in Latin, on pages 355–452. The second of these is the one cited by Dedekind in footnote 17.

[6] Richard Dedekind. *Gesammelte mathematische Werke.* Edited by Robert Fricke, Emmy Noether and Öystein Ore. Chelsea Publishing Co., New York, 1968. Volumes I–III. Reprinting of the original edition, published by F. Vieweg & Sohn, Braunschweig, 1932. Available online at [20].

[7] Richard Dedekind. *Theory of Algebraic Integers.* Cambridge University Press, Cambridge, 1996. A translation of [4], translated and introduced by John Stillwell.

[8] Peter Gustave Lejeune Dirichlet. *Vorlsesungen über Zahlentheorie.* Vieweg, Braunschweig, 1863. Subsequent editions in 1871, 1879, 1894, with "supplements" by Richard Dedekind. Translated as [9].

[9] Peter Gustave Lejeune Dirichlet. *Lectures on number theory*, volume 16 of *History of Mathematics.* American Mathematical Society, Providence, RI, 1999. A translation of [8], translated and introduced by John Stillwell.

[10] Harold M. Edwards. The genesis of ideal theory. *Archive for History of Exact Sciences*, 23:321–378, 1980.

[11] Harold M. Edwards. *Divisor theory.* Birkhäuser Boston Inc., Boston, MA, 1990.

[12] Harold M. Edwards. Mathematical ideas, ideals, and ideology. *Math. Intelligencer*, 14(2):6–19, 1992.

[13] Harold M. Edwards. *Fermat's last theorem: a genetic introduction to algebraic number theory*, volume 50 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1996. Corrected reprint of the 1977 original.

[14] William Ewald, editor. *From Kant to Hilbert: A Source Book in the Foundations of Mathematics.* Clarendon Press, Oxford, 1996. Volumes 1 and 2.

[15] José Ferreirós. *Labyrinth of thought: a history of set theory and its role in modern mathematics*, volume 23 of *Science Networks. Historical Studies.* Birkhäuser Verlag, Basel, 1999.

[16] Eberhard Knobloch. From Gauss to Weierstrass: determinant theory and its historical evaluations. In *The intersection of history and mathematics*, volume 15 of *Sci. Networks Hist. Stud.*, pages 51–66. Birkhäuser, Basel, 1994.

[17] Dirk Schlimm and Wilfried Sieg. Dedekind's analysis of number: systems and axioms. To appear in *Synthese*.

[18] Howard Stein. Logos, logic, and logistiké. In William Aspray and Phillip Kitcher, editors, *History and Philosophy of Modern Mathematics*, pages 238–259. University of Minnesota, 1988.

[19] Hermann Weyl. *Algebraic theory of numbers*. Princeton Landmarks in Mathematics. Princeton University Press, Princeton, NJ, 1998. Reprint of the 1940 original, Princeton Paperbacks.

[20] Göttinger DigitalisierungsZentrum GDZ. http://gdz.sub.uni-goettingen.de/en/.

[21] The MacTutor History of Mathematics archive. http://www-history.mcs.st-and.ac.uk/history/.

[22] University of Michigan Historical Mathematics Collection. http://www.hti.umich.edu/u/umhistmath/.

X. On the composition of binary quadratic forms

§159.

The theory of binary quadratic forms, and the equivalence and composition thereof, constitutes only a special case of the theory of those nth-degree homogeneous forms in n variables that can be decomposed into linear factors with algebraic coefficients. These forms were first considered by *Lagrange.*[8] Later, *Dirichlet*[9] was often preoccupied with this subject, but of his general investigations he only published those that deal with the transformation of such forms into themselves (cf. §§61, 62) or, in other words, with the theory of units for the corresponding algebraic numbers. Finally, *Kummer,*[10] through the introduction [Schöpfung] of ideal numbers, introduced a new method which not only allows for a more convenient manner of expression, but also leads to a deeper insight into the true nature of algebraic numbers. In striving to introduce the reader to these new ideas, we will establish for ourselves a somewhat higher standpoint, and, from there, begin to introduce concepts that seem to be well-suited to serve as a foundation for higher algebra and related parts of number theory.

I. By a *field [Körper]* we mean an infinite system [System] of real or complex numbers, which is closed and complete in itself, so that the addition, subtraction, multiplication, and division of any two of these numbers always yields yet another number of the same system. The simplest field consists of all the rationals, and the largest field consists of all numbers. We call a field A a *divisor* of field M, and the latter a *multiple* of the former, when all the numbers in A are also found in M. One easily sees that the field of rational numbers is a divisor of every other field. The totality [Inbegriff] of numbers which are in two fields A and B at the same time form yet another field D, which can be called the *greatest [größte]* common divisor of the pair of

[8] *Sur la solution des problèmes indéterminés du second degré.* §VI. Mém. de l'Ac. de Berlin. T. XXIII, 1769. (Oeuvres de L. T. II, 1868, p. 375) — *Additions aux Éléments d'Algèbre par L. Euler.* §IX.

[9] Cf. the notes to §141.

[10] Cf. the notes to §16.

fields A, B, and clearly each divisor of both A and B is necessarily a divisor of D. Likewise there is always a field M which should be called the *least [kleinste]* common multiple of A and B, since it is a divisor of every other common multiple of both fields. If furthermore there corresponds to each number a in the field A a number $b = \varphi(a)$, in such a way that $\varphi(a + a') = \varphi(a) + \varphi(a')$ and $\varphi(aa') = \varphi(a)\varphi(a')$, then the numbers b (assuming they do not all vanish) form a field B, which is *conjugate* to A, and arises from A from the *substitution* φ; and conversely $B = \psi(A)$ is conjugate to B. Two fields that are conjugate to a third are also conjugate to one another, and every field is conjugate to itself. Numbers in two conjugate fields A and B that correspond as a and $b = \varphi(a)$ are called *conjugate numbers*.

The simplest fields are those that have only a *finite* number of divisors. Call m given numbers $\alpha_1, \alpha_2, \ldots, \alpha_m$ *dependent on one another* or *independent*, depending on whether or not the equation $x_1\alpha_1 + x_2\alpha_2 + \cdots + x_m\alpha_m$ is solvable by rational numbers $x_1, x_2, \ldots, x_m$ that do not all vanish. Via very simple considerations that we will not go into here, one finds that in a field Ω of the indicated type,[11] it is possible to choose a finite number [Anzahl] n of independent numbers $\omega_1, \omega_2, \ldots, \omega_n$, so that every number ω of the field can be represented in the form

$$\omega = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n = \sum h_i\omega_i \tag{1}$$

in a unique way, where $h_1, h_2, \ldots, h_n$ denote rational numbers. We call the number n the *degree*, the system of n independent numbers ω_i a *basis of the field* Ω, and the n numbers h_i the *coordinates of the number* ω corresponding to this basis. Clearly any n numbers of the form (1) form such a basis when the determinant from the corresponding n^2 coefficients is nonzero. Such a *transformation* of the basis by linear substitutions corresponds to a transformation of the coordinates via the so-called *transposed* substitution.

The requirement that the numbers ω of the field Ω are closed [sich reproduzieren] under addition and subtraction is already guaranteed by the common form (1). For closure under multiplication it is further necessary and sufficient that each product $\omega_i\omega_{i'}$ can again be expressed in the form (1). These conditions, of which there are $\frac{1}{2}n(n+1)$, can be combined most simply

[11] If one replaces the rational numbers everywhere by numbers of a field R, then the following observations also hold for a field Ω which has only a finite number of divisors that are also multiples of R.

by viewing the coordinates h_i as *variables* and writing

$$\omega^2 = 2\sum H_i\omega_i, \tag{2}$$

where now $H_1, H_2, \ldots, H_n$ are certain homogeneous quadratic functions of the coordinates, with rational coefficients. The constitution of the field Ω is entirely determined by these n functions H_i, whose analytic properties we will come back to. First, it is possible to show that the numbers of the form (1) are also closed under division. By total differentiation of (2) one has

$$\omega d\omega = \sum dH_i\omega_i. \tag{3}$$

If one assigns arbitrary rational values to the coordinates and their derivatives, then by the previous equality the product of any two numbers ω and $d\omega$ of the field Ω are reduced to the form (1). In particular, from (3) one has

$$\omega\omega_r = \sum \frac{\partial H_i}{\partial h_r}\omega_i. \tag{4}$$

If one now assigns any rational values that do not all vanish to the coordinates h_i, the corresponding value of the functional determinant

$$H = \sum \pm \frac{\partial H_1}{\partial h_1}\frac{\partial H_2}{\partial h_2}\cdots\frac{\partial H_n}{\partial h_n} \tag{5}$$

does not vanish either. For, otherwise, as is well-known, there would be n rational numbers dh_i that do not all vanish, such that for each index r

$$dH_r = \sum \frac{\partial H_r}{\partial h_i}dh_i = 0.$$

But then it would also follow that $\omega d\omega = 0$, whereas in fact neither ω nor $d\omega$ vanishes. From this it also follows, reversing the n equations (4), that the n quotients ω_i/ω are again numbers of the form (1).[12] The same holds for any quotients α/ω, where α is any number of the form (1). Thus all the numbers of the form (1) really form a field.

Eliminating the n numbers ω_i from the n equations (4), we have the equality

$$\begin{vmatrix} \frac{\partial H_1}{\partial h_1} - \omega & \frac{\partial H_2}{\partial h_1} & \cdots & \frac{\partial H_n}{\partial h_1} \\ \frac{\partial H_1}{\partial h_2} & \frac{\partial H_2}{\partial h_2} - \omega & \cdots & \frac{\partial H_n}{\partial h_2} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{\partial H_1}{\partial h_n} & \frac{\partial H_2}{\partial h_n} & \cdots & \frac{\partial H_n}{\partial h_n} - \omega \end{vmatrix} = 0. \tag{6}$$

[12] [Here and in the text below, I will use the notation a/b instead of Dedekind's $a : b$.]

Hence each number ω in the field Ω is the root of an equation of degree n with rational coefficients (which is independent of the choice of basis), and so an *algebraic* number. It can easily be shown that in the field Ω there also exist numbers that do not satisfy any equation with rational coefficients of degree less than n, for which the previous equation is *irreducible*.[13] Let θ be any such number, so that clearly the powers $1, \theta, \theta^2, \ldots, \theta^{n-1}$ likewise form a basis of the field Ω, and Ω is the system of all numbers which can be obtained from θ by any iteration of the four basic arithmetic operations. If one now

[13]The proof of this assertion can be based, for example, on the following lemma:

If a homogeneous linear function $\omega = \sum h_i \omega_i$ in n variables h_i satisfies an identity of the form

$$A\omega^m + A_1\omega^{m-1} + \ldots + A_m = 0, \tag{1}$$

where $A, A_1, \ldots, A_m$ are whole functions in the variables h_i with *rational* coefficients, that do not vanish identically, and if the degree m is *smaller* than the number of variables n, then the n quantities ω_i are *dependent* on one another.

By total differentiation of the identity (1) we then have

$$Md\omega + \omega^m dA + \omega^{m-1} dA_1 + \ldots + dA_{m-1} = 0 \tag{2}$$

where for short we set

$$M = mA\omega^{m-1} + (m-1)A_1\omega^{m-2} + \ldots + A_{m-1}.$$

One can now clearly assume that there is no identity of the form (1) of degree less than m, so that the product AM does not identically vanish. Now it is always possible to assign rational values to the variables h_i so that AM takes on a nonzero value. Then because $m < n$ one can assign to the n differentials dh_i rational values that do not all vanish and satisfy the m homogeneous linear equations

$$AdA_1 = A_1 dA, AdA_2 = A_2 dA, \ldots, AdA_m = A_m dA.$$

One now multiplies (1) by dA, (2) by A, and subtracts, and $AMd\omega = 0$ follows, as well as $d\omega = \sum dh_i \omega_i = 0$, as was to be proved.

It follows next that if the values ω_i and ω are given their old interpretation, the coordinates of the n values $1, \omega, \omega^2, \ldots, \omega^{n-1}$ form a determinant D, which is a homogeneous function of the variables h_i of degree $\frac{1}{2}n(n-1)$. This cannot vanish, because otherwise ω would satisfy an identity of the form (1) of degree lower than n, and then the values ω_i would be dependent on one another. If one now assigns the coordinates h_i rational values for which D takes a nonzero value, then it follows directly that the corresponding number ω of the field Ω is an irreducible equation of degree n.

Every solution to the equation $D = 0$ in rational numbers h_i corresponds to a number ω which belongs to a divisor of the field Ω of degree less than n. The degree of any such divisor is always a divisor of n.

substitutes for θ the sequence of all roots of the same irreducible equation, just as many corresponding equations arise, which are clearly conjugate to Ω and to one another. It is easy to show that no fields other than these are conjugate to Ω. To prevent any misunderstandings, however, we hereby remark that some or even all of these n fields, and the totalities of numbers that are contained therein, may well be the same, although they arise from n *different* substitutions from one another.[14]

Since, now, by virtue of the notion of conjugate fields, equation (4) remains valid if the numbers of the field Ω are replaced by the corresponding numbers of a conjugate field, it easily follows that all the roots of equation (6) are conjugate to ω. One thus uses $N(\omega)$ to denote the so-called *norm* of the number ω, i.e. the product of all n conjugate roots, which can be equal to each other in groups. Then as a consequence of (6) we have

$$N(\omega) = H, \tag{7}$$

i.e. the homogeneous function H is the product of n conjugate factors of degree one with algebraic coefficients. From this definition we immediately have the following theorem: *the norm of a product is always equal to the product of the norms of the factors.* If, further, we write

$$N(\omega) = \omega\omega' \tag{8}$$

then ω' is also a number of the field Ω, since $N(\omega)$ is a rational number contained in Ω, a fact which also follows from (6). In particular we have

$$N(\omega') = N(\omega)^{n-1}; \tag{9}$$

we call ω' the number *adjunct [adjungierte] to* ω.[15] So the number adjunct to ω' is $= \omega N(\omega)^{n-2}$.

If $\alpha_1, \alpha_2, \ldots, \alpha_n$ are arbitrary numbers of the field Ω, and $\beta_i, \gamma_i, \ldots, \lambda_i$ denote the remaining $(n-1)$ numbers conjugate to α_i, then we write for short

$$(\sum \pm\alpha_1\beta_2 \ldots \lambda_n)^2 = \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) \tag{10}$$

[14]By pursuing these topics further one arrives immediately at the principles introduced to algebra by *Galois* (*Sur les conditions de résoubilité des équations par radicaux*; Journ. de Math., p. p. Liouville. T. XI. 1846). In this connection it is then appropriate to search for the simple reciprocity laws which govern the greatest common divisors and the least common multiple of any two fields like Ω.

[15]This expression was used in an entirely different sense by *Galois*.

and we call this squared determinant the *discriminant* of the n numbers $\alpha_1, \alpha_2, \ldots, \alpha_n$. This is a symmetric function of the n numbers conjugate to θ, and therefore a rational number. In particular,

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = m^2 \Delta(\omega_1, \omega_2, \ldots, \omega_n) \tag{11}$$

where m is the determinant comprised of the coordinates of the numbers $\alpha_1, \alpha_2, \ldots, \alpha_n$. Since the discriminant $\Delta(1, \theta, \theta^2, \ldots, \theta^{n-1})$ is well-known to be the product of all the differences between the numbers conjugate to θ, and therefore nonzero (since an irreducible equation must have distinct roots), $\Delta(\alpha_1 \ldots \alpha_n)$ is $= 0$ if and only if the numbers $\alpha_1, \alpha_2, \ldots, \alpha_n$ are independent of one another. Finally, in general, we have

$$\Delta(\omega\alpha_1, \omega\alpha_2, \ldots, \omega\alpha_n) = N(\omega)^2 \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n). \tag{12}$$

II. All the concepts and theorems that we will need in the sequel have been developed above. For elucidation, however, we further wish to disclose here the important and subsequent results from the great riches of analytic developments that consideration of the functions H_i touches upon. A fundamental relation holds of these n functions, which one obtains when one forms products of *three* arbitrary numbers of the field Ω in all possible ways (cf. §§1, 2). If d' further denotes any variation, then, from (4), we have

$$d'\omega\omega_r = \sum d' \left(\frac{\partial H_i}{\partial h_r} \right) \omega_i.$$

If one now multiplies (3) by $d'\omega$, and replaces the products $d'\omega\omega_i$ accordingly in the sum in the previous equation, we have

$$\omega d\omega d'\omega = \sum dH_i d' \left(\frac{\partial H_{i'}}{\partial h_i} \right) \omega_{i'}.$$

Since the left side is symmetric with respect to d and d', and since the n numbers $\omega_{i'}$ are independent, it follows that the functions H_i satisfy the n differential equations

$$\sum dH_i d' \left(\frac{\partial H_r}{\partial h_i} \right) = \sum d' H_i d \left(\frac{\partial H_r}{\partial h_i} \right), \tag{13}$$

where r is any of the indices $1, 2, \ldots, n$. To bring the significance of these relations more to the fore, we shall ground the subsequent developments on them, without using the relationship between H_i and the field Ω.

First we would like to note that the functional determinant H, which, as a consequence of its definition (5) is a whole homogeneous function of degree n with rational coefficients, is reproduced under multiplication; if K and L are formed from H in such a way that the coordinates h_i are replaced by dh_i and dH_i respectively, then

$$L = HK. \tag{14}$$

For, if one replaces the coordinates h_i by dh_i, then each homogeneous linear function[16]

$$\frac{\partial H_r}{\partial h_s} \quad \text{becomes} \quad d\left(\frac{\partial H_r}{\partial h_s}\right),$$

and therefore H becomes

$$K = \sum \pm d\left(\frac{\partial H_1}{\partial h_1}\right) d\left(\frac{\partial H_2}{\partial h_2}\right) \ldots d\left(\frac{\partial H_n}{\partial h_n}\right).$$

If, however, the coordinates h_i are substituted in the bilinear functions dH_i, then from (13)

$$\frac{\partial H_r}{\partial h_s} \quad \text{becomes} \quad \sum \frac{\partial}{\partial h_s}\left(\frac{\partial H_r}{\partial h_i}\right) dH_i = \sum \frac{\partial H_i}{\partial h_s} d\left(\frac{\partial H_r}{\partial h_i}\right),$$

and therefore H in $L = HK$, as was to be proved. This is the theorem on the norm of a product that has already been introduced above.

If φ is an arbitrary function of the coordinates h_i, and one defines the variation δ in such a way that

$$\delta\varphi = \sum \frac{\partial \varphi}{\partial H_i} h_i, \quad \text{and thus} \quad \delta H_i = h_i, \tag{15}$$

then it follows from (13), if one replaces d' by δ,

$$\sum dH_i \delta\left(\frac{\partial H_r}{\partial h_i}\right) = \sum h_i d\left(\frac{\partial H_i}{\partial h_i}\right) = dH_r,$$

since H_r is a homogeneous function of degree two. Hence

$$\delta\left(\frac{\partial H_r}{\partial h_s}\right) = 1 \quad \text{or} \quad = 0, \tag{16}$$

[16][The next term is incorrectly given as $\frac{\partial H_r}{\partial h_s}$ in Dedekind's *Werke*.]

depending on whether r and s are equal or not. From this it follows that the n variations δh_i are *constant rational numbers*. If further the variation δ' is defined by

$$\delta'\varphi = H\sum \frac{\partial\varphi}{\partial H_i}\delta h_i, \quad \text{and thus} \quad \delta' H_i = H\delta h_i, \tag{17}$$

it follows, if one substitutes d' by δ' in (13), that

$$\begin{aligned}\sum dH_i\delta'\left(\tfrac{\partial H_r}{\partial h_i}\right) &= H\sum \delta h_i d\left(\tfrac{\partial H_r}{\partial h_i}\right) = Hd\sum \tfrac{\partial H_r}{\partial h_i}\delta h_i \\ &= Hd\delta H_r = Hdh_r,\end{aligned}$$

and therefore

$$\delta'\left(\frac{\partial H_r}{\partial h_s}\right) = H\frac{\partial h_r}{\partial H_s}. \tag{18}$$

Now, the expression on the right side is the coefficient of the element

$$\frac{\partial H_s}{\partial h_r}$$

in the determinant H, and is therefore a *whole homogeneous function of degree* $(n-1)$ in the coordinates h_i with rational coefficients. So the same holds of the quantities

$$h'_r = \delta' h_r = H\sum \frac{\partial h_r}{\partial H_i}\delta h_i, \tag{19}$$

and conversely it follows from (18) that the coefficients of each and every one of the n^2 elements in the determinant H can be represented as a homogeneous linear function of the n quantities h'_i just defined. If φ is any function of the coordinates h_i, we will use φ' to denote the same function of the quantities h'_i. Then equation (18) reads

$$\frac{\partial H'_r}{\partial h'_s} = H\frac{\partial h_r}{\partial H_s}, \tag{20}$$

and from this

$$H' = H^{n-1}; \quad H\frac{\partial h'_s}{\partial H'_r} = \frac{\partial H_s}{\partial h_r} \tag{21}$$

follows as well.

Since H is a functional determinant, it is well-known[17]

$$d \log H = \sum \frac{\partial dH_i}{\partial H_i} - \sum \frac{\partial dh_i}{\partial h_i}.$$

Therefore, taking (13) into consideration, it follows that

$$\sum \frac{\partial \log H}{\partial h_i} dH_i = \sum \frac{\partial}{\partial H_{i'}} \left(\frac{\partial H_{i'}}{\partial h_i} \right) dH_i = \sum d \left(\frac{\partial H_{i'}}{\partial h_i} \right) \frac{\partial H_i}{\partial H_{i'}} = d \sum \frac{\partial H_i}{\partial h_i}.$$

If one then introduces the *homogeneous linear function*

$$S = \sum \frac{\partial H_i}{\partial h_i}, \tag{22}$$

then

$$\sum \frac{\partial \log H}{\partial h_i} dH_i = dS; \quad \frac{\partial \log H}{\partial h_r} = \frac{\partial S}{\partial H_r}. \tag{23}$$

Then, taking (20) into consideration,

$$\frac{\partial H}{\partial h_r} = H \sum \frac{\partial S}{\partial h_i} \frac{\partial h_i}{\partial H_r} = \sum \frac{\partial S}{\partial h_i} \frac{\partial H'_i}{\partial h'_r}.$$

If one then considers the *second degree homogeneous linear function*

$$T = \sum \frac{\partial S}{\partial h_i} H_i, \tag{24}$$

one has

$$\frac{\partial H}{\partial h_r} = \frac{\partial T'}{\partial h'_r}; \quad dH = \sum \frac{\partial T'}{\partial h'_i} dh_i. \tag{25}$$

[17] *Jacobi: De determinantibus functionalibus* §*9* (*Crelles* Journal XXII). The formula above takes into the consideration the case that the differentials dh_i are functions of the variables h_i. If one replaces d by δ',

$$\sum \frac{\partial h'_i}{\partial h_i} = 0$$

follows immediately from (17) and (19).

Hence the derivatives of the form H can also be represented as homogeneous linear functions in the quantities h' defined in (19); and, conversely, the latter in terms of the former. A further consequence of (20) is

$$\sum \frac{\partial H_i'}{\partial h_s'} \frac{\partial H_r}{\partial h_i} = H \quad \text{or} \quad = 0,$$

depending on whether or not r and s are equal. Multiplying by h_s' or dh_s' and summing with respect to s, we have

$$2 \sum H_i' \frac{\partial H_r}{\partial h_i} = H h_r'; \quad \sum dH_i' \frac{\partial H_r}{\partial h_i} = H dh_r',$$

and hence, differentiating,

$$h_r' dH - H dh_r' = 2 \sum H_i' d \left(\frac{\partial H_r}{\partial h_i} \right). \tag{26}$$

With the help of (25) and (26) one is also capable of forming higher-order differentials of H. In this way one finds

$$H dd' H - dH d' H = 2H \sum \frac{\partial H}{\partial h_i} dd' h_i - 2 \sum \frac{\partial^2 T}{\partial h_i \partial h_{i'}} H_i' dd' H_{i'}. \tag{27}$$

From the equation (26), with the help of (13), one can also obtain

$$h_r' dH - H dh_r' = \sum \frac{\partial H_i'}{\partial h_{i'}'} \frac{\partial H_r'}{\partial h_i'} dh_{i'}.$$

Then (26) also yields the functional determinant

$$\sum \pm \frac{\partial h_1'}{\partial h_1} \frac{\partial h_2'}{\partial h_2} \cdots \frac{\partial h_n'}{\partial h_n} = (-1)^{n-1} (n-1) H^{n-2} \tag{28}$$

and therefore from (25) the *Hessian* determinant of the form H, namely

$$\sum \pm \frac{\partial^2 H}{\partial h_1^2} \cdots \frac{\partial^2 H}{\partial h_n^2} = (-1)^{n-1} (n-1) H^{n-2} \sum \pm \frac{\partial^2 H}{\partial h_1^2} \cdots \frac{\partial^2 T}{\partial h_n^2}. \tag{29}$$

Equations (16), (22), (24), (25), (26), (27) immediately yield the following results concerning the variation δ:

$$\begin{gathered} \delta S = n; \delta T = S; h_r' \delta H - H \delta h_r' = 2 H_r'; \\ \delta H = S'; \delta' H = \delta H^2 - H \delta^2 H = 2T'. \end{gathered} \tag{30}$$

III. All these theorems are deduced from the assumption that the system of n whole homogeneous functions H_i of degree two satisfy condition (13), and that its functional determinant does not identically vanish. If one further introduces the assumption that the coefficients of these functions are rational numbers, and that the form H is *irreducible*, i.e. cannot be decomposed into factors of lower degree whose coefficients are also rational numbers, it can be proved that, conversely, that there is an algebraic number field Ω of the type considered above that belongs to this function system. For brevity we will introduce a symbol [Charakteristik] ε, which has the following meaning: if φ is any function of the coordinates h_i, and one replaces the latter by $h_i - \omega\delta h_i$, where ω for the moment is an *arbitrary* function, then φ is transformed into a new function, which will be denoted $\varepsilon(\varphi)$. From this definition

$$d\varepsilon(\varphi) = \varepsilon(d\varphi) - \varepsilon(\delta\varphi)d\omega \tag{31}$$

follows at once, under the assumption that the differential dh_i is *constant*. Hence one can define the function ω as the root of an equation of degree n

$$\varepsilon(H) = 0, \tag{32}$$

which, as a consequence of (16), agrees completely with equation (6). Thus one can prove that ω is a *whole* (homogeneous) function of the first degree, i.e. that $dd'\omega = 0$, if the differentials $dh_i, d'h_i$ are taken to be constant. In fact, by successive differentiation of identity (32) according to the rule given by (31), one has

$$\varepsilon(\delta H)d\omega = \varepsilon(dH) \tag{33}$$

and

$$\varepsilon(\delta H)^3 dd'\omega = \varepsilon(R), \tag{34}$$

where for brevity we set

$$\left\{ \begin{array}{c} \delta H^2 dd'H + \delta^2 H dH d'H \\ -\delta H dH d'\delta H - \delta H d'H d\delta H \end{array} \right\} = R,$$

a homogeneous function of degree $(3n-4)$. That this function R is divisible by H, or, in symbols, that $R \equiv 0$,[18] is obtained in the following way.

[18]This applies generally to the expression

$$d'Hd'''Hdd''H + dHd''Hd'd'''H - d'''HdHd'd''H - d'Hd''Hdd'''H.$$

From (30) it follows that

$$h'_r \delta H = 2H'_r + H\delta h'_r \equiv 2H'_r,$$

and, further, that

$$h'_r \delta^2 H = 2\delta H'_r + H\delta^2 h'_3 \equiv 2\delta H'_r.$$

Hence, eliminating h'_r,

$$\delta^2 H H'_r - \delta H \delta H'_r \equiv 0.$$

Since now, as a consequence of (27), $dHd'H - Hdd'H$ is a homogeneous linear function of the n quantities H'_i, it also follows that

$$\delta^2 H(dHd'H - Hdd'H) - \delta H \delta(dHd'H - Hdd'H) \equiv 0.$$

But the left side differs from R only in components that are divisible by H. Hence $R = PH$, where P is a whole function, and therefore $\varepsilon(R) = \varepsilon(P)\varepsilon(H) = 0$. Since, now, from the assumptions on H it is possible to prove that $\varepsilon(\delta H)$ does not identically vanish, from (34) the equation $dd'\omega = 0$ follows, i.e. the root ω of the equality (32) is a whole function of degree one. It goes without saying that it is homogeneous as well, since $H, \delta H, \ldots, \delta^{n-1}H$ and therefore also ω vanish concurrently with the coordinates h_i. If one now sets

$$\frac{\delta\omega}{\delta h_i} = \omega_i, \quad \omega = \sum h_i \omega_i, \tag{1}$$

then one obtains from (33) that

$$\sum \delta h_i \omega_i = \delta\omega = 1, \tag{35}$$

and

$$\varepsilon\left(\frac{\partial H}{\partial h_i}\right) = \varepsilon(\delta H)\omega_i. \tag{36}$$

Since, as a further consequence of (23), we have

$$\sum \frac{\partial H}{\partial h_i} dH_i = HdS \equiv 0$$

and

$$\varepsilon(dH_i) = dH_i - \omega d\delta H_i = dH_i - \omega dh_i,$$

it follows that

$$\begin{aligned} 0 &= \varepsilon(H)dS = \sum \varepsilon\left(\frac{\delta H}{\delta h_i}\right)\varepsilon(dH_i) \\ &= \varepsilon(\delta H)\sum \omega_i(dH_i - \omega dh_i). \end{aligned}$$

Hence

$$\omega d\omega = \sum dH_i\omega_i, \tag{3}$$

and thus also

$$\omega^2 = 2\sum H_i\omega_i, \tag{2}$$

whereby we have returned to our original assumptions. One can also prove — though we will not go into it here — that from the assumptions on H the *independence* of the n numbers ω_i follows.

Finally, we add to these developments the following easily proved remarks. The expanded form of the equality (32) or (6) is as follows:

$$0 = H - \delta H\frac{\omega}{1} + \delta^2 H\frac{\omega^2}{1\cdot 2} - \delta^3 H\frac{\omega^3}{1\cdot 2\cdot 3} + \ldots. \tag{37}$$

Furthermore, we have

$$H = \prod \omega = N(\omega) \tag{7}$$

where the product symbol $\prod$ includes all n roots ω. One finds as well (if one substitutes δ' for d in (3)) that

$$H = \omega\omega', \tag{8}$$

where

$$\omega' = \delta'\omega - \sum h_i'\omega_i \tag{38}$$

is adjunct to ω, and

$$S = \sum \omega, \quad 2T = \sum \omega^2, \tag{39}$$

where the summation symbol includes all n roots as well. The quadratic form T is characteristic of the number of real roots; if one further forms the *Hessian* determinant of the product $H = \prod\omega$, then, in combination with (29), one obtains the discriminant

$$\Delta(\omega_1, \omega_2, \ldots, \omega_n) = \sum \pm\frac{\partial^2 T}{\partial h_1^2}\cdots\frac{\partial^2 T}{\partial h_n^2}, \tag{40}$$

which also follows immediately from (39).

§160

The totality of *all* algebraic numbers also clearly constitutes a field.[19] In approaching the subject at hand, we now define a number α to be an *algebraic integer [ganze algbraische Zahl]* when it is the root of an equation with rational integer coefficients. Here we remark once and for all that by the *coefficients* of a function of degree m

$$F(x) = cx^m + c_1x^{m-1} + c_2x^{m-2} + \cdots + c_m,$$

or of an equation $F(x) = 0$, we invariably mean the m quotients

$$-\frac{c_1}{c}, +\frac{c_2}{c}, \ldots, (-1)^m\frac{c_m}{c}.$$

From this definition it follows first that a rational number is a rational integer if and only if it is an integer in the usual sense of the word (cf.§5, 4.). From now on we will call these *rational integers*, whereas we will call algebraic integers *integers* for short. With this assumed, we now turn to the proof of the following fundamental theorems.

1. *The sum, difference, and product of two integers α, β are again integers.*

If a and b are, respectively, the degrees of equations $\varphi(\alpha) = 0, \psi(\beta) = 0$, whose coefficients are rational integers, let $\omega_1, \omega_2, \ldots, \omega_n$ denote all ab products of the form $\alpha^{a'}\beta^{b'}$, where a' is any of the numbers $0, 1, 2, \ldots, (a-1)$, and b' is any of the numbers $0, 1, 2, \ldots, (b-1)$. Then if $\omega = \alpha + \beta$, or $= \alpha - \beta$, or $= \alpha\beta$, then with the help of the equations $\varphi(\alpha) = 0, \psi(\beta) = 0$, each of the products $\omega\omega_1, \omega\omega_2, \ldots \omega\omega_n$ can be brought into the form $r_1\omega_1 + r_2\omega_2 + \ldots + r_n\omega_n$, where $r_1, r_2, \ldots, r_n$ are rational integers. Eliminating the n quantities $\omega_1, \omega_2, \ldots, \omega_n$ from these equations, we obtain an equality of degree n involving ω (like (6) in §159) whose coefficients are rational integers, as was to be proved (cf. §139).

[19] To my knowledge it was Liouville who first proved that there are so-called *transcendental* numbers in addition to the algebraic ones (*Sur des classes très-étendues de quantités dont la valeur n'est ni algebrique, ni même réductible à des irrationelles algébrique*, Journ. de Math. T. XVI, 1851). It is conjectured that Ludolph's number π is such a transcendental number, but even just the special case that it is impossible to square the circle has to this day not yet been established. (Cf. *Euler: De relatione inter ternas pluresve quantitates instituenda.* §10, Opusc. anal. T. II, 1785.)

2. The integer α is said to be *divisible* by the integer β, or a *multiple* of β, if the quotient α/β is also an integer. Conversely, β is said to be a *divisor [Divisor oder Teiler]* of α (cf. §3). Similarly we write $\alpha \equiv \beta \pmod{\gamma}$ when $\alpha - \beta$ is divisible by γ, and say that α and β are *congruent with respect to the modulus* γ (cf. §17). One sees immediately (by 1.) that the theorems of §3 as well as those of §17 remain valid (for the moment, with the exception of 6. and 8.; cf. §164, 3).

3. *Each root ω of an equation whose coefficients are integers is again an integer.*

If ω is the root of an equation $F(\omega) = 0$ of degree m whose coefficients $\alpha, \beta, \ldots$ are integers, and, further, $a, b, \ldots$ are, respectively, the degrees of the equations $\varphi(\alpha) = 0, \psi(\beta) = 0, \ldots$ with rational coefficients, one forms all products of the form $\omega^{m'}\alpha^{a'}\beta^{b'}$, in which the integer exponents satisfy the conditions $0 \leq m' < m, 0 \leq \alpha' < a, 0 \leq \beta' < b, \ldots$. Then, by virtue of the equations $F(\omega) = 0, \varphi(\alpha) = 0, \psi(\beta) = 0, \ldots$ each of the n products $\omega\omega_1, \omega\omega_2, \ldots, \omega\omega_n$ can be brought into the form $r_1\omega_1 + r_2\omega_2 + \ldots + r_n\omega_n$, where $r_1, r_2, \ldots, r_n$ are rational integers. The theorem follows immediately from this.

Thus, e.g., if α is an integer, and r is any (whole or fractional) *positive* rational number, then α^r is an integer (cf. §5, 4.).

4. It is well-known that the concepts of divisibility and multiplicity of the rational integers transfer directly to rational integer functions, and there is an algorithm for finding the greatest common divisor $\varphi(x)$ of two given functions $F(x), f(x)$ which is fully analogous to the number-theoretic one (§4). If the coefficients of $F(x)$ and $f(x)$ are all contained in a field K, then the coefficients of $\varphi(x)$ will also be in K, since they are obtained by addition, multiplication, subtraction, and division of the coefficients of $F(x)$ and $f(x)$. From this it easily follows that if α is a root of such an equation $F(\alpha) = 0$ whose coefficients are numbers in the field K, then there must be such an equation $\varphi(\alpha) = 0$ of *lowest degree*, which is called *irreducible* in K and which clearly can have no roots that are not also roots of the equation $F(\alpha) = 0$. From this we have the theorem:

If α is an integer, and K is any given field, and $\varphi(\alpha) = 0$ is its irreducible equation in K, then all the coefficients of φ are integers.

For because α is an integer, it is the root of an equation $F(\alpha) = 0$ whose coefficients are rational integers, and therefore also numbers of the field K (§159). So the equation $\varphi(\alpha) = 0$, which is irreducible in K, and which is

satisfied by α, can only have integer roots. But the coefficients of such an equation are obtained from its roots via addition and multiplication, so (by 1.) the coefficients of the equation $\varphi(\alpha) = 0$ are also integers, as was to be proved.

The simplest case, in which K is the field of rational numbers, is found in Gauss.[20]

5. *If ρ is any algebraic number, there are always infinitely many (nonzero) rational integers h with the property that $h\rho$ is an integer. In fact, these numbers h are all rational multiples of the smallest such one.*

If ρ is an algebraic number, then it is the root of an equation of the form

$$c\rho^m + c_1\rho^{m-1} + c_2\rho^{m-2} + \ldots + c_m = 0$$

where $c, c_1, c_2, \ldots, c_m$ are rational integers. Multiplying by c^{m-1}, we have that $c\rho$ is an integer. If furthermore $a\rho, b\rho$ are integers, where a, b are rational integers whose greatest common divisor is $= h$, it follows easily (from 1. and §4) that $h\rho$ is also an integer. The theorem to be proved follows immediately from this.

6. By a *unit* we mean an integer ε which divides every integer. In particular it also divides 1, so $1 = \varepsilon\varepsilon'$, where ε' is an integer. If now ε satisfies the irreducible equation

$$\varepsilon^m + c_1\varepsilon^{m-1} + \ldots + c_m = 0$$

in the field of rational numbers, then (by 4.) c_m must be ± 1, since ε' satisfies the irreducible equation

$$c_m\varepsilon'^m + c_{m-1}\varepsilon'^{m-1} + \ldots + c_1\varepsilon' + 1 = 0.$$

Conversely, if this is the case, then ε divides 1 and therefore every integer, and so it is a unit. Clearly there are infinitely many units.

If α is divisible by α', and $\varepsilon, \varepsilon'$ are any units, then clearly $\varepsilon\alpha$ divides $\varepsilon'\alpha'$. With respect to divisibility the numbers $\varepsilon\alpha$, where ε ranges over units, behave just like α. We will call two integers whose quotient is not a unit *essentially different [wesentlich verschieden].*

7. If one tries to formulate the concept of a *prime number* by saying that it has no divisors essentially different from it and a unit, and is also not a unit

[20] D. A. [Disquisitiones Arithmeticae] art. 42

itself, one realizes at once that no such number exists. For, if α is an integer but not a unit, then α has infinitely many essentially different divisors, e.g. the numbers $\sqrt{\alpha}$, $\sqrt[3]{\alpha}$, $\sqrt[4]{\alpha}$ and so forth, which (by 3.) are integers.

In contrast, the concept of *relative primality* can be completely defined, and this question will actually show us the right path to take to drive forward in our investigation. Since *for the moment* we cannot speak of the greatest common divisor of two numbers (cf. §164, 3), it is impossible to formulate the definition of relative primality as it is put forward in the theory of rational numbers (§5). But several theorems followed from this definition, each of which, conversely, completely characterized the behavior of relatively prime numbers, without assuming knowledge of their divisors. One such theorem is e.g. the following (§7): if a, b are relatively prime numbers, then any number that is divisible by both a and b is divisible by ab. This theorem can in fact be turned around: if every number that is divisible by both a and b is divisible by ab as well, then a, b are relatively prime. For if the two numbers $a = ha', b = hb'$ had the common factor $h > 1$, then $ha'b'$ would be divisible by a and b, but not by ab.

These considerations lead us to put forward the following more general definition for the domain of algebraic integers:

Two nonzero integers α, β are said to be relatively prime if every number that is divisible by α and β is also divisible by $\alpha\beta$.

Right away we remark that two relatively prime numbers in the old sense of the phrase, i.e. two rational integers a, b whose greatest common divisor is equal to 1, remain relatively prime in the new sense. For if an algebraic integer γ is divisible by a and b, then the quotient $\rho = \gamma/ab$ is an algebraic number with the property that $a\rho$ and $b\rho$ are integers; thus (by 5.) ρ must also be an integer as well, and so γ is divisible by ab, as was to be proved. From the new definition it also goes without saying that two relatively prime numbers in the new sense of the word are also relatively prime numbers in the old sense.

We will further call the integers $\alpha, \beta, \gamma, \delta, \ldots$ relatively prime for short if each of them is relatively prime to each of the others (cf. §6). If then an integer ω is divisible by each of them, it is divisible by their product (cf. §7) because, as one easily sees, the following theorem (§5, 3.) also remains valid: if each of the numbers $\alpha', \beta', \gamma', \ldots$ is relatively prime to each of the numbers $\alpha'', \beta'', \gamma'', \delta'', \ldots$ then the products $\alpha'\beta'\gamma' \ldots$ and $\alpha''\beta''\gamma''\delta'' \ldots$ are relatively prime, and conversely.

But how should one determine whether or not two given integers α, β are relatively prime? One might attempt the following. Since α^{-1} and β^{-1} are algebraic numbers, there are always (by 5.) two smallest positive rational numbers a, b with the property that $a\alpha^{-1}$ and $b\beta^{-1}$ are integers, i.e. such that a, b are divisible, respectively, by α, β. If it turns out that a and b are relatively prime, then we know that α and β are relatively prime numbers. But one should not think that the converse holds, so that the *smallest rational multiples* a, b of two relatively prime numbers α, β must themselves be relatively prime. For example, the two conjugate numbers $\alpha = 2 + i$ and $\beta = 2 - i$ are relatively prime, and yet $a = b = 5$. An essential reduction in our task is, however, effected by the following theorem:

If two integers α, β satisfy the test for relative primality with respect to a field K to which they belong, i.e. if each number in K that is divisible by both α and β is also divisible by $\alpha\beta$, then α, β are in fact relatively prime.

For, if ω is any integer divisible by α and β, and if

$$\omega^m + \gamma_1\omega^{m-1} + \gamma_2\omega^{m-2} + \ldots + \gamma_m = 0$$

is the equation satisfied by ω that is irreducible in K, then (by 4.) the numbers $\gamma_1, \gamma_2, \ldots, \gamma_m$ are integers of K. Furthermore the integers $\alpha' = \omega/\alpha$ and $\beta' = \omega/\beta$ respectively satisfy equations

$$\begin{aligned} (\alpha\alpha')^m + \gamma_1(\alpha\alpha')^{m-1} + \ldots + \gamma_m &= 0 \\ (\beta\beta')^m + \gamma_1(\beta\beta')^{m-1} + \ldots + \gamma_m &= 0, \end{aligned}$$

it follows (by 4.) that the quotients γ_n/α^n and γ_n/β^n are also integers of the field K. Since, furthermore, by assumption, every number in K that is divisible by α and β is divisible by γ, it easily follows that each number γ_n in K, which is divisible by both α^n and β^n is also divisible by $\alpha^n\beta^n$, and so is of the form $\alpha^n\beta^n\gamma_n'$, where γ_n' is an integer. If one now sets $\omega = \alpha\beta\omega'$, then ω' satisfies the equation

$$\omega'^m + \gamma_1'\omega'^{m-1} + \ldots + \gamma_m' = 0,$$

in which the coefficients are integers. Hence (by 3.) ω' is an integer, i.e. ω is also divisible by $\alpha\beta$, as was to be proved.

From this it follows that in order to understand the behavior of two integers α, β with respect to each other, it suffices to consider the smallest field K to which they both belong. And it is easy to see that these fields are always of the kind we considered in the preceding section.

§161

So as not to interrupt the presentation later on, we now interpose some very general observations. This separate inquiry will be of great use to us in our subsequent topic of study, as well as for many others.

1. A system $\mathfrak{a}$ of real or complex numbers α, whose *sums* and *differences* themselves belong to $\mathfrak{a}$, will be called a *module*. When the difference of two numbers ω, ω' is contained in $\mathfrak{a}$, we will call them *congruent with respect to* $\mathfrak{a}$, and denote this with the congruence

$$\omega \equiv \omega' \pmod{\mathfrak{a}}.$$

Such congruences can be added and subtracted, and therefore also multiplied by an arbitrary rational integer, like equalities. Since any two numbers that are congruent to a third are congruent to one another, one can divide all the existing numbers into *classes* (mod $\mathfrak{a}$), such that any two congruent numbers are taken to be in the same class, and any two incongruent numbers are taken to be in different classes.

2. If all the numbers of a module $\mathfrak{a}$ are also numbers of a module $\mathfrak{d}$, then $\mathfrak{a}$ is called a *multiple* of $\mathfrak{d}$, and $\mathfrak{d}$ a *divisor* of $\mathfrak{a}$. Alternatively, we say $\mathfrak{d}$ *divides* $\mathfrak{a}$ *[gehe in* $\mathfrak{a}$ *auf]*, or $\mathfrak{a}$ *is divisible by* $\mathfrak{d}$. From any congruence $\omega \equiv \omega' \pmod{\mathfrak{a}}$ it follows that also $\omega \equiv \omega' \pmod{\mathfrak{d}}$. Clearly $\mathfrak{d}$ is comprised of either finitely or infinitely many classes (mod $\mathfrak{a}$).

If $\mathfrak{a}, \mathfrak{b}$ are any two modules, then all the numbers that are contained in both $\mathfrak{a}$ and in $\mathfrak{b}$ form the *least* common multiple $\mathfrak{m}$ of $\mathfrak{a}$ and $\mathfrak{b}$, since every common multiple of $\mathfrak{a}$ and $\mathfrak{b}$ is also divisible by the module $\mathfrak{m}$. If α runs through all the numbers of the module $\mathfrak{a}$, and β runs through all the numbers of the module $\mathfrak{b}$, then the numbers $\alpha + \beta$ form *greatest* common divisor of $\mathfrak{a}$ and $\mathfrak{b}$, since any common divisor of $\mathfrak{a}$ and $\mathfrak{b}$ divides the module $\mathfrak{d}$.

3. If the numbers $\omega_1, \omega_2, \ldots, \omega_n$ are given, then all the numbers of the form

$$\omega = h_1\omega_1 + h_2\omega_2 + \ldots + h_n\omega_n, \tag{1}$$

where $h_1, h_2, \ldots, h_n$ run through all the rational integers, comprise a *finite* module $\mathfrak{o}$. We will call the system [Komplex] of n numbers $\omega_1, \omega_2, \ldots, \omega_n$ a *basis* of the module $\mathfrak{o}$, whether they are dependent or independent from one another. Then the following theorem holds:

If all numbers ω of a finite module $\mathfrak{o}$ can be transformed into numbers of a finite module $\mathfrak{m}$ through multiplication by nonzero rational numbers, then $\mathfrak{o}$ contains only a finite number of incongruent numbers (mod $\mathfrak{m}$).

For, if we are given n nonzero rational numbers $r_1, r_2, \ldots, r_n$ with the property that the products $r_1\omega_1, r_2\omega_2, \ldots, r_n\omega_n$ are contained in $\mathfrak{m}$, then there is also a rational nonzero integer, s, with the property that all products $s\omega \equiv 0 \pmod{\mathfrak{m}}$. If one therefore lets each of the n rational integers $h_1, h_2, \ldots, h_n$ run through a complete residue system (mod s), then s^n numbers of the form (1) arise, and each number of the module $\mathfrak{o}$ is itself congruent to at least one of these (mod $\mathfrak{m}$). Hence the number of elements of $\mathfrak{o}$ that are incongruent with respect to $\mathfrak{m}$ is not more than s^n, as was to be proved.

It is, however, important to determine the number of incongruent elements *exactly*. To that end we consider the smallest common multiple $\mathfrak{a}$ of the two modules $\mathfrak{o}$ and $\mathfrak{m}$. Since any two numbers ω, ω' of the module $\mathfrak{o}$ that are congruent with respect to $\mathfrak{m}$ are also congruent with respect to $\mathfrak{a}$, and conversely, then our task is that of determining the number of classes (mod $\mathfrak{a}$), of which $\mathfrak{o}$ is comprised. Hence we initially try to determine the general form of all the numbers

$$\alpha = k_1\omega_1 + k_2\omega_2 + \ldots + k_n\omega_n \tag{2}$$

in $\mathfrak{a}$, where $k_1, k_2, \ldots, k_n$ are all rational integers. If now r is any given index from the sequence $1, 2, \ldots, n$, then among all numbers $\alpha = \theta_r$ in which $k_{r+1} = 0, k_{r+2} = 0, \ldots, k_n = 0$, there are some in which k_r is nonzero (e.g., $s\omega_r$). Among these, let

$$\alpha_r = \alpha_1^{(r)}\omega_1 + \alpha_2^{(r)}\omega_2 + \ldots + a_r^{(r)}\omega_r \tag{3}$$

be one in which k_r has the *smallest* positive value $a_r^{(r)}$. Then it is clear that the value of k_r in each number θ_r is divisible by $a_r^{(r)}$, and so of the form $a_r^{(r)}x_r$, where x_r is a rational integer. It is therefore clear that $\theta_r - x_r\alpha_r = \theta_{r-1}$ is a number α, in which $k_r, k_{r+1}, \ldots, k_n$ vanish. From this it follows immediately that after one has determined for each index r a particular such α_r of the module $\mathfrak{a}$,[21] we know that each number α can be brought to the form

$$\alpha = x_1\alpha_1 + x_2\alpha_2 + \ldots + x_n\alpha_n, \tag{4}$$

[21]The system of these n particular numbers is completely determined if one adds the conditions that $0 \leq a_r^{(r')} < a_r^{(r)}$ should hold, when $r' > r$.

where $x_1, x_2, \ldots, x_n$ are rational integers. The numbers $k_1, k_2, \ldots, k_n$ appearing in expression (2) are obtained from these using the equations

$$k_r = a_r^{(r)} x_r + a_r^{(r+1)} x_{r+1} + \ldots + a_r^{(n)} x_n. \tag{5}$$

Conversely, all numbers α of the form (4) are contained in $\mathfrak{a}$.

If now a number ω of the form (1) is given, so $h_1, h_2, \ldots, h_n$ are given rational integers, then *all* numbers ω' of the module $\mathfrak{o}$ that are congruent to it with respect to $\mathfrak{m}$, and which thus form a class (mod $\mathfrak{a}$), are of the form

$$\omega' = \omega + \alpha = h_1' \omega_1 + h_2' \omega_2 + \ldots + h_n' \omega_n, \tag{6}$$

where, as a consequence of (5),

$$h_r' = h_1 + a_r^{(r)} x_r + a_r^{(r+1)} x_{r+1} + \ldots a_r^{(n)} x_n.$$

From this it follows that one can always successively determine the arbitrary rational integers $x_n, x_{n-1}, \ldots, x_2, x_1$, and in a unique way, so that the n numbers h_r' satisfy the conditions

$$0 \leq h_r' < a_r^{(r)}. \tag{7}$$

Hence in each class there exists one and only one *representative* ω' of the form (6) which satisfies this condition (7). Hence the *number* of different classes (mod $\mathfrak{a}$) of which the module $\mathfrak{o}$ consists is equal to the product $a_1' a_2'' \ldots a_n^{(n)}$, i.e. equal to the *determinant* of the system of coefficients of the n particular numbers α_r of the form (3), which form a basis of $\mathfrak{a}$.[22]

§162

From now on we will restrict our attention to the study of integers contained in a finite field Ω (§159).

1. Since each algebraic number (by §160, 5.) can be transformed into an integer through multiplication by a nonzero rational integer, we may assume

[22] The further development of the general theory of modules would lead us too far astray here (cf. §163). We mention only the following theorem: if the basis numbers of a finite module are dependent on one another, then there is always a basis of the same module consisting of independent numbers. The most elegant method of finding the new basis consists of a generalization of the method of handling partial determinants applied by *Gauss* (D.A. art. 234, 236, 279).

that the numbers $\omega_1, \omega_2, \ldots, \omega_n$ which form a basis of the field Ω are all integers. Then we know (by §160, 1.) that each number

$$\omega = \sum h_i \omega_i \tag{1}$$

is an integer, assuming all the coordinates h_i are rational integers. But the converse does not hold in general, i.e. ω may well be an integer even if some or all of its coordinates are fractions. This is one of the most important points of the theory, and must therefore be clarified from the start.

First, we make the evident remark that the discriminant [§159, (10)] of any system of n independent integers is known to be a nonzero rational number. In fact it is an *integer*, since it is obtained from the addition, subtraction, and multiplication of other integers. Suppose now there is actually an integer

$$\beta = \frac{\sum k_i \omega_i}{s}, \tag{2}$$

in Ω, where $s, k_1, k_2, \ldots, k_n$ are rational integers with no common divisor; in particular, $s > 1$. We assert that s^2 divides the discriminant $\Delta(\omega_1, \omega_2, \ldots, \omega_n)$, and that one can find a new basis of integers $\beta_1, \beta_2, \ldots, \beta_n$, whose discriminant is less than $\Delta(\omega_1, \omega_2, \ldots, \omega_n)$ in absolute value.

To prove this, we let $\mathfrak{m}$ denote the module consisting of all integers that are divisible by s, and we let $\mathfrak{o}$ denote the system of all numbers ω of the form (1), whose coordinates are *integers*. Since each product $s\omega$ is an element of $\mathfrak{m}$, we can apply the general investigation of the preceding section to the case at hand. All the numbers α in $\mathfrak{o}$ that are divisible by s are thus of the form

$$\alpha = \sum x_i \alpha_i = s \sum x_i \beta_i,$$

where the n numbers $\alpha_i = s\beta_i$ are particular numbers α, the β_i are thus *integers* of the field Ω, and the x_i are arbitrary rational integers.

Since now every number $s\omega$ is such a number α, one can set

$$\omega_r = \sum b_i^{(r)} \beta_i, \quad \Delta(\omega_1, \omega_2, \ldots, \omega_m) = b^2 \Delta(\beta_1, \beta_2, \ldots, \beta_n),$$

where the coefficients $b_i^{(r)}$ are rational integers, and b is the determinant they comprise. Conversely it follows that the n products $b\beta_i$ are *numbers of the system* $\mathfrak{o}$, and hence all the quotients $b\alpha/s$.

We now apply this result to assumption (2), that β is an integer, and so its numerator $\sum k_i \omega_i$ is a number of the form α, although the numbers

$s, k_1, k_2, \ldots, k_n$ have no common divisor. It follows directly that b *is divisible by* s, whereby at the same time the above assertion is proved.

Now since the discriminant of each system of n independent integers of the field Ω is a nonzero rational integer, there is one of these discriminants whose value — disregarding the sign — is *minimum*. From the previous investigation it follows directly that if a basis consists of numbers $\omega_1, \omega_2, \ldots, \omega_n$ for which the discriminant takes on this minimum value, the corresponding coordinates h_i of each integer ω of the field must necessarily be a rational integer. We will call such a basis $\omega_1, \omega_2, \ldots, \omega_n$ an *integral basis [Grundreihe]* of the field Ω. Other integral bases of the same field are obtained from it if one chooses n integers ω of the form (1) in such a way that the n^2 associated coordinates form a determinant $= \pm 1$.

The minimal discriminant itself plays an important role, both with respect to the inner[23] constitution of the field Ω, as well as with respect to its relationship to other fields.[24] We will therefore call this positive or negative rational integer the *ground number* [*Grundzahl*] or the *discriminant of the field* Ω, and denote it by $\Delta(\Omega)$. Clearly it is identical to the ground number of each of the fields conjugate with Ω.[25]

The numbers of a quadratic field, e.g., are of the form $t + u\sqrt{D}$, where t, u run through the rational integers and D is a rational integer which is neither square nor divisible by a square other than 1. If $D \equiv 1 \pmod 4$ then the numbers 1 and $\frac{1}{2}(1 + \sqrt{D})$ form an integral basis of the field, and its discriminant is $= D$. If on the other hand $D \equiv 2$ or $\equiv 3 \pmod 4$ the numbers 1 and $\sqrt{D}$ form an integral basis of the field, and its discriminant is $= 4D$.

If, furthermore, θ is a primitive root of the equation $\theta^m = 1$ (§139), where $m > 2$, then the numbers $1, \theta, \theta^2, \ldots, \theta^{n-1}$ form an integral basis of the field

[23]Cf. *Kronecker: Über die algebraisch auflösbaren Gleichungen* (Monatsbericht der Berliner Ak. 14. April 1856).

[24]The first hint of this relationship can be seen in an elegant inquiry by *Kronecker* (*Mémoir sur les facteurs irréductibles de l'expression* $x^n - 1$; Journ. de Math., p. p. Liouville; T. XIX, 1854). In order to indicate the character of these laws, whose development I will save for another occasion, I will put forth only the simplest example: the least common multiple of two distinct quadratic fields A, B is a biquadratic field K, which has yet a third quadratic C as a divisor; the ground number of K is exactly the product of the ground numbers of A, B, C, and therefore a perfect square.

[25][To conform with modern usage, I will henceforth use the terms *discriminant* and *integral basis* wherever Dedekind uses *Grundzahl* and *Grundreihe*, respectively.]

of degree $n = \varphi(m)$, whose discriminant is

$$\left(\frac{m\sqrt{-1}}{\sqrt[a-1]{a}\,\sqrt[b-1]{b}\,\sqrt[c-1]{c}\ldots} \right)^n$$

where $a, b, c \ldots$ are all the different prime numbers that divide m. If $m = 3$ (or $= 6$), then this field is a quadratic field, with discriminant $= -3$. If $m = 4$, the discriminant of the quadratic field is $= -4$.

2. From the preceding principles we easily have the following fundamental theorem:

If μ is a nonzero integer of the field Ω, then the number of integers of the field that are incongruent with respect to μ is equal to the absolute value of the norm of the modulus μ.

Let $\mathfrak{m}$ be the system of all integers that are divisible by μ (so $\mathfrak{m}$ is closed under addition and subtraction). Let $\mathfrak{o}$ be the system of *all* integers of the field Ω, i.e. all numbers ω of the form (1), where the numbers ω_i form an integral basis of the field and the coordinates h_i are any rational integers. Since each quotient ω/μ (by §160, 5.) can be transformed into an integer through multiplication by a nonzero rational integer, the investigations of the preceding section apply to the case at hand. Hence all the numbers α of the system $\mathfrak{o}$ that are divisible by μ are of the form

$$\alpha = \sum x_i \alpha_i = \mu \sum x_i \beta_i,$$

where the n numbers $\alpha_i = \mu\beta_i$ are particular such numbers α, and so the numbers β_i are in $\mathfrak{o}$; and the quantities x_i can take on any rational integer value. The number of *classes* into which the system decomposes with respect to the modulus μ is further equal to the determinant a consisting of the coordinates of the n numbers $\alpha_1, \alpha_2, \ldots, \alpha_n$. This is equal (from §159, (11), (12)) to

$$\Delta(\alpha_1 \ldots \alpha_n) = a^2 \Delta(\Omega) = N(\mu)^2 \Delta(\beta_1 \ldots \beta_n).$$

Since each of number α of the system $\mathfrak{o}$ that is divisible by μ is of the form $\alpha = \mu\omega$, and thus of the form $\mu \sum x_i \beta_i$, each number ω of the system $\mathfrak{o}$ is also of the form $\sum x_i \beta_i$. Hence the numbers β_i also form an integral basis of the field, and it follows that $\Delta(\beta_1 \ldots \beta_n) = \Delta(\Omega)$. So $a = \pm N(\mu)$, as was to be proved.

At the same time it is clear that, by the methods of the preceding section, one can establish a system of a incongruent representatives of the different classes, which is therefore a *complete residue system for the module* μ.[26]

3. If one now wants to test whether two given integers θ, μ are relatively prime, one clearly only has to run through a complete system of residues (mod μ), and determine how often $\theta\omega \equiv 0 \pmod{\mu}$. If it turns out that this happens only when $\omega \equiv 0 \pmod{\mu}$, then each integer $\theta\omega$ that is divisible by θ and μ is also divisible by $\theta\mu$, whereby θ, μ are relatively prime. If, however, the congruence $\theta\omega \equiv 0 \pmod{\mu}$ also has a root ω which is not $\equiv 0 \pmod{\mu}$, then the corresponding number $\theta\omega$ is divisible by θ and μ, but not by $\theta\mu$, whereby θ, μ are not relatively prime.

If θ is relatively prime to μ (e.g. $\theta = 1$), then $\theta\omega$ runs through a complete residue system (mod μ) concurrently with ω. It follows that each congruence $\theta\omega = \theta' \pmod{\mu}$ always has exactly one root ω (cf. §22). If furthermore $\psi(\mu)$ is the number of classes whose numbers are relatively prime to the modulus μ, then $\theta\omega$ runs through the representatives of these classes concurrently with ω. Since the product of these numbers ω are also relatively prime to μ, we have the theorem

$$\theta^{\psi(\mu)} \equiv 1 \pmod{\mu},$$

to which *Fermat*'s theorem corresponds (§19).

4. If one pursues this analogy with the theory of rational numbers further, then the question as to the composition of numbers of the system $\mathfrak{o}$ (that is, the integers of the field Ω) from factors that again belong to $\mathfrak{o}$ forces itself upon us again and again. Right away it becomes clear that the unlimited factorizability of integers which is possible in the infinite field of *all* algebraic numbers (§160, 7.) disappears in finite fields Ω. But a very peculiar property crops up for infinitely many such fields Ω, one that has already (§16) been remarked upon in passing.[27] A number in $\mathfrak{o}$ is called *decomposable* when it

[26] If the n numbers ω_i are *any* basis of the field Ω, and if $\mathfrak{o}$ is the system of all numbers ω of the form (1) whose coordinates are *integers*, then the system of numbers of $\mathfrak{o}$ is closed under addition and subtraction. If one further requires that it is closed under multiplication, it follows at the same time that they are *integers*. If one calls two numbers ω, ω' congruent with respect to a third such number μ if and only if the quotient $(\omega - \omega')/\mu$ is again a number of the system $\mathfrak{o}$, then the the number of elements of $\mathfrak{o}$ that are incongruent with respect to μ is always $= \pm N(\mu)$. Cf. §165, 4.

[27] The example there does not fit here exactly, insofar as the integers of the quadratic field corresponding to the equation $\rho^2 = -1$ are not of exhausted by those of the form $t + u\rho$, but, rather, by the form $t + u\theta$, where $2\theta = 1 + \rho$. The numbers $3, 5, 2 + \rho, 2 - \rho$ are in

is the product of two numbers in $\mathfrak{o}$, neither of which is a unit; and *indecomposable* when this is not the case. Clearly every decomposable number μ is representable as a product of a finite number of indecomposable elements (cf. §8), since the norm of μ is equal to the product of the norms of the individual factors (§159). But it frequently occurs that this decomposition is not totally determined, but rather there exist several *essentially different* compositions of the same number into indecomposable factors (§160, 6). This contradicts so many notions governing the character of prime numbers (§8) that we therefore can no longer recognize indecomposable numbers as prime. In order to preserve the character of primes we therefore search for a criterion to characterize them that is more robust that the inadequate criterion of indecomposability. Just as we did earlier with the concept of relative primality (§160, 7), rather than decomposing the number μ under consideration, we will consider its behavior as a *modulus*:

An integer μ, which is not a unit, will be called a prime number *if every product $\eta\rho$ that is divisible by μ, has at least one factor η or ρ that is divisible by μ.*

It then follows immediately that the highest power of a prime number μ that divides a product is the product of the highest powers of μ that divide the individual factors, and that any number that is not divisible by μ is relatively prime to μ. One easily sees further that the smallest rational integer p divisible by μ is necessarily a prime number (in the field of rational numbers), and therefore the norm of μ is a power of p, since it must be a rational divisor of $N(p) = p^n$. We will therefore know that we have discovered all the prime numbers of a field Ω when we have considered the divisors of all rational prime numbers p.

5. If however μ is not a prime number (and is also not a unit), there exist two numbers η, ρ which are not divisible by μ, whose product $\eta\rho$ is divisible by μ. So, we will aim for a factorization of μ into actual or *ideal*, i.e. fictional factors. If, in particular, there is in $\mathfrak{o}$ a greatest common divisor of the pair of numbers η and $\mu = \nu\mu'$, with the property that the quotients η/ν and μ/ν are relatively prime, then μ decomposes into the factors ν and μ', neither of which is a unit, because neither ρ nor η is divisible by μ. The

fact decomposable: $3 = \theta(1-\theta), 5 = (1+\theta)(2-\theta), 2-\rho = -\theta(1+\theta), 2+\rho = -(1-\theta)(2-\theta)$. The four numbers $\theta, 1-\theta, 1+\theta, 2-\theta$ are prime numbers in this field. The phenomenon under consideration, however, really does occur in the quadratic field corresponding to the equation $\kappa^2 = -5$, in the example $3 \cdot 5 = (1+2\kappa)(1-2\kappa)$ (cf. §21; the pair of numbers $3, 7$ are not representable by the principal form of determinant -5).

factor μ' is essentially determined by the property that all the roots α' of the congruence $\eta\alpha' \equiv 0 \pmod{\mu}$ are divisible by μ' (e.g. also $\alpha' = \rho$), and that moreover each number α' that is divisible by μ' also satisfies the preceding congruence. Conversely, if there is in $\mathfrak{o}$ a number μ' which divides all the roots α' of the congruence $\eta\alpha' \equiv 0 \pmod{\mu}$, and only these, then μ is also divisible by μ', and the quotient $\nu = \mu/\mu'$ is the greatest common divisor of the pair of numbers η and μ.

But it can well be the case that there is no such number μ' to be found in $\mathfrak{o}$. This is the phenomenon that *Kummer* confronted (with respect to numbers formed from roots of unity). He came upon the fortunate idea of nonetheless feigning [fingieren] such numbers μ' and introducing them as *ideal* numbers. The *divisibility* of a number α' by these ideal numbers μ' depends entirely on whether α' is a root of the congruence $\eta\alpha' \equiv 0 \pmod{\mu}$, and consequently these ideal numbers are only treated as moduli; so there are absolutely no problems with this manner of introducing them. The only misgiving is that the immediate transfer of the usual concepts of the *actual* numbers can, initially, easily evoke mistrust of the certainty of the proof. This has caused us to inquire after a means of clothing the theory in a different garb, so that we always consider *systems* of actual numbers.

§163

We ground the theory of the numbers of $\mathfrak{o}$, i.e. all the integers of the field Ω, on the following new concept.

1. A system $\mathfrak{a}$ of infinitely many numbers contained in $\mathfrak{o}$ will be called an *ideal* if it satisfies the following pair of conditions:

I. The sum and difference of any two numbers in $\mathfrak{a}$ is again a number in $\mathfrak{a}$.

II. Each product of a number in $\mathfrak{a}$ and a number in $\mathfrak{o}$ is again a number in $\mathfrak{a}$.

If α is contained in $\mathfrak{a}$, we will say that α is *divisible by* $\mathfrak{a}$, and that $\mathfrak{a}$ *divides* α, since this manner of expression will prove convenient. We further call two numbers ω, ω' contained in $\mathfrak{o}$ whose difference is in $\mathfrak{a}$ *congruent with respect to* $\mathfrak{a}$ (cf. §161), and denote this with the congruence $\omega \equiv \omega' \pmod{\mathfrak{a}}$. These congruences can be added and subtracted (by I), and multiplied (by II), as equations. Since each of two numbers congruent to a third are also congruent to one another, one can divide all numbers into *classes* $\pmod{\mathfrak{a}}$ in such a way that any two congruent numbers are put in the same class and any

two incongruent numbers are put in different classes. Now, if μ is a nonzero number in $\mathfrak{a}$, any two numbers that are congruent with respect to μ are also congruent with respect to $\mathfrak{a}$ (by II). It thereby follows immediately that $\mathfrak{a}$ consists of one or more classes (mod μ), and so (by §162, 2) $\mathfrak{o}$ decomposes into finitely many classes (mod $\mathfrak{a}$).[28] If one chooses a representative from each class, these form a *complete system of residues* (mod $\mathfrak{a}$); the number of such classes or incongruent numbers will be called the *norm* of $\mathfrak{a}$ and will be denoted $N(\mathfrak{a})$.

If η is a nonzero number in $\mathfrak{o}$, then the numbers in $\mathfrak{o}$ that are divisible by η form an ideal, which will be denoted $\mathfrak{i}(\eta)$. Such ideals are distinguished especially and are called *principal ideals [Hauptideale];* the norm of $\mathfrak{i}(\eta)$ is $= \pm N(\eta)$. If η is a unit, then $\mathfrak{i}(\eta) = \mathfrak{o}$, and conversely.

2. If every number of an ideal $\mathfrak{a}$ is also in an ideal $\mathfrak{d}$, then clearly $\mathfrak{d}$ consists of one or more classes $\mathfrak{a}$, and we will say that $\mathfrak{a}$ is a *multiple of* $\mathfrak{d}$ or is *divisible by* $\mathfrak{d}$; and that $\mathfrak{d}$ *is a divisor of* $\mathfrak{a}$, or $\mathfrak{d}$ *divides* $\mathfrak{a}$.

If $\mathfrak{d}$ consists of r classes (mod $\mathfrak{a}$), then $N(\mathfrak{a}) = rN(\mathfrak{d})$. In particular, if δ runs through the representatives of these r classes and γ is a complete system of residues (mod $\mathfrak{d}$), then the $rN(\mathfrak{d})$ numbers $\gamma + \delta$ form a complete system of residues (mod $\mathfrak{a}$). For, first of all, each number in $\mathfrak{o}$ is congruent to a number γ (mod $\mathfrak{d}$), and so $\equiv \gamma + \delta$ (mod $\mathfrak{a}$); and second, if γ', δ' have denotations similar to those of γ, δ, from $\gamma + \delta = \gamma' + \delta'$ (mod $\mathfrak{a}$) it follows successively that $\gamma + \delta \equiv \gamma' + \delta'$ (mod $\mathfrak{d}$), $\gamma \equiv \gamma'$ (mod $\mathfrak{d}$), $\gamma = \gamma'$, and so $\delta \equiv \delta'$, $\delta = \delta'$. In other words, the numbers $\gamma + \delta$ are all incongruent (mod $\mathfrak{a}$).

It follows that each ideal has only finitely many divisors. If $\mathfrak{m}$ is divisible by $\mathfrak{a}$, and $\mathfrak{a}$ by $\mathfrak{d}$, then $\mathfrak{m}$ is also divisible by $\mathfrak{d}$. The principal ideal $\mathfrak{o}$ itself divides each ideal, and is at the same time the *unit* ideal, which contains 1 and more generally every unit, and whose norm is $= 1$.

The system of those numbers that are contained in each of two ideals $\mathfrak{a}, \mathfrak{b}$ is the *least common multiple* $\mathfrak{m}$ of $\mathfrak{a}, \mathfrak{b}$, insofar as every common multiple of $\mathfrak{a}, \mathfrak{b}$ is divisible by the ideal $\mathfrak{m}$. If α runs through all the numbers of $\mathfrak{a}$, and β runs through all the numbers of $\mathfrak{b}$, then the system of all numbers $\alpha + \beta$ is the *greatest common divisor* $\mathfrak{d}$ of the ideals $\mathfrak{a}, \mathfrak{b}$, since each common divisor of $\mathfrak{a}, \mathfrak{b}$ divides the ideal $\mathfrak{d}$.[29]

[28] This follows immediately from §161; if, in particular, ω is any number in $\mathfrak{o}$, then one can multiply the quotient ω/μ by a nonzero rational integer to obtain an integer, so that ω (by II) is transformed into a number of the ideal $\mathfrak{a}$.

[29] The extension of these definitions of $\mathfrak{m}$ and $\mathfrak{d}$ to more than two ideals $\mathfrak{a}, \mathfrak{b}, \ldots$ is

If r is the number of elements of $\mathfrak{b}$ which are incongruent (mod $\mathfrak{a}$), then $\mathfrak{b}$ consists of r classes (mod $\mathfrak{m}$), and $\mathfrak{d}$ consists of r classes (mod $\mathfrak{a}$). So $N(\mathfrak{m}) = rN(\mathfrak{b})$, $N(\mathfrak{a}) = rN(\mathfrak{d})$, and $N(\mathfrak{m})N(\mathfrak{d}) = N(\mathfrak{a})N(\mathfrak{b})$.

If $\mathfrak{b}$ is a principal ideal $\mathfrak{i}(\eta)$, then there are r numbers $\beta = \eta\omega$ in $\mathfrak{b}$ that are incongruent (mod $\mathfrak{a}$). At the same time, r is also the norm of the ideal $\mathfrak{r}$ consisting of all roots ρ of the congruence $\eta\rho \equiv 0$ (mod $\mathfrak{a}$), because two numbers ω, ω' are congruent (mod $\mathfrak{r}$) if and only if $\eta\omega \equiv \eta\omega'$ (mod $\mathfrak{a}$). Hence, in this case $N(\mathfrak{a}) = N(\mathfrak{r})N(\mathfrak{d})$.

3. An ideal $\mathfrak{p}$ distinct from $\mathfrak{o}$ which has no divisor other than $\mathfrak{o}$ and $\mathfrak{p}$ is called a *prime ideal*. We have the following theorem:

If $\eta\rho \equiv 0$ (mod $\mathfrak{p}$), then at least one of the two numbers η, ρ is divisible by $\mathfrak{p}$. In particular, if η is not $\equiv 0$ (mod $\mathfrak{p}$), then the roots ρ of the congruence $\eta\rho \equiv 0$ (mod $\mathfrak{p}$) clearly form an ideal which divides $\mathfrak{p}$, and which, since it does not contain the number 1, is distinct from $\mathfrak{o}$. It follows that this ideal is equal to $\mathfrak{p}$, as was to be proved.

This theorem characterizes the prime ideals, since the following converse holds: *If every product which is divisible by an ideal $\mathfrak{p}$ (which is distinct from $\mathfrak{o}$) has at least one factor that is divisible by $\mathfrak{p}$, then $\mathfrak{p}$ is a prime ideal.* For, if $\mathfrak{q}$ is a divisor of $\mathfrak{p}$ that is different from $\mathfrak{p}$, then there is a number ω in $\mathfrak{q}$ that is not in $\mathfrak{p}$; then (by assumption) no power $\omega^2, \omega^3, \ldots$ is divisible by $\mathfrak{p}$. Since there exist only finitely many incongruent numbers (mod $\mathfrak{p}$), there must in particular be two *distinct* exponents m and $m + s > m$ satisfying $\omega^{m+s} \equiv \omega^m$ (mod $\mathfrak{p}$), so the product $\omega^m(\omega^s - 1)$ is divisible by $\mathfrak{p}$. Since now ω^m is not divisible by $\mathfrak{p}$, then (by the assumption) the other factor $\omega^s - 1$ must be divisible by $\mathfrak{p}$, and therefore is also divisible by $\mathfrak{q}$. Then ω, and, since $s > 0$, also ω^s, are $\equiv 0$ (mod $\mathfrak{q}$). Thus the number 1 is also in $\mathfrak{q}$, and so $\mathfrak{q} = \mathfrak{o}$, as was to be proved.

If we call an ideal distinct from $\mathfrak{o}$ *composite [zusammengesezt]* when it is not a prime ideal, we can also express this theorem in the following way: *If $\mathfrak{a}$ is a composite ideal, then there are two numbers η, ρ, not divisible by $\mathfrak{a}$, whose product $\eta\rho$ is divisible by $\mathfrak{a}$.* We prove it for a second time in the following manner. Let $\mathfrak{e}$ be a divisor of $\mathfrak{a}$ which is distinct from $\mathfrak{o}$. Then there is in $\mathfrak{e}$ a number η that is not divisible by $\mathfrak{a}$, and the greatest common divisor $\mathfrak{d}$ of $\mathfrak{a}$ and $\mathfrak{i}(\eta)$ is divisible by $\mathfrak{e}$. So it is distinct from $\mathfrak{o}$, whereby $N(\mathfrak{d}) > 1$. The ideal $\mathfrak{r}$ consisting of all of the roots ρ of the congruence $\eta\rho \equiv 0$ (mod $\mathfrak{a}$) is a divisor of $\mathfrak{a}$, and so (by 2.) $N(\mathfrak{a}) = N(\mathfrak{r})N(\mathfrak{d}) > N(\mathfrak{r})$. So $\mathfrak{r}$ is distinct

immediate.

from $\mathfrak{a}$ and therefore has a number ρ that is not divisible by $\mathfrak{a}$, as was to be proved.

It is now clear that the smallest (nonzero) rational number p, which is contained in the prime ideal $\mathfrak{p}$, is necessarily a *prime* number (in the field of rationals); and further $\mathfrak{p}$ divides $\mathfrak{i}(p)$, so $N(\mathfrak{p})$ is a divisor of $N(p) = p^n$, and so also a power p^f of the prime p. One easily finds (cf. §162, 3.) that every number ω in $\mathfrak{o}$ satisfies the congruence[30]

$$\omega^{p^f} \equiv \omega \pmod{\mathfrak{p}}.$$

The general theorems of §§26, 27, 29, 30, 31 on congruences with respect to the modulus $\mathfrak{p}$ also carry over without difficulty.

If the least common multiple $\mathfrak{m}$ *of ideals* $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$ *is divisible by the prime ideal* $\mathfrak{p}$*, then* $\mathfrak{p}$ *divides at least one of the ideals* $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$. For if none of these ideals is divisible by $\mathfrak{p}$, there are numbers $\alpha, \beta, \gamma, \ldots$ in $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$ respectively

[30]This is the basis of the overlap with the *theory of higher congruences*(cf. §26), which serves in determining the prime ideals. This was first carried out in the study of fields of degree $n = \varphi(m)$ which arise from a primitive root of the equation $\theta^m = 1$, indeed by *Kummer*, the creator of the theory of ideal numbers. A complete account of the portion of his inquiry that is relevant here can be found in the works *Mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers* (Journ. de Math. p. p. Liouville, T. XVI, 1851). – *Theorie der idealen Primfaktoren der komplexen Zahlen, welche aus den Wurzel der Gleichung* $\omega^n = 1$ *gebildet sind, wenn n eine zusammengesetzte Zahl ist* (Abh. der Berliner Ak. 1856). The main result follows more easily from our theory and in our manner of presentation is expressed as follows: if p is a rational prime number and m' is the largest divisor of $m = p'm'$ that is not divisible by p, p further *belongs* to the exponent $f \pmod{m'}$, where $\varphi(m') = ef$ (§28). So $\mathfrak{i}(p) = (\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_e)^{\varphi(p')}$, where $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_e$ are prime ideals distinct from one another, whose norms are $= pf$. If $p' > 1$, then $\mathfrak{i}(1 - \theta^{m'}) = \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_e$.

For complex numbers of higher degree cf. *Kummer: Über die allgemeinen Reziprozitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist* (Abh. der Berliner Ak. 1859).

For those fields Ω, whose conjugate fields are equal to to Ω, and which I call *Galois fields*, cf. *Selling: Über die idealen Primfaktoren der komplexen Zahlen, welche aus den Wurzeln einer beliebigen irreduktibelen Gleichung rational gebildet sind* (*Schlömlichs* Zeitschrift für Math. u. Phys, Bd. 10. 1865).

The special case of biquadratic fields is completely carried out by *Bachmann: Die Theorie der komplexen Zahlen, welche aus zwei Quadratwurzeln zusammengesetzt sind. 1867.*

For a certain class of cubic fields cf. *Eisenstein: Allgemeine Untersuchungen über die Formen dritten Grades mit drei Variabeln, welche der Kreisteilung ihre Entstehung verdanken* (*Crelles* Journ. XXVIII).

that are not divisible by $\mathfrak{p}$. Then the product $\alpha\beta\gamma\ldots$ is in $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$ and therefore also in $\mathfrak{m}$, and is not divisible by the prime ideal $\mathfrak{p}$. It follows that $\mathfrak{p}$ does not divide $\mathfrak{m}$, as was to be proved.

If the number η is not divisible by the ideal $\mathfrak{a}$, then there is always a number ν that is divisible by η, with the property that all the roots π of the congruence $\nu\pi \equiv 0 \pmod{\mathfrak{a}}$ form a prime ideal. All the roots β of the congruence $\eta\beta \equiv 0 \pmod{\mathfrak{a}}$ form an ideal $\mathfrak{b}$ that divides $\mathfrak{a}$, and which is distinct from $\mathfrak{o}$, since it does not contain the number 1. If $\mathfrak{b}$ is a prime ideal, the theorem is proved. If $\mathfrak{b}$ is not a prime ideal, there are then two numbers η', ρ', not divisible by $\mathfrak{b}$, whose product $\eta'\rho' \equiv 0 \pmod{\mathfrak{b}}$. So all the roots γ of the congruence $\eta'\gamma \equiv 0 \pmod{\mathfrak{b}}$, that is, the congruence $\eta\eta'\gamma \equiv 0 \pmod{\mathfrak{a}}$, form an ideal $\mathfrak{c}$ that divides $\mathfrak{b}$. Indeed we have (from 2.) $N(\mathfrak{c}) < N(\mathfrak{b})$, since ρ' is contained in $\mathfrak{c}$ but not in $\mathfrak{b}$. Furthermore, $\mathfrak{c}$ is distinct from $\mathfrak{o}$, since η' is not contained in $\mathfrak{b}$ and so the number 1 is not contained in $\mathfrak{c}$. If $\mathfrak{c}$ is a prime ideal, the theorem is proved. If, however, $\mathfrak{c}$ is not a prime ideal, one can carry on in the same way. Ultimately the sequence of ideals $\mathfrak{b}, \mathfrak{c}, \mathfrak{d}, \ldots$, whose norms decrease but remain > 1, must yield a prime ideal $\mathfrak{p}$, in which all roots π of the congruence $\nu\pi \equiv 0 \pmod{\mathfrak{a}}$ remain, where $\nu = \eta\eta'\eta''\ldots$ is divisible by η.

4. If μ is a nonzero number in $\mathfrak{o}$ and not a unit, then by these last theorems (in which one can set $\eta = 1$) there exists in any case a number ν with the property that all roots π of the congruence $\nu\pi \equiv 0 \pmod{\mu}$ form a prime ideal $\mathfrak{p}$. We will henceforth call prime ideals which arise as the roots of such a congruence *simple* ideals. If now r is any non-negative rational integer exponent, then all the roots ρ of the congruence $\rho\nu^r \equiv 0 \pmod{\mu^r}$ form an ideal, which will be called the *rth power* of $\mathfrak{p}$ and will be denoted $\mathfrak{p}^r$. This definition is independent of the pair of numbers μ, ν used in the definition of $\mathfrak{p}$; for if μ' is any nonzero number divisible by $\mathfrak{p}$, then $\nu\mu' = \mu\nu'$, and multiplying the congruence $\rho\nu^r \equiv 0 \pmod{\mu^r}$ by μ'^r and dividing by μ^r we have $\rho\nu'^r \equiv 0 \pmod{\mu'^r}$, and conversely. The following theorems on simple ideals $\mathfrak{p}$ are of the utmost importance:

If $s \geq r$, then $\mathfrak{p}^s$ is divisible by $\mathfrak{p}^r$. For if σ is contained in $\mathfrak{p}^s$, then $\sigma\nu^s = \tau\mu^s$, and it follows that

$$\left(\frac{\sigma\nu^r}{\mu^r}\right)^s = \tau^r\sigma^{s-r}$$

is an integer. Hence (from §160, 3.) the relevant quotient $\sigma\nu^r/\mu^r$ is always an *integer* in the field Ω, and therefore contained in $\mathfrak{o}$, since $\mathfrak{o}$ comprises *all* the

integers of the field Ω.[31] So each number σ of the ideal $\mathfrak{p}^s$ is also contained in $\mathfrak{p}^r$.

If ρ is a nonzero number in $\mathfrak{o}$, then there is always a highest power of $\mathfrak{p}$ that divides ρ. For if there were infinitely many exponents r such that the product $\rho\nu^r$ were divisible by μ^r, then, since there are only finitely many incongruent numbers (mod ρ), there would necessarily be two distinct such exponents r satisfying

$$\frac{\rho\nu^r}{\mu^r} \equiv \frac{\rho\nu^s}{\mu^s} \pmod{\rho}, \quad \left(\frac{\nu}{\mu}\right)^r = \left(\frac{\nu}{\mu}\right)^s + \omega,$$

where ω is an integer. Hence, from this it would follow (from §160, 3.) that ν is divisible by μ, which is not the case, since otherwise $\mathfrak{p}$ would be $= \mathfrak{o}$.

If $\mathfrak{p}^r, \mathfrak{p}^s$ are the highest powers of $\mathfrak{p}$ dividing ρ, σ, respectively, then $\mathfrak{p}^{r+s}$ is the highest power of $\mathfrak{p}$ dividing $\rho\sigma$. For, since $\rho\nu^r = \rho'\mu^r$, $\sigma\nu^s = \sigma'\mu^s$, and neither of the products $\nu\rho', \nu\sigma'$ is divisible by μ, it follows that $\rho\sigma\nu^{r+s} = \rho'\sigma'\mu^{r+s}$, and $\nu\rho'\sigma'$ cannot be divisible by μ, since $\mathfrak{p}$ is a prime ideal.

If $e \geq 1$ is the exponent of the highest power of $\mathfrak{p}$ that divides μ itself, then $\mu\nu^e = \kappa\mu^e$, where $\nu\kappa$ is not divisible by μ. So it follows that $\nu^e = \kappa\mu^{e-1}$, i.e. the exponent of the highest power of $\mathfrak{p}$ that divides ν is $= e - 1$. The ideal $\mathfrak{p}^e$ consists of all the roots θ of the congruence $\kappa\theta \equiv 0 \pmod{\mu}$. The integer $\lambda = \kappa\mu/\nu = \sqrt[e]{\mu\kappa^{e-1}}$ is divisible by $\mathfrak{p}$ but not by $\mathfrak{p}^2$. Hence λ^r is divisible by $\mathfrak{p}^r$ but not by $\mathfrak{p}^{r+1}$, whereby it follows, parenthetically, that the ideals $\mathfrak{p}^r$ and $\mathfrak{p}^{r+1}$ are really *distinct*. Finally, the following theorem is clear:

Each power $\mathfrak{p}^r$ of a simple ideal $\mathfrak{p}$ is not divisible by any prime ideal other than $\mathfrak{p}$. For if π is any number in $\mathfrak{p}$, then any prime ideal that divides $\mathfrak{p}^r$ must also divide π^r, and so (by 3.) divide π itself; i.e. it must divide $\mathfrak{p}$ itself, and so must be equal to $\mathfrak{p}$.

5. The importance of the simple ideals and their analogy with the rational primes comes immediately to the fore in the following main theorem:

If all the powers of simple ideals that divide a nonzero number μ also divide a number η, then η is divisible by μ. If η is not divisible by μ, then (by 3.) there is a number ν divisible by η with the property that all roots π of the congruence $\nu\pi \equiv 0 \pmod{\mu}$ form a simple ideal $\mathfrak{p}$ that divides μ. If $\mathfrak{p}^e$ is the highest power that divides μ, then (from 4.) $\mathfrak{p}^{e-1}$ is the highest power that divides ν. Since ν is divisible by η, then η cannot be divisible

[31] When this condition is not satisfied, the above theorem loses its *general* validity; this is important for the generalization of the definition of an ideal (cf. §165, 4).

by $\mathfrak{p}^e$, as was to be proved. Clearly the same theorem can also be expressed as follows: *Every principal ideal* $\mathfrak{i}(\mu)$ *is the least common multiple of all the powers of simple ideals that divide* μ. At once we have the corollary:

Every prime ideal $\mathfrak{p}$ *is a simple ideal.* If μ is any nonzero number in $\mathfrak{p}$, then $\mathfrak{p}$ (by 3.) must divide powers of simple ideals whose least common multiple is $\mathfrak{i}(\mu)$; thus $\mathfrak{p}$ itself (by 4.) is a simple ideal. — We will therefore speak only of prime ideals in the future, and no longer of simple ideals.

If all the powers of prime ideals that divide an ideal $\mathfrak{m}$ *also divide a number* η*, then* η *is divisible by* $\mathfrak{m}$. If η is not divisible by $\mathfrak{m}$, then (from 3.) there is a number ν divisible by η with the property that all the roots π of the congruence $\nu\pi \equiv 0 \pmod{\mathfrak{m}}$ form a prime ideal $\mathfrak{p}$. If $\mathfrak{p}^e$ is the highest power of $\mathfrak{p}$ that divides $\mathfrak{m}$, then in $\mathfrak{m}$ there is a number μ that is not divisible by $\mathfrak{p}^{e+1}$, and such that the ideal $\mathfrak{r}$ consisting of all the roots ρ of the congruence $\nu\rho \equiv 0 \pmod{\mu}$ is divisible by $\mathfrak{p}$, since $\nu\rho \equiv 0 \pmod{\mathfrak{m}}$. If now $\mathfrak{p}^e, \mathfrak{p}'^{e'}, \mathfrak{p}''^{e''}, \ldots$ are all the highest powers of prime ideals $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'', \ldots$ that divide μ, then, as a consequence of the main theorem above, $\mathfrak{r}$ consists of all the common roots ρ of the congruences $\nu\rho \equiv 0 \pmod{\mathfrak{p}^e}, \nu\rho \equiv 0 \pmod{\mathfrak{p}'^{e'}}, \nu\rho \equiv 0 \pmod{\mathfrak{p}''^{e''}}$ etc., i.e. $\mathfrak{r}$ is the least common multiple of ideals $\mathfrak{q}, \mathfrak{q}', \mathfrak{q}'', \ldots$ which consist, respectively, of the roots of each of these congruences. Since now the ideals $\mathfrak{q}', \mathfrak{q}'', \ldots$, as divisors of $\mathfrak{p}'^{e'}, \mathfrak{p}''^{e''}, \ldots$, are not divisible by $\mathfrak{p}$, and since $\mathfrak{r}$ is divisible by $\mathfrak{p}$, $\mathfrak{q}$ must also (by 4.) be divisible by $\mathfrak{p}$. Consequently $\mathfrak{p}^e$ can not divide ν (since otherwise $\mathfrak{q}$ would be $= \mathfrak{o}$, and so not divisible by $\mathfrak{p}$). Then ν is divisible by η, and so $\mathfrak{p}^e$ cannot divide η, as was to be proved.

Clearly this *fundamental theorem* can also be expressed as follows: *Every ideal is the least common multiple of all the powers of prime ideals that divide it.* This corresponds to the fundamental theorem of rational number theory on the composition of numbers from primes (§8). It follows that every ideal $\mathfrak{m}$ is *completely determined* once the highest powers $\mathfrak{p}^e, \mathfrak{p}'^{e'}, \mathfrak{p}''^{e''}, \ldots$ of prime ideals that divide it are given. Without further work we also have the following theorem: *An ideal* $\mathfrak{m}$ *is divisible by an ideal* $\mathfrak{d}$ *if and only if all the powers of prime ideals that divide* $\mathfrak{d}$ *also divide* $\mathfrak{m}$. This follows immediately from the concept of the least common multiple.

If $\mathfrak{m}$ *is the least common multiple of* $\mathfrak{p}^e, \mathfrak{p}'^{e'}, \mathfrak{p}''^{e''}, \ldots$*, where* $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}''$ *are distinct prime ideals, then* $N(\mathfrak{m}) = N(\mathfrak{p})^e N(\mathfrak{p}')^{e'} N(\mathfrak{p}'')^{e''} \ldots$. There is always (by 4.) a number η that is divisible by $\mathfrak{p}^{e-1}$ but not by $\mathfrak{a} = \mathfrak{p}^e$. The ideal $\mathfrak{r}$ consisting of all roots ρ of the congruence $\eta\rho \equiv 0 \pmod{\mathfrak{a}}$ is distinct from $\mathfrak{o}$ (because it does not contain the number 1) and is a divisor of $\mathfrak{p}$ (by 4.), and is therefore equal to $\mathfrak{p}$. Since, furthermore, the greatest common divisor $\mathfrak{d}$ of

the ideals $\mathfrak{a} = \mathfrak{p}^e$ and $\mathfrak{i}(\eta)$ are equal to $\mathfrak{p}^{e-1}$ by the fundamental theorem we have just proved, it follows (from 2.) that $N(\mathfrak{a}) = N(\mathfrak{r})N(\mathfrak{d})$, i.e. $N(\mathfrak{p}^e) = N(\mathfrak{p})N(\mathfrak{p}^{e-1})$, and hence, in general, $N(\mathfrak{p}^e) = N(\mathfrak{p})^e$. — Now (by Definition 2.) the least common multiple $\mathfrak{m}$ of the ideals $\mathfrak{p}^e, \mathfrak{p}'^{e'}, \mathfrak{p}''^{e''} \ldots$ is at the same time that of the ideals $\mathfrak{a} = \mathfrak{p}^e$ and $\mathfrak{b}$, where $\mathfrak{b}$ is the least common multiple of the ideals $\mathfrak{p}'^{e'}, \mathfrak{p}''^{e''} \ldots$. Since, further (by the fundamental theorem), $\mathfrak{o}$ is the greatest common divisor of $\mathfrak{a}$ and $\mathfrak{b}$, it follows (by 2.) that $N(\mathfrak{m}) = N(\mathfrak{a})N(\mathfrak{b})$, i.e. $N(\mathfrak{m}) = N(\mathfrak{p})^e N(\mathfrak{b})$. The theorem to be proved clearly follows from this.

6. If one multiplies all the numbers of an ideal $\mathfrak{a}$ with all the numbers of an ideal $\mathfrak{b}$, these products and their sums form an ideal that is divisible by $\mathfrak{a}$ and $\mathfrak{b}$, which will be called the *product of* $\mathfrak{a}$ *and* $\mathfrak{b}$ and denoted $\mathfrak{ab}$. From this definition it is immediately clear that $\mathfrak{ao} = \mathfrak{a}$, $\mathfrak{ab} = \mathfrak{ba}$, and further $(\mathfrak{ab})\mathfrak{c} = \mathfrak{a}(\mathfrak{bc})$ (cf. §§1, 2, 147). We also obtain the following theorem:

If $\mathfrak{p}^a, \mathfrak{p}^b$ *are the highest powers of a prime ideal* $\mathfrak{p}$ *that divide* $\mathfrak{a}, \mathfrak{b}$ *respectively, then* $\mathfrak{p}^{a+b}$ *is the highest power of* $\mathfrak{p}$ *that divides* $\mathfrak{ab}$. *Also,* $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.

For, from the definition it follows immediately (considering 4.) that $\mathfrak{ab}$ is divisible by $\mathfrak{p}^{a+b}$. Since, furthermore, there exists a number α in $\mathfrak{a}$ that is not divisible by $\mathfrak{p}^{a+1}$, and a number β in $\mathfrak{b}$ that is not divisible by $\mathfrak{p}^{b+1}$, there is a number $\alpha\beta$ in $\mathfrak{ab}$ that is not divisible by $\mathfrak{p}^{a+b+1}$, whereby the first part of the theorem is proved. If $\mathfrak{a}$ is the least common multiple of the powers $\mathfrak{p}^a, \mathfrak{p}'^{a'}, \mathfrak{p}''^{a''}, \ldots$ of distinct prime ideals $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'', \ldots$, and $\mathfrak{b}$ is the least common multiple of the powers $\mathfrak{p}^b, \mathfrak{p}'^{b'}, \mathfrak{p}''^{b''}, \ldots$, then $\mathfrak{ab}$ is the least common multiple of the powers $\mathfrak{p}^{a+b}, \mathfrak{p}'^{a'+b'}, \mathfrak{p}''^{a''+b''}, \ldots$, whereby (considering 5.) the second part of the theorem follows as well.

Since the equation $\mathfrak{p}^a\mathfrak{p}^b = \mathfrak{p}^{a+b}$ also follows from this theorem, the terminology and notation we chose above (in 4.) is justified. If furthermore $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'', \ldots$ are distinct prime ideals, then $\mathfrak{p}^a\mathfrak{p}'^{a'}\mathfrak{p}''^{a''} \ldots$ is the least common multiple of the powers $\mathfrak{p}^a, \mathfrak{p}'^{a'}, \mathfrak{p}''^{a''}, \ldots$. It is also clear that the concept of exponentiation can be extended to any ideal $\mathfrak{a}$ by the definition $\mathfrak{a}^{r+1} = \mathfrak{a}\mathfrak{a}^r$. Finally, if $\mathfrak{a}$ is divisible by $\mathfrak{d}$, there is always exactly one ideal $\mathfrak{r}$ with the property that $\mathfrak{a} = \mathfrak{r}\mathfrak{d}$; for if $\mathfrak{p}^a, \mathfrak{p}^d$ are the highest powers of $\mathfrak{p}$ that divide $\mathfrak{a}, \mathfrak{d}$ respectively, then $d \leq a$, and $\mathfrak{d}$ is the product of all the powers $\mathfrak{p}^{a-d}$. Considering this, we easily see that the previous theorems (in 2.) can now be expressed more simply.

7. We now call $\mathfrak{a}$ and $\mathfrak{b}$ *relatively prime ideals* when their greatest common divisor is $= \mathfrak{o}$. Likewise, a number η will also be called *relatively prime to*

the ideal $\mathfrak{a}$ when $\mathfrak{a}$ and $\mathfrak{i}(\eta)$ are relatively prime ideals. It is then clear that the theorems of rational number theory on relative primality can easily be carried over to the theory of ideals. However, here we will rest content to prove the following important theorem (cf. §25):

If $\mathfrak{a}, \mathfrak{b}$ *are relatively prime ideals, and* μ, ν *are two given numbers, then there is always exactly one class of numbers* $\eta \pmod{\mathfrak{ab}}$ *that satisfy the conditions* $\eta \equiv \mu \pmod{\mathfrak{a}}, \eta \equiv \nu \pmod{\mathfrak{b}}$. For if μ, ν, η run through complete residue systems for the three modules $\mathfrak{a}, \mathfrak{b}, \mathfrak{ab}$ respectively, then each number η corresponds to exactly one combination μ, ν in such a way that $\mu \equiv \eta \pmod{\mathfrak{a}}, \nu \equiv \eta \pmod{\mathfrak{b}}$. If further two different numbers η, η' of the residue system for the module $\mathfrak{ab}$ corresponded to the same combination μ, ν, then $\eta - \eta'$ would be divisible by $\mathfrak{a}$ as well as by $\mathfrak{b}$, and so also by $\mathfrak{ab}$ (since $\mathfrak{a}, \mathfrak{b}$ are relatively prime ideals); but then $\eta \equiv \eta' \pmod{\mathfrak{ab}}$, contrary to our assumption. Hence as η runs through all its values, of which there are $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$, it gives rise to just as many *different* combinations μ, ν. Since there are in fact exactly this many different combinations μ, ν, every combination μ, ν must in turn correspond to some number η, as was to be proved.

If $\psi(\mathfrak{a})$ is the number of incongruent relatively prime numbers $\pmod{\mathfrak{a}}$ that are relatively prime to $\mathfrak{a}$, and $\mathfrak{a}, \mathfrak{b}$ are relatively prime, then $\psi(\mathfrak{ab}) = \psi(\mathfrak{a})\psi(\mathfrak{b})$. If further $\mathfrak{p}$ is a prime ideal and $e \geq 1$, then $\psi(\mathfrak{p}^e) = N(\mathfrak{p}^e) - N(\mathfrak{p}^{e-1}) = N(\mathfrak{p})^{e-1}(N(\mathfrak{p}) - 1)$. For, if δ runs through all r numbers that are divisible by $\mathfrak{p}$ and incongruent with respect to $\mathfrak{p}^e$, and further γ runs through a complete system of residues $\pmod{\mathfrak{p}}$, then the numbers $\gamma + \delta$ form (by 2.) a complete residue system $\pmod{\mathfrak{p}^e}$; then $N(\mathfrak{p}^e) = rN(\mathfrak{p})$, and $r = N(\mathfrak{p}^{e-1})$. Now, such a number $\gamma + \delta$ is relatively prime to $\mathfrak{p}^e$ if and only if γ is not $\equiv 0 \pmod{\mathfrak{p}}$. Therefore there are $r(N(\mathfrak{p}) - 1)$ such numbers $\gamma + \delta$ relatively prime to $\mathfrak{p}^e$, as was to be proved.

If $\mathfrak{p}$ is a prime ideal, there is always (by 4.) a number λ which is divisible by $\mathfrak{p}$ but not by $\mathfrak{p}^2$, and hence a number λ^e which is divisible by $\mathfrak{p}^e$ but not by $\mathfrak{p}^{e+1}$. If not $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'', \ldots$ are distinct prime ideals, and $\lambda', \lambda'', \ldots$ bears the same relationship to $\mathfrak{p}', \mathfrak{p}'', \ldots$ as λ bears to $\mathfrak{p}$, then there always exists, for given exponents $e, e', e'', \ldots$, a number η, which satisfies the congruences

$$\eta \equiv \lambda^e \pmod{\mathfrak{p}^{e+1}}, \eta \equiv \lambda'^{e'} \pmod{\mathfrak{p}'^{e'+1}},$$
$$\eta \equiv \lambda''^{e''} \pmod{\mathfrak{p}''^{e''+1}} \ldots$$

since the moduli are relatively prime ideals. Then clearly $\mathfrak{i}(\eta) = \mathfrak{m}\mathfrak{p}^e\mathfrak{p}'^{e'}\mathfrak{p}''^{e''} \ldots$,

and the ideal $\mathfrak{m}$ is not divisible by any of the prime ideals $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'', \ldots$. Hence, the next theorem follows immediately:

If $\mathfrak{a}, \mathfrak{b}$ are any two ideals, then there is always an ideal $\mathfrak{m}$ relatively prime to $\mathfrak{b}$, such that $\mathfrak{am}$ is a principal ideal. For if $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'', \ldots$ are all the different prime ideals that divide $\mathfrak{ab}$, and $\mathfrak{a} = \mathfrak{p}^e \mathfrak{p}'^{e'} \mathfrak{p}''^{e''} \ldots$ (where the exponents can also be $= 0$), then, as we have just shown, there is a principal ideal $\mathfrak{i}(\eta) = \mathfrak{am}$, divisible by $\mathfrak{a}$, with the property that $\mathfrak{b}$ and $\mathfrak{m}$ are relatively prime.

From this it also follows that each ideal $\mathfrak{a}$ which is not a principal ideal can always be seen as the greatest common divisor of *two* principal ideals. For, one can choose a principal ideal $\mathfrak{i}(\eta') = \mathfrak{ab}$ at will, and one can always choose a second $\mathfrak{i}(\eta) = \mathfrak{am}$ so that $\mathfrak{b}$ and $\mathfrak{m}$ are relatively prime ideals. All the numbers of the ideal $\mathfrak{a}$ are then of the form $\eta\omega + \eta'\omega'$, where ω, ω' run through all the numbers in $\mathfrak{o}$.