Dedekind's treatment of Galois theory in the *Vorlesungen*

Edward T. Dean

December 14, 2009

Technical Report No. CMU-PHIL-184

Philosophy

Methodology

Logic

Carnegie Mellon

Pittsburgh, Pennsylvania 15213

Dedekind's treatment of Galois theory in the *Vorlesungen*

Edward T. Dean*

December 14, 2009

Abstract

We present a translation of §§160–166 of Dedekind's Supplement XI to Dirichlet's *Vorlesungen über Zahlentheorie*, which contain an investigation of the subfields of $\mathbb{C}$. In particular, Dedekind explores the lattice structure of these subfields, by studying isomorphisms between them. He also indicates how his ideas apply to Galois theory.

After a brief introduction, we summarize the translated excerpt, emphasizing its Galois-theoretic highlights. We then take issue with Kiernan's characterization of Dedekind's work in his extensive survey article on the history of Galois theory; Dedekind has a nearly complete realization of the modern "fundamental theorem of Galois theory" (for subfields of $\mathbb{C}$), in stark contrast to the picture presented by Kiernan at points.

We intend a sequel to this article of an historical and philosophical nature. With that in mind, we have sought to make Dedekind's text accessible to as wide an audience as possible. Thus we include a fair amount of background and exposition.

1 Introduction

Dirichlet's *Vorlesungen über Zahlentheorie* [14] were based on his lectures on number theory at the University of Göttingen; Dedekind edited the volume, which was first published after Dirichlet's 1859 death. Through the course of four editions from 1863 to 1894, Dedekind added eleven substantial supplements to the material; the subject of the present article is a treatment of fields and Galois theory that appears in a portion of Supplement XI from 1894. Given the protracted formation of the final version of the *Vorlesungen*, and at the hands of someone as influential as Dedekind, it is no surprise that the finished work

*The contents of this article are ultimately intended to be incorporated into a larger project. The translation grew out of an historico-philosophical seminar on Galois theory led by Jeremy Avigad of Carnegie Mellon and Ken Manders of the University of Pittsburgh. Avigad provided comments on an early version, and Wilfried Sieg answered a handful of queries concerning the translation itself.

can be seen as something of a bridge between different eras in the development of number theory (and perhaps of mathematics as a whole).

The first four chapters cover the basics of elementary number theory up to Gauss' results on quadratic forms from the 1801 *Disquisitiones Arithmeticae* [17]. The fifth chapter – also the last before Dedekind's supplements – gives Dirichlet's derivation of the class number formula for both real and imaginary quadratic fields. Another landmark result of Dirichlet's can be found in Dedekind's Supplement VI:

Theorem (Dirichlet)**.** *If a, d are coprime, then the arithmetic progression*

$$a,\ a+d,\ a+2d,\ a+3d,\ \ldots$$

contains infinitely many primes.

Dirichlet's proof of this theorem involved the first significant application of analytic methods to number theory.

So up to this point the volume already contains significant advances due to Dirichlet in both algebraic and analytic number theory. But Dedekind's supplements also offer crucial advances of his own. There is his well-known theory of *ideal divisors* for rings of integers in algebraic number fields, for instance; Dedekind gave varying accounts of this theory through the course of the four editions of the *Vorlesungen*, and elsewhere. The treatment of field theory in the excerpt below is of undeniable importance as well, and it greatly embodies the modern approach to Galois theory.

We summarize the translated excerpt in Section 2, and in Section 3 we criticize – on the basis of our exposition – Kiernan's analysis of Dedekind from [19], arguing that Kiernan does not properly recognize the extent to which Dedekind can be said to have realized the fundamental theorem of Galois theory. Before proceeding further, however, let us finish this introduction by very briefly recounting the fundamental theorem and some concepts undergirding it, in the spirit of being relatively self-contained.

Consider the divisibility relation $a \mid b$ which holds between positive integers a, b if and only if a divides evenly into b. This relation partially orders $\mathbb{Z}_+$. Moreover, any $a, b \in \mathbb{Z}_+$ have a *greatest lower bound* and a *least upper bound* in this ordering, namely the greatest common factor and least common multiple, respectively. Thus $\langle \mathbb{Z}_+, | \rangle$ is a paradigmatic example of a *lattice*.[1] And given any positive integer n, its collection of divisors form a *sublattice* of $\langle \mathbb{Z}_+, | \rangle$. (See Figure 1.)

Given a group G, its collection $\mathrm{Sub}(G)$ of subgroups also forms a lattice when it is equipped with the subgroup relation $\leq$. Similarly, the subfields of a field B form a lattice under the subfield relation $\subseteq$. And given a particular subfield A of B – or to put it another way, given an extension $B : A$ – the collection $\mathrm{Int}(B : A)$ of intermediate fields is a sublattice of the aforementioned. (Again, see Figure 1.) The fundamental theorem of Galois theory spells out a

[1] To be clear, a lattice is *precisely* a partially ordered set in which every two elements have a greatest lower bound and a least upper bound.

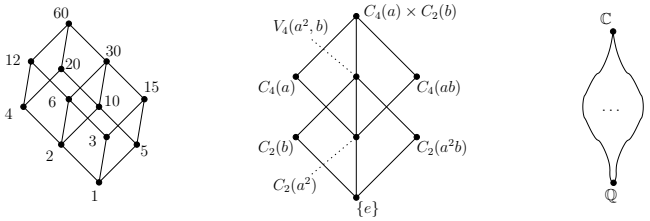

Figure 1: Examples of lattices. The divisors of 60, the subgroups of a particular finite abelian group (with generators in parentheses), and the subfields of $\mathbb{C}$ (which obviously cannot be drawn).

relationship between the lattice of intermediate fields of a (particular kind of) field extension $B : A$ and the lattice of subgroups of a corresponding group, known today as the "Galois group" of the extension.

Suppose we have a field extension $B : A$. It is now well-known that B can be viewed as a vector space over A; we call the extension *finite* if

$$[B : A] := \text{dimension of } B \text{ as an } A\text{-vector space}$$

is finite. We call the extension $B : A$ *Galois* if

$$\mathrm{Fix}(\mathrm{Aut}_A(B)) = A.$$

Here $\mathrm{Aut}_A(B)$ denotes the group of automorphisms of B which fix the field A, and $\mathrm{Fix}(G)$ denotes the subfield of B that is fixed by any $G \leq \mathrm{Aut}(B)$. This $\mathrm{Aut}_A(B)$ is the aforementioned *Galois group* of $B : A$.

We can now state the fundamental theorem of Galois theory; we express it (essentially) as in Hungerford's standard graduate algebra text [18].

Theorem (Fundamental theorem of Galois theory)**.** *Suppose we have a field extension $B : A$ that is both* finite *and* Galois*. Then:*

1. *The map*

$$\begin{array}{rcl} \mathscr{G} : \langle \mathrm{Int}(B : A), \subseteq \rangle & \longrightarrow & \langle \mathrm{Sub}(\mathrm{Aut}_A(B)), \geq \rangle \\ K & \longmapsto & \mathrm{Aut}_K(B) \end{array}$$

   is an isomorphism of lattices, with inverse $G \mapsto \mathrm{Fix}(G)$.

2. *For each intermediate field K, the degree of the extension $B : K$ equals the order of its image under $\mathscr{G}$:*

$$[B : K] = |\mathrm{Aut}_K(B)|.$$

3. *B is Galois over every intermediate K, but K is Galois over A iff*

$$\mathrm{Aut}_K(B) \lhd \mathrm{Aut}_A(B),$$ [2]

[2] I.e. this is a *normal* subgroup.

and in this case

$$\frac{\mathrm{Aut}_A(B)}{\mathrm{Aut}_K(B)} \cong \mathrm{Aut}_A(K).$$

2 Summary of the Excerpt

Here we give a summary of the translated excerpt, highlighting the results pertaining directly to Galois theory. Along the way we relate Dedekind's terminology to that of today, expressing many of Dedekind's notions and results in modern terms. At the end of this section, we indicate the precise extent to which Dedekind can be said to have formulated the fundamental theorem of Galois theory.

§160. Dedekind begins with his definition of a "field," which is more restricted than the modern axiomatic definition; Dedekind's fields are precisely *subfields of* $\mathbb{C}$, and henceforth in this section the locution "field" will always mean a subfield of $\mathbb{C}$. Thus, for Dedekind there is a largest field $\mathbb{C}$ which contains all others, and a smallest field $\mathbb{Q}$ of rationals which is contained in all others.

After this initial definition, Dedekind's first step is to define when a field A is a *divisor* of another field B (equivalently, B is a *multiple* of A). This amounts to nothing more than $A \subseteq B$, and so in this context a Dedekindian divisor is, in modern terms, a *subfield*, and a multiple is a *field extension*. Dedekind's use of the language of divisibility regarding extensions and subfields is not insignificant. Recall that the divisibility relation on $\mathbb{Z}_+$ is a staple example of a lattice; Dedekind's use of divisibility terminology underscores his recognition of the lattice structure on the subfields of $\mathbb{C}$ under the subfield relation.[3]

Given any collection $\{A_i\}_{i\in I}$ of subfields of $\mathbb{C}$, their intersection is nonempty since $\mathbb{Q}$ is contained in each of them. It is easy to check that

$$\gcd\{A_i\}_{i\in I} := \bigcap_{i\in I} A_i$$

is itself a field, and is moreover the *greatest common divisor* of the A_i's. That is, it is a divisor (subfield) of each of them, and it contains in turn any other common divisor. Building on this, Dedekind notes that for any collection of numbers $G \subseteq \mathbb{C}$, we have the field given as

$$\gcd\{M \supseteq G \mid M \text{ is a field}\} = \bigcap\{M \supseteq G \mid M \text{ is a field}\}.^4$$

Today we call this the field *generated by* G.

[3] Not long after publication of the fourth edition of the *Vorlesungen*, Dedekind laid the groundwork for lattice theory as its own subject [10, 9]. The concept he termed a *Dualgruppe* is exactly the modern notion of a lattice.

[4] He remarks that the set in this definition is nonempty, since $\mathbb{C}$ itself is certainly such an M. It is by virtue of working in the enveloping surroundings of the lattice of subfields of $\mathbb{C}$ that Dedekind is able to give this definition of the generated field as a greatest lower bound.

Dedekind goes on to give an explicit description of the numbers in this field as those which are *rationally representable* by the members of G, justifying the following notation for the generated field: $\mathbb{Q}(g', g'', \dots)$, where g', g'', $\dots$ are the members of G. He notes that, in Galois' terms, $\mathbb{Q}(g', g'', \dots)$ is the result of *adjoining* the members of G to the field $\mathbb{Q}$. And this generalizes to $A(g', g'', \dots)$ for any field A:

$$A(g', g'', \dots) := \bigcap \{M \supseteq (A \cup G) \mid M \text{ is a field}\}.$$

Now given any collection $\{A_i\}_{i \in I}$ of fields, their *product* is defined to be the field generated by the set of all their elements, i.e. the common extension

$$\prod_{i \in I} A_i := \bigcap \left\{ M \supseteq \bigcup_{i \in I} A_i \mid M \text{ is a field} \right\}.$$

Akin to the earlier terminology, Dedekind also calls the product the *least common multiple* of the fields A_i.

Thus Dedekind has shown that the subfields of $\mathbb{C}$ do indeed form a lattice. In fact, he has shown more; *any* collection of subfields has a greatest lower bound and a least upper bound, not just finite collections (which is all that is required by the definition of a lattice). In modern terms, he has shown that we have a *complete* lattice.

§161. Here Dedekind isolates the notion of a *field isomorphism* (or a *permutation* in his terms) as a function π on a field A that preserves field structure thus:

$$\begin{aligned} \pi(u+v) &= \pi(u) + \pi(v) \\ \pi(u-v) &= \pi(u) - \pi(v) \\ \pi(uv) &= \pi(u)\pi(v) \\ \pi(u/v) &= \pi(u)/\pi(v) \end{aligned}$$

for all $u, v \in A$.[5] Dedekind goes on to show that the image $\pi[A]$ of such a homomorphism is again a field, and moreover that π is necessarily injective; so all field homomorphisms are in fact monomorphisms, hence A is isomorphic to $\pi[A]$.[6]

Now suppose we have a collection $\Phi = \{\varphi_i : A_i \to B_i\}_{i \in I}$ of field isomorphisms. Dedekind calls a number $a \in \bigcap_{i \in I} A_i$ *one-valued*, or *two-valued*, etc. *in* Φ according to the number of distinct images a has under the permutations φ_i. For instance, any $q \in \mathbb{Q}$ is one-valued in any Φ because all rationals are fixed by any field isomorphism. Armed with this definition, Dedekind establishes the following:

[5] As Dedekind realizes, an equivalent characterization is for π to satisfy the first and third equations, plus the condition of not being constantly 0.

[6] Note that Dedekind's way of speaking allows him to rarely mention the range (or, codomain) of field isomorphisms. He will speak of a "permutation of A" without explicitly designating the field to which it maps.

Theorem (§161). *Given a set* $\Phi = \{\varphi_i : A \to B_i\}_{i=1,\dots,n}$ *of* distinct *isomorphisms from the common field* A*, there are infinitely many* $a \in A$ *which are* n*-valued in* Φ*.*

As a corollary, Dedekind observes that

Theorem (§161). *Given a set* $\Phi = \{\varphi_i : A \to B_i\}_{i=1,\dots,n}$ *of* distinct *isomorphisms from the common field* A*, there exist* n *numbers* a', a'', $\dots$, $a^{(n)}$ *in* A *for which*

$$\begin{vmatrix} \varphi_1(a') & \varphi_1(a'') & \cdots & \varphi_1(a^{(n)}) \\ \varphi_2(a') & \varphi_2(a'') & \cdots & \varphi_2(a^{(n)}) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_n(a') & \varphi_n(a'') & \cdots & \varphi_n(a^{(n)}) \end{vmatrix} \neq 0.$$

This introduction of talk of determinants foreshadows the linear-algebraic approach Dedekind takes in his proofs in §§164–5.

§162. In this section Dedekind merely defines the composition (or, in his terms, the *resultant*) of field isomorphisms, and notes some easy consequences such as the transitivity of isomorphism (or of *conjugacy* in his terms):

Theorem (§162). *If* $A \cong A'$ *and* $A' \cong A''$*, then also* $A \cong A''$*.*

§163. Dedekind presents one theorem in this section, and with it he begins progress toward the fundamental theorem of Galois theory.

Theorem (§163). *Let* $\Pi = \{\pi_i : M_i \to N_i\}_{i \in I}$ *be a collection of field isomorphisms. Then:*

1. $A := \{a \in \bigcap_{i \in I} M_i \mid a \text{ is one-valued in } \Pi\}$ *forms a field.*
2. *The* π_i*'s all have a common restriction* ψ *to* A*.*
3. ψ *extends any common restriction of the* π_i*'s.*

It is not hard to check that the set A is indeed a field, and the other parts follow immediately. Dedekind calls this collection A of all numbers which are one-valued in Π the *field of* Π, and he notes that the field of Π need not be the full intersection of the M_i's. (See Figure 2.) The notion of the field of Π becomes the *fixed field* once we consider Galois-theoretic settings. Specifically, there Π will be a set of *automorphisms* of a single field M that form a *group*, and in that setting the field of Π is exactly the subfield of M which is fixed by each member of Π. This is of course a central concept in the statement of the fundamental theorem of Galois theory.

§164. With this section, linear algebra comes to the fore. Dedekind calls a set of complex numbers $\omega_1, \dots, \omega_n$ *reducible* over the field A if there are $a_1, \dots, a_n \in A$, not all $= 0$, such that

$$\sum_{i=1}^{n} a_i \omega_i = 0.$$

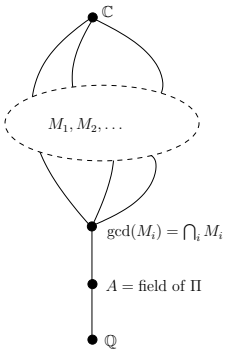

Figure 2: The theorem from §163 pictured in the lattice of subfields of $\mathbb{C}$.

Otherwise, they are *irreducible* over A. These are just the modern notions of linear dependence and independence.[7]

Given an irreducible set $\omega_1, \ldots, \omega_n$ over A, Dedekind observes that the collection Ω of linear combinations $\sum_{i=1}^{n} a_i\omega_i$ of the ω_i's using coefficients from A form what he calls a *family*; this is exactly the modern notion of an n-dimensional A-vector space, with the ω_i's as *basis*.

Suppose now that we have two fields A and B, with $\omega_1, \ldots, \omega_n$ from B being irreducible over A. Suppose further that any $n+1$ numbers from B are reducible over A. Dedekind defines this scenario as B being *finite and of degree* n over A, and denotes it thus:

$$(B, A) = n.$$

In this case, Dedekind shows that the collection Ω detailed above is in fact just the product field AB.[8]

By virtue of his result VII in the section, Dedekind concludes a result which shows, in particular, that finite extensions are algebraic:

Theorem. *When* $(B, A) = n$*, every number in* AB *is* algebraic[9] *over* A*, and of degree* $\leq n$*.*

Dedekind also notes that adjoining a single n-th degree number to a field results in an extension of the same degree:

[7] Dedekind himself mentions "dependent" and "independent" as alternative terminology for "reducible" and "irreducible."

[8] In particular, any finite extension $B : A$ of degree n can be seen as an n-dimensional A-vector space, since $AB = B$ in this case. Dedekind's notation (B, A) matches the modern $[B : A]$ exactly for a field extension $B : A$.

[9] An extension $B : A$ is called *algebraic* if every $b \in B$ is *algebraic over* A, i.e. there is some polynomial

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

in $A[x]$ of which b is a root. (There is a least n such that there is such a polynomial f with degree n. We call this n the *degree* of b over A.)

Theorem (§164, IX)**.** *If θ is algebraic of degree n over A, then $(\mathbb{Q}(\theta), A) = n$ (hence also $(A(\theta), A) = n$) and the powers $\theta^{n-1}, \ldots, \theta, 1$ form a basis for $A(\theta)$ over A.*

Later (§165, VI) Dedekind proves an important converse to the foregoing. Namely, any finite extension of A is of the form $A(\theta)$ for some θ of degree n. See below for more detail.

Finally, Dedekind establishes a result that specializes to the familiar tower law for field extensions:

Theorem (§164, X)**.** *If B is finite over A and C is finite over AB, then BC is finite over A, and in fact*

$$(BC, A) = (C, AB)(B, A).$$

Corollary (Tower law)**.** *When $A \subseteq B \subseteq C$, we have*

$$(C, A) = (C, B)(B, A).$$

§165. With this section, Dedekind ties together the developments of the previous sections. The following theorem, which refines that of §163, is the primary result. For Galois theory, its importance lies in the fact that the theorem proved in §166 depends upon it.

Theorem (§165, III)**.** *Suppose the field B is finite over A, and that φ is a permutation of A. Let Π be the set of permutations of AB extending φ. Then:*

1. *$|\Pi| = (B, A)$.*
2. *A is the field of Π.*
3. *φ is the remainder of Π.*

For the rest of our summary, when dealing with some fields A, B with $(B, A) = n$, we will restrict our attention to the case when B is in fact an extension of A; this allows us to more clearly exposit the Galois-theoretic interest.[10] Furthermore, as Dedekind actually does, let us now consider the case where the φ of the previous theorem is the *identity* on A. With our assumptions, the theorem tells us that

The number of isomorphisms from B that *fix* A is equal to (B, A). $(\star)$

Dedekind observes:

Theorem. *Let $A \subseteq B \subseteq \mathbb{C}$. The following are equivalent:*

1. *(B, A) is finite.*

[10] Throughout, Dedekind works in the general setting where B need not be an extension. With our restriction we get, e.g., to speak simply of B at points where Dedekind must speak of the product AB.

2. The lattice of intermediate fields between A and B is finite.

Dedekind quickly proves (2) from (1) using ($\star$) and the tower law, and merely remarks that the proof of (1) from (2) would be lengthy, but not difficult. This equivalence is obviously a key step toward analyzing the structure of the lattice of intermediate fields: when our extension is finite, so too is $\mathrm{Int}(B : A)$.

Let us note one more result from §165, which we pointed to earlier, namely:

Theorem (§165, VI)**.** *If $B : A$ is an extension with $[B : A] = n$, then there are infinitely many $\theta \in B$ of degree n over A, any one of which generates B when adjoined to A:*

$$B = A(\theta).$$

In modern terms, this last part has Dedekind observing that any finite extension $B : A$ is a *simple* one; that is, it is generated by a single element adjoined to A. Note that this does not hold in general for the modern, more inclusive notion of field; it is crucial that Dedekind's fields are subfields of $\mathbb{C}$. Here is the relevant result for modern fields:

Theorem (Theorem of the primitive element)**.** *Any finite and* separable[11] *field extension is a simple extension. (The single generating addition is the "primitive element" at hand.)*

Dedekind is able to obtain his result because in fields of characteristic[12] 0 (as is the case with subfields of $\mathbb{C}$) any finite extension is already separable.

§166. Dedekind calls a set of n permutations a *group* if it is closed under composition. He observes that this implies that all the elements are in fact *automorphisms* of a common field M, and that the identity automorphism is among them. So in modern terms, Dedekind's notion of being a group of permutations corresponds precisely with the modern notion of being some subgroup of the automorphism group $\mathrm{Aut}(M)$ of some field.

Given such a group Π of automorphisms of M, we know from ($\star$) that Dedekind's notion of the field of Π just coincides with the modern notion of

[11] In any algebraic extension $B : A$, every $b \in B$ has a(n essentially) unique *minimal polynomial* $f_b(x) \in A[x]$: the degree of f_b is the degree of b over A, f_b is monic, and $f_b(b) = 0$. We call an algebraic extension $B : A$ *separable* if the minimal polynomial f_b of any $b \in B$ is *separable*: each of its irreducible factors has no repeated roots in the algebraic closure $\overline{A}$ of A.

[12] For any ring R (such as any field), we can define its *characteristic* as follows. Consider the ring homomorphism $\varphi : \mathbb{Z} \to R$ given by

$$\begin{aligned} 0 &\mapsto 0_R \\ 1 &\mapsto 1_R \\ n &\mapsto \underbrace{1_R + \cdots + 1_R}_{n} \end{aligned}$$

Either φ is injective, in which case $\varphi[\mathbb{Z}] \cong \mathbb{Z}$, or it is not, in which case it can be shown that $\varphi[\mathbb{Z}] \cong \mathbb{Z}_m$ for some m, using the ring isomorphism theorem. In the former case we say that R has characteristic 0; in the latter case we say that it has characteristic m. (As an example, the order of any finite field is of the form p^n, with p a prime; such a field has characteristic p.)

the *fixed field* $\mathrm{Fix}(\Pi)$ of Π. Doing nothing more than translating Dedekind's terminology into our modern terms, we can state Dedekind's theorem from this section thus:

Theorem (§166, I)**.** *Let $M \subseteq \mathbb{C}$. For any finite subgroup $\Pi \leq \mathrm{Aut}(M)$,*

$$[M : \mathrm{Fix}(\Pi)] = |\Pi|.$$

Let us note that Dedekind has isolated in the hypotheses for this theorem a condition which is easily seen to be equivalent to the Galois condition:

Lemma. *The following are equivalent:*

1. *$M : A$ is a Galois extension.*
2. *$A = \mathrm{Fix}(\Pi)$ for some $\Pi \leq \mathrm{Aut}(M)$.*

Proof. (1) $\Rightarrow$ (2). To say that $M : A$ is Galois is just to say that $A = \mathrm{Fix}(\mathrm{Aut}_A(M))$. But then of course $M : A$ is of the appropriate form, setting $\Pi := \mathrm{Aut}_A(M) \leq \mathrm{Aut}(M)$.

(2) $\Rightarrow$ (1). We need to check that $\mathrm{Fix}(\Pi) = \mathrm{Fix}(\mathrm{Aut}_{\mathrm{Fix}(\Pi)}(M))$. We certainly have

$$\mathrm{Fix}(\Pi) \subseteq \mathrm{Fix}(\mathrm{Aut}_{\mathrm{Fix}(\Pi)}(M))$$

just from the definitions. Also straight from the definitions, it is clear that

$$\Psi \subseteq \mathrm{Aut}_{\mathrm{Fix}(\Psi)}(M) \tag{$\dagger$}$$

for any $\Psi \subseteq \mathrm{Aut}(M)$. Furthermore, it is obvious that Fix is anti-monotonic in the following sense:

$$\Psi \subseteq \Psi' \implies \mathrm{Fix}(\Psi) \supseteq \mathrm{Fix}(\Psi').$$

Simply plugging Π into ($\dagger$) and applying this last fact yields

$$\mathrm{Fix}(\mathrm{Aut}_{\mathrm{Fix}(\Pi)}(M)) \subseteq \mathrm{Fix}(\Pi),$$

and so $\mathrm{Fix}(\Pi) = \mathrm{Fix}(\mathrm{Aut}_{\mathrm{Fix}(\Pi)}(M))$ as desired. □

Thus Dedekind is working with a Galois extension in his theorem. This is necessary in order to reach his conclusion since, as we will see, Dedekind can go on to conclude the fundamental theorem of Galois theory from his Theorem I. Moreover, we will see that Dedekind explicitly acknowledges the fact that his extension meets the modern Galois criterion, though he does not spell out a proof that it does.[13]

So how does Dedekind proceed from Theorem I? Immediately after his proof, Dedekind continues (where his A is our $\mathrm{Fix}(\Pi)$, and his n is our $[M : \mathrm{Fix}(\Pi)] = |\Pi|$):

[13]Of course, we have just shown that a proof of their equivalence is quite trivial, and certainly would have been for Dedekind.

> Now if a part of the group Π likewise forms a group Π', which consists of p permutations π', then the field A' of Π' is a divisor of M and a multiple of A, because each number one-valued in Π is also one-valued in Π', and at the same time $n = pq$, where $p = (M, A')$, $q = (A', A)$.

The visual on the foregoing quote can be seen in Figure 3. Dedekind goes on:

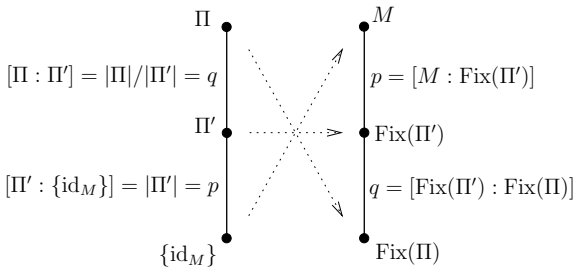

Figure 3: The initial correspondence indicated by Dedekind.

> Conversely, if a field A' is a divisor of M and a multiple of A, one easily sees that the permutations of M which are multiples of the identity permutation of A' form a group Π' contained in Π, *and* A' *is the field belonging to* Π'. (my emphasis)

Note the last part; Dedekind is asserting precisely that $\mathrm{Fix}(\mathrm{Aut}_{A'}(M)) = A'$ for any $\mathrm{Fix}(\Pi) \subseteq A' \subseteq M$. In particular, he is explicitly recognizing that $M : \mathrm{Fix}(\Pi)$ is a Galois extension, and that so too is $M : A'$ for any intermediate field A'.[14] Building on what went before, we can picture things as in Figure 4, and we see how the maps $\mathrm{Aut}_{\cdot}(M)$ and $\mathrm{Fix}(\cdot)$ are shaping up to be inverses as in the statement of the fundamental theorem. Iteratively applying the correspondence Dedekind has laid out, we see that the correspondence in fact holds for any chain in the (finite) lattice $\mathrm{Int}(M : \mathrm{Fix}(\Pi))$. That is, any chain in $\mathrm{Int}(M : \mathrm{Fix}(\Pi))$ is mirrored (upside down) in the lattice of subgroups of $\mathrm{Aut}_{\mathrm{Fix}(\Pi)}(M)$, with the proper numerical relationships between indices. Moreover:

> If, furthermore, Π'' is likewise a group contained in Π, and A'' is the field belonging to it, then the permutations common to both groups Π', Π'' again form a group; and the field belonging to it is the product $A'A''$.
>
> From [this discussion] *one recognizes that the complete determination of all these fields* $A', A'', \ldots$ *and the investigation of their mutual relations is completely settled by the determination of all groups* $\Pi', \Pi'', \ldots$ *contained in the group* Π, and this task belongs to the general theory of groups. (my emphasis)

[14] Cf. the third part of the statement of the fundamental theorem in our introduction.

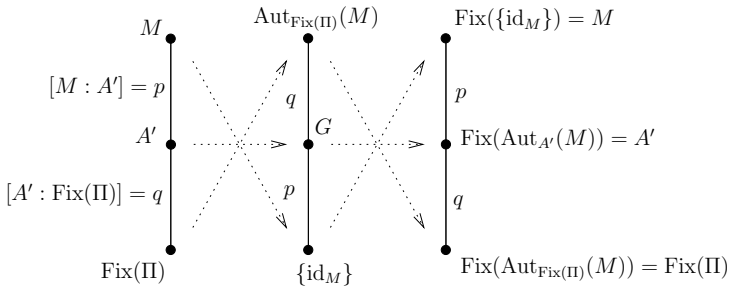

Figure 4: The further correspondence indicated by Dedekind. (For shorthand here we have set $G := \mathrm{Aut}_{A'}(M)$.)

With that first remark Dedekind paints a small part of the picture that the entire lattice structure is preserved when going between intermediate fields of $M : \mathrm{Fix}(\Pi)$ and subgroups of $\mathrm{Aut}_{\mathrm{Fix}(\Pi)}(M)$. He then immediately goes on to simply assert that the one structure completely mirrors the other. In sum, Dedekind has spelled out the bulk of the fundamental theorem of Galois theory (for subfields of $\mathbb{C}$):

Theorem (Dedekind's fundamental theorem of Galois theory)**.** *Let $A \subseteq B \subseteq \mathbb{C}$, and suppose the extension $B : A$ is finite and Galois. Then:*

1. *The map*

$$\begin{array}{rcl} \mathscr{G} : \langle \mathrm{Int}(B : A), \subseteq \rangle & \longrightarrow & \langle \mathrm{Sub}(\mathrm{Aut}_A(B)), \geq \rangle \\ K & \longmapsto & \mathrm{Aut}_K(B) \end{array}$$

   is an isomorphism of lattices, with inverse $G \mapsto \mathrm{Fix}(G)$.

2. *For each intermediate field K, the degree of the extension $B : K$ equals the order of its image under $\mathscr{G}$:*

$$[B : K] = |\mathrm{Aut}_K(B)|.$$

3. *B is Galois over every intermediate field K.*

3 An Historical Point

Emil Artin [1] is generally credited with the formulation of the fundamental theorem of Galois theory. There is nothing wrong with such an attribution; he was the first to state and prove the result in its modern form for the general notion of field, and to make it the prominent centerpiece of a presentation of Galois theory. Furthermore, the fact that Artin owed a great debt to Dedekind's work is not unrecognized. In large part, this debt is recognized in Kiernan's

extensive survey article [19] on the history and development of Galois theory; nonetheless, we will take issue with the exact characterization of Dedekind's work found therein.

Kiernan's paper proceeds largely chronologically, tracing advances made from the times of Vandermonde and Lagrange up through those of Artin. Along the way, Kiernan has a section on the development of field theory in the hands of Kronecker and Dedekind; this includes an exposition of our chosen excerpt from Supplement XI. What is puzzling in Kiernan's analysis is that his characterization of Dedekind's contribution to the fundamental theorem of Galois theory is different in the section on field theory than it is in his section on Artin. We examine the latter first.

Here is (a very superficial reworking of) Artin's statement of the fundamental theorem of Galois theory.[15]

Theorem (Artin)**.** *Consider a field extension $B : A$, where B is the splitting field of some separable polynomial $p \in A[x]$. Then:*

1. *The map*

$$\begin{array}{rcl} \mathscr{G} : \langle \mathrm{Int}(B:A), \subseteq \rangle & \longrightarrow & \langle \mathrm{Sub}(\mathrm{Aut}_A(B)), \geq \rangle \\ K & \longmapsto & \mathrm{Aut}_K(B) \end{array}$$

   is an isomorphism of lattices, with inverse $G \mapsto \mathrm{Fix}(G)$.

2. *For each intermediate field K, the degree of the extension $B : K$ equals the order of its image under $\mathscr{G}$:*

$$[B:K] = |\mathrm{Aut}_K(B)|.$$

3. *B is Galois over every intermediate K, but K is Galois over A iff*

$$\mathrm{Aut}_K(B) \lhd \mathrm{Aut}_A(B),$$

   and in this case

$$\frac{\mathrm{Aut}_A(B)}{\mathrm{Aut}_K(B)} \cong \mathrm{Aut}_A(K).$$

This should look familiar of course; in fact, Artin's hypothesis is yet another equivalent way of saying that $B : A$ is a finite Galois extension,[16] and so the content is exactly the same as what we quoted from Hungerford's text earlier. Given our foregoing summary, it is clear that this is just the generalization of Dedekind's result to arbitrary fields (plus the last bit about when intermediate extensions $K : A$ are Galois). Kiernan acknowledges, "Much of [Artin's]

[15] We have simply reworded things for the sake of comparing Artin's statement with those given above. Note also that we use the terminology laid out in the introduction, rather than Artin's. For instance, Artin uses the term "normal extension" for what we call a finite Galois extension.

[16] Artin includes in his theorem a proof that his kind of extension is Galois.

work was prefigured in the presentations of Dedekind and Weber" (144). For instance, he points out that Artin's linear-algebraic approach comes directly from Dedekind, as does his analogue to Dedekind's Theorem III from §165 (and even its proof). In fact, Kiernan goes so far as to say that Artin's work "[popularizes] a presentation *almost identical* with that offered by Dedekind in the 1890's" (149, my emphasis). As the reader might guess, we agree with this sentiment.

Now let us see what Kiernan has to say directly about Dedekind's work in the earlier section of the survey. Here too Kiernan already begins to acknowledge that Artin owes a significant debt to Dedekind. For instance, he writes that "[the theorem from §163] was to be of use to Artin in his reformulation of Galois Theory" (130). He adds furthermore: "Many results developed here by Dedekind on the interpretation of an extension field as a vector space over the ground field were later used by Artin in his formulation of Galois Theory" (131). Yet at the end of Kiernan's take on Dedekind, he states Theorem I from §166, sketches its proof, and then continues:

> Dedekind remarks almost offhandedly that if Π' is a subgroup of Π, then there exists a field A', $A \subset A' \subset M$, which belongs to Π', that is, every automorphism of M in Π' keeps A' fixed. Further, the degrees are related, he says, by
>
> $$(M, A')(A', A) = (M, A).$$
>
> This result, when applied to Galois Theory, will be one of the key points in Artin's development. But for Dedekind it remains merely a remark which he considers as so obvious from his previous development that he offers no proof at all at this point, nor does he formalize it as a theorem. (132)

There is much that is wrong with what Kiernan writes here. First of all, the field A' is just the "field of Π'" whose existence is *proved* (straightforwardly) in the theorem from §163. Secondly, Dedekind established the tower law already in §164, as we observed. More to the point, the facts Kiernan isolates here are just supporting facts which Dedekind *uses* to lay out the correspondence between the lattices in question. Kiernan makes no mention of the correspondence which Dedekind explains, or the fact that Dedekind indicates a *complete reduction* of questions about the lattice $\mathrm{Int}(M : A)$ to questions about the lattice of subgroups of $\mathrm{Aut}_A(M)$.

The quoted passage is the last thing Kiernan writes about Dedekind's text, leaving the impression that Dedekind says nothing more, and that it is only with Artin that we get something resembling the modern fundamental theorem of Galois theory. It should be clear from our summary that this is quite an injustice. Now some of Kiernan's statements above could be fairly applied to Dedekind's recognition of the fundamental theorem (though, as we noted, that is not what Kiernan actually did): Dedekind does not "formalize" this as a theorem (in the sense of offsetting it and giving it a number, say), and he does

not offer a detailed, full proof of everything.[17] But we believe it is plain to see that Dedekind had full cognizance of the structure of the fundamental theorem of Galois theory, that he gave voice to the statement we provide above, and that he more than outlined a proof.

To further drive home how off base Kiernan's characterization of Dedekind's contribution is, let us note that Dedekind even gives another characterization of just when a finite extension is Galois. Specifically, at the end of §166 Dedekind looks at the general case when $[B : A] = n$ and isolates a criterion that guarantees the assumption of his Theorem I, i.e. that $B : A$ is Galois. In §165, Dedekind has introduced the notion of the "norm" (with respect to A) of a field B that is finite over A.[18] Let $(B, A) = n$; we then know from $(\star)$ that there are exactly n isomorphisms $\pi_1, \ldots, \pi_n$ from B which extend id_A; note that these π_i need not be *auto*morphisms, and can instead map B onto some other field. Set $B_i := \pi_i[B]$, and without loss of generality let $\pi_1 := \mathrm{id}_B$. The *norm* of B with respect to A is then just the product $\mathrm{Norm}_A(B) := B_1 B_2 \cdots B_n$. (See Figure 5.) Dedekind calls B a *normal field* over A if B is its own norm: $\mathrm{Norm}_A(B) = B$.[19]

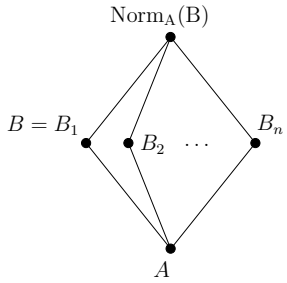

Figure 5: The norm of B with respect to A.

As Dedekind observes, it is easy to see that when B is normal over A, the collection Π of isomorphisms extending id_A is in fact a *group*. If $\mathrm{Norm}_A(B) = B$, then clearly all $B_i = B$, and so Π consists only of automorphisms of B. Of course, they are precisely the ones fixing A, so Π is just the group $\mathrm{Aut}_A(B)$. Moreover, it is clear from III in §165 that A is the field of $\mathrm{Aut}_A(B)$, i.e. that $A = \mathrm{Fix}(\mathrm{Aut}_A(B))$ and we have a Galois extension.

To sum up, Artin's formulation of the fundamental theorem of Galois theory is a direct generalization of Dedekind's result for subfields of $\mathbb{C}$. Dedekind's

[17] Then again, the other point Kiernan made is also no doubt right: Dedekind probably considered the matters obvious given his build-up to them. Moreover, Dedekind's Supplement XI is primarily concerned with algebraic number theory, and not Galois theory *per se*, further justifying a somewhat sketchy treatment of the matter.

[18] Recall that we are currently making the slightly simplifying assumption that B actually extends A in our discussion.

[19] We mentioned in footnote 15 that what we call a finite Galois extension, Artin calls a normal extension. Kiernan correctly points out the equivalence between being finite and Galois on the one hand, or satisfying the normality condition we are currently defining on the other hand. However, Kiernan attributes this notion to Weber.

notion of field isomorphism, his viewing field extensions as vector spaces, his characterizations of finite and Galois extensions, even his methods of proof generalize to the wider setting of arbitrary fields. In the end, Dedekind's structuralist tendencies got the concepts "right" and Emmy Noether's oft-quoted line applies well to the fundamental theorem of Galois theory: "Es steht schon bei Dedekind."[20] To reiterate, we are not saying anything earth-shattering here. Dedekind's contribution is generally well understood, and is even strongly asserted by Kiernan himself at points; we merely wanted to address the mischaracterization found in part of [19].

4 Notes on the Translation

Stillwell produced an English translation of the *Vorlesungen* [15], but it does not include Supplements X and XI. Avigad [2] has translated the 1871 version of Supplement X, which features a treatment of ideal theory, providing copious notes and a generous introduction which offers both historical and technical insights.[21]

As far as I know, there is no extant English translation of Supplement XI available. The excerpt below consists merely of §§160-166, which is but a small portion of the full §§159-187 comprising the entire supplement. Let us note a few things about our text itself:

1. In the original text, Dedekind's footnotes are not numbered; here we have numbered them, but with roman numerals in order to contrast with our own, which of course are numbered with arabic numerals.

2. Textual emphasis in the original is always achieved via expanded spacing between characters. We have instead generally used *italics* to emphasize text. Exceptions are names, which we emphasize with Small Caps, and theorems, which we emphasize with sans-serif font.

3. We have not altered Dedekind's notation, except for altering the appearance of ellipses at some points.

4. Regarding the language itself of the translation, we have aimed primarily for ease of readability in the English, and have not focused too much attention on trying to faithfully capture Dedekind's style of writing in German.[22] That said, we use words such as "thereat," "commodious" and "protuberant" in our translation both because they seem to be faithful choices, and because they sound (to these ears) not too out of place for something written in 1894.

[20] "It's already in Dedekind."

[21] Dedekind later produced substantially different versions of ideal theory; there is the 1877 version [6] (translated from the French by Stillwell [11]), and the 1894 version from the final edition of the *Vorlesungen*. See Avigad's [3] for further details and discussion.

[22] In any case, we are simply not equipped linguistically to gauge success in such an endeavor.

5. The § titles we use are from the table of contents of the third volume of Dedekind's collected works. We note that where the term "finite fields" appears in the titles of §§164-5, the term "endlich Körper" is indeed used in the German edition. It should be clear, but we remark anyway, that the term is being used to refer to one field being finite *over* another, e.g. $(B, A) = n$, and has nothing to do with actual finite fields (in the modern sense).

5 Dedekind's Supplement XI: §§160-166

§ 160. Number fields

In order to achieve this goal,[23] we must investigate in particular the most important foundations of today's algebra, and this is the concern of the following paragraphs. The starting point of our investigation is the aforementioned definition:

A system A of real or complex numbers a is a *field*[i] *[Körper]* if the sums, differences, products and quotients of any two of the numbers a are themselves in the system A.

We can express this same idea by saying that the numbers of a field reproduce themselves under the rational operations (addition, subtraction, multiplication, division). Here we take it as self-evident that the number zero can never be the denominator of a quotient; therefore we also always presuppose that a field contains at least one number different from zero, because otherwise one could not speak at all about quotients within the system.

Obviously the system R of all rational numbers forms a field, and this is the simplest or, as we can also say, the smallest field, because it is completely contained in every other field A. Indeed, if one selects an arbitrary non-zero number a from A, then the quotient of this number a with itself, i.e. the number 1, is likewise in A according to the definition of a field, and also all whole rational numbers by repeated addition and subtraction of this number, and from here all rational numbers are formed by division, so that R is completely contained in A.

Each particular irrational root θ of a quadratic equation with rational coefficients produces, as already noted in §159, a particular quadratic field, which we will denote by $R(\theta)$; it consists of all numbers of the form $x + y\theta$, where x and y range over all rational numbers. One can easily see that there are infinitely many different quadratic fields $R(\theta)$, although one and the same field can always be produced by infinitely many different numbers θ.

The system Z of all real and complex numbers is likewise a field, and is surely the largest imaginable, because every other field is contained in it. Between the

[i] Cf. §159 of the second edition of this work (1871). This name should, just as in the natural sciences, in geometry and in the life of human society, designate here too a system which posesses a certain completeness, perfection, closure, whereby it appears as an organic whole, a natural unit. At first, in my Göttingen lectures (1857 to 1858), I had used the name *rational domain [rationales Gebiet]* for this same concept, but this is less commodious. The concept essentially coincides with that which Kronecker has called a *domain of rationality [Rationalitätsbereich]* (*Grundzüge einer arithmetischen Theorie der algebraischen Größen.* 1882) [20]. Cf. also *Theorie der algebraischen Funktionen einer Veränderlichen* written by H. Weber and myself (*Crelle's* Journal, Bd. 92, 1882) [12].

[23] At the tail end of the previous (and initial) section of Supplement XI, Dedekind indicates that his ultimate purpose will be to extend Kummer's use [21] of *ideal numbers* for the purpose of factorization in cyclotomic fields (which come from the consideration of equations of the form $x^n - 1 = 0$). Dedekind wants to do the same for domains "arising from an arbitrary algebraic equation" and to develop "the *foundations of a general number theory* which subsumes all special cases without exception."

two extremes R and Z lies the field which consists of all reals numbers, both rational and irrational.

As can already be seen from the examples given above, one very often wants to express the fact that all numbers of a field D also belong to another field M; in such a case we say for the sake of brevity that D is a *divisor [Divisor]* of M, or that M is a *multiple [Multiplum]* of D. Thus every field is a divisor and multiple of itself, and if each of the two fields A, B is a divisor of the other then they are identical, which is written $A = B$. If D is a divisor of M, but different from M, then we call D a *proper divisor* of M, and M a *proper multiple* of D. If A is a divisor of B, and B a divisor of C, then A is also a divisor of C. The field R is a common divisor, and the field Z a common multiple, of all fields.

From given fields we can now form new fields according to certain rules; in the following we consider two such field constructions, namely those of the *greatest common divisor* and the *least common multiple*, or *product*.

If A and B are two arbitrary fields, then the collection D which consists of all numbers u, v, ... belonging to both fields is again a field, because the sums, differences, products and quotients of u, v, ... are contained in both A and B, thus also in D. This field D is a common divisor of A and B, and is called the *greatest common divisor* of A and B. If A is a divisor of B, then $D = A$, and vice versa.

This notion can be directly transferred to a system of more than two, even infinitely many, fields A, B, ...; the collection of those numbers belonging to all of these fields is again a field, and is called their greatest common divisor.

The second kind of field construction is based on the following, likewise very simple consideration. If a certain system G of numbers g is given, whose cardinality [Anzahl] can be finite or infinite, then there is always a field M' (e.g. the field Z defined above) which contains all of these numbers g; the greatest common divisor M of all such fields M' is itself such a field, and moreover is the smallest such. It is important, in and of itself, to provide a clear picture of the field M, which is completely determined by the system G, via a simple construction, for which we may assume that G does not consist only of the number zero. First M must contain any number h which is either a number g itself or a product of several[ii] factors g; these numbers h reproduce themselves under multiplication. Then M must contain any number k which is either a number h itself or a sum of several numbers h; these numbers k, among which the numbers g are also found, reproduce themselves under addition and multiplication. Furthermore M must contain any difference l of two arbitrary numbers k; these numbers l reproduce themselves under addition, subtraction and multiplication, and among them we find all numbers $k = (k+k)-k$. Finally M must also contain any quotient m of two arbitrary numbers l; these numbers m reproduce themselves under all four rational operations and obviously form the field M, because among them is found every number $l = ll : l$, thus also every number k, h, g. In this way it has resulted that every number m of this field M is obtainable by a finite number of rational operations on the

[ii] Here, and also later, this should always designate a *finite* number of things.

numbers $g', g'' \dots$ of the given system G; such numbers m are called *rationally representable by the system* G; the field M is the collection of all these numbers m and can appropriately be designated by $R(G)$ or $R(g', g'' \dots)$. Following a mode of expression which is due to Galois we also want to say, the field M results from the field R of rational numbers by *adjunction [Adjunktion]* of the system G of numbers $g', g'' \dots$; more generally, if A is any field, we designate with $A(g', g'' \dots)$ the field obtained by adjunction of the numbers $g', g'' \dots$ to A, i.e. the smallest field which contains, besides the numbers of the field A, the numbers $g', g'' \dots$ as well.

Now if we have any system of fields A, B, $\dots$, and we let the system G consist of all and only those numbers g that are contained in at least one of these fields, then the field M which consists of all numbers m that are rationally representable by these numbers g is a common multiple of A, B, $\dots$, and is moreover the smallest, because according to the above every other M' is a multiple of M. For the sake of brevity we will also call the field M the *product of the factors* A, B, $\dots$ and will denote it by $AB \dots$, in which expression the order of the factors is unimportant; for it is obvious that $AB = BA$, $(AB)C = A(BC)$, etc. If one applies this construction of the field M to the case of two fields A, B, then the system G consists of all the numbers a of the field A and all numbers b of the field B, the numbers h are products ab, the numbers k and l are sums of such products, and therefore the product AB consists of all quotients of the form

$$m = \frac{a'_1 b'_1 + a'_2 b'_2 + \dots + a'_r b'_r}{a_1 b_1 + a_2 b_2 + \dots + a_s b_s}.$$

The fact that A is a divisor of B can be conveniently expressed by $AB = B$, and it is always the case that $AA = A$.

§ 161. Permutations of a field

In mathematics and in other sciences it happens very often that, given a system A of things or elements a, each particular element a is replaced according to a certain rule by a corresponding element a' (which may or may not be contained in A); such a law is often termed a *substitution*, and one says that by this substitution the element a transforms into the element a', and likewise that the system A transforms into the system A' of elements a'.[iii] This way of speaking becomes somewhat more comfortable and more descriptive if one understands this substitution, as we want to do, as a *mapping [Abbildung]* of the system A, and accordingly calls a' the *image [Bild]* of a, likewise A' the image of A. For the sake of clarity it is often necessary to use a particular symbol in

[iii] It was stated already in the third edition of this work (1879, note on p.470) that this faculty of the mind, to compare a thing a with a thing a', or to apply a to a', or to let a correspond to an a', without which no thought at all is possible, also grounds the entire science of numbers. The execution of these ideas has since been published in my paper *"Was sind und was sollen die Zahlen?"* (Braunschweig 1888) [8]; the system of notation for mappings and their compositions applied thereat deviates slightly from that used here, in a superficial way. [Trans. – The notational deviation mentioned is that Dedekind uses today's preferred notation for functions, e.g. $\varphi(a)$ rather than $a\varphi$, in his monograph on arithmetic.]

order to differentiate such a mapping-rule from others, e.g. φ; given this, we also want to designate the image a', into which a transforms under φ, by $a\varphi$; furthermore if T is a part of A, i.e. a system of elements t all of which belong to A, then $T\varphi$ is to mean the system which consists of the images $t\varphi$ of all the elements t; therefore $A\varphi$ is identical to the A' above.

We now apply this notion to an arbitrary *number field* A, considering however only such substitutions φ by which each number a contained in A transforms into another number $a' = a\varphi$. In this general setting, such substitutions still would not be of any interest; we ask rather whether it is possible to map the numbers a of the field A into numbers a' in such a way *that all rational relations holding between the numbers a transfer completely to the images* a'; or in other words, we require that if a number t is derived from arbitrary numbers u, v, w ... of the field A by means of rational operations–which number t likewise belongs to the field A–then these same rational operations applied to the images u', v', w' ... always yields the image t' of the number t. We call a substitution or mapping φ which is distinguished above all by this property a *permutation [Permutation] of the field A*. Since each rational operation is composed of a finite number of simple additions, subtractions, multiplications and divisions, it is then clear that the mapping φ is a permutation if and only if for any two numbers u, v in A the following four *basic rules* hold:

$$(u+v)' = u'+v' \tag{1}$$
$$(u-v)' = u'-v' \tag{2}$$
$$(uv)' = u'v' \tag{3}$$
$$\left(\frac{u}{v}\right)' = \frac{u'}{v'}. \tag{4}$$

Of these characteristic, i.e. necessary and sufficient, conditions for a permutation the last obviously requires *that the images* a' *do not all vanish*; conversely, if a mapping φ under which each number a of the field A maps to a number a' possesses this property and also obeys the laws (1) and (3), then the laws (2) and (4) follow from this, as we now want to prove, and therefore φ is a *permutation* of the field A. Indeed, equation (2) follows directly from equation (1) if, as is obviously permitted, one replaces the arbitrary number u of the field A by the number $(u-v)$ which is likewise contained in A; if $v \neq 0$, one may likewise replace u in (3) by the quotient u/v, whereby

$$u' = \left(\frac{u}{v}\right)' v'$$

results; now were $v' = 0$, then the images u' of *all* numbers u contained in A would vanish, which however stands in contradiction with our explicit condition; therefore the image v' of each non-zero number v is likewise non-zero, and thus law (4) holds, which was to be proven.

Furthermore, it follows that the system A', into which a permutation φ transforms the field A, is itself a field. If one considers the fact that A' consists of all and only those numbers u', v', ... which are images of numbers u, v ...

from the field A, and that according to (1) every non-zero number v' of the system A' is the image of a non-zero number from the field A, it then follows that the sums, differences, products and quotients of any two numbers u', v' from A' are likewise contained in A', because according to the conditions (1)-(4) they are all images of numbers from the field A; therefore A' is a field, which was to be proven.

We notice then that any two numbers u, v of the field A which are *distinct* from one another also have images u', v' which are *distinct* from one another[iv] because otherwise according to (2) the image of the non-zero number $(u - v)$ would vanish, which, as we have already proved above, is not possible. Therefore each particular number a' contained in the field A' is the image of only one completely determined number a of the field A, and it follows that one can oppose the permutation φ, under which A maps into A', with a mapping of A' denoted by φ^{-1}, under which each determined number a' contained in A' transforms into this particular number a of the field A; this mapping φ^{-1}, however, is certainly a *permutation of the field* A'; because if u', v' denote two arbitrary numbers of the field A', and u, v denote the appropriate numbers of the field A, then according to (1) and (3) the numbers $u' + v'$ and $u'v'$ of the field A' transform under φ^{-1} into the numbers $u + v$ and uv, which was to be shown. In addition it is clear that the field A' transforms under φ^{-1} into the entire field A, rather than a proper divisor of A; because each number a contained in A is really the image produced by the permutation φ^{-1} of some number a' contained in A'. We want to call each of these two permutations φ and φ^{-1} the *converse* or *inverse* of the other, the two fields A and A' should be called *conjugate fields*, and two numbers a and a' corresponding to one another should be called *conjugate numbers*.

That mapping of a field A under which each of its numbers transforms *into itself* obviously meets the sufficient conditions (1), (2), (3), (4) and is therefore a permutation; we want to call it the *identity permutation* of A. From here it is seen that every field is conjugate to itself.

The field J or $R(i)$ considered in §159 possesses besides the identity yet another permutation, under which each number $x+yi$ contained in it transforms into the conjugate number $x - yi$. This same permutation obtains, if x, y are not limited to rational numbers but rather denote arbitrary real numbers, also for the field Z consisting of all numbers.

We have seen in the previous section that every field A also contains all rational numbers; now if φ is again an arbitrary permutation of A, and one applies condition (4) to the case $u = v$, then it follows that $1' = 1$, and considering the conditions (1), (2), (3), (4) it follows from here that each *rational* number of the field A, because it results from a finite number of simple rational operations on the number 1, maps *to itself* under the permutation φ. The field R of rational numbers therefore has no permutation other than the identity.

If φ is a permutation of the field A, then we want to say conversely that A

[iv] Therefore, in the terminology used in §3 of the text cited above, any permutation of a field is a *similar [ähnliche]* or *distinct [deutliche]* mapping of it; A and A' are *similar* systems.

belongs to φ or is the field *belonging to* φ, or for the sake of brevity we also want to call A the *field of the permutation* φ, while $A\varphi$ is called the *field produced by* φ.

We will indicate by $\varphi = \psi$ that φ and ψ are only different symbols for one and the same field-permutation; thus it lies herein that φ and ψ are permutations of the same field A, and that $a\varphi = a\psi$ holds for each number a contained in A. If one of these two conditions is not fulfilled, we call φ and ψ *distinct*.

If Φ denotes a system of permutations of any fields, then we want to call a number contained in all of these fields (thus also in their greatest common divisor) *one-valued*, *two-valued* etc. *with respect to* Φ or *in* Φ, according to whether the number of *distinct* values to which it maps under all these permutations is 1, 2 etc. From the foregoing, therefore, every *rational* number is one-valued with respect to any system Φ; the following theorem is just as important:

If Φ is a system of n distinct permutations $\varphi_1, \varphi_2, \ldots, \varphi_n$ of the same field A, then there exist in the latter infinitely many numbers which are n-valued in Φ.

In order to prove this, we want to write briefly $t\varphi_r = t_r$, when t denotes an arbitrary number in A. If $n = 2$, then the theorem is understood immediately from above. If $n > 2$, then we may assume that a number a in A has already been found, which maps under the $n-1$ permutations $\varphi_2, \varphi_3 \ldots \varphi_n$ to just as many distinct numbers $a_2, a_3 \ldots a_n$. Now if a_1 is likewise distinct from all of these numbers, then the number a satisfies the property expressed by the theorem. In the alternate case, if e.g. $a_1 = a_2$, one selects from A another number b, which maps under φ_1, φ_2 to two different numbers b_1, b_2, and considers all numbers of the form $y = ax + b$, which are produced by arbitrary *rational* numbers x and thus themselves belong to the field A; since, from the foregoing, x maps to itself under any permutation, then generally from rules (1) and (3) $y_r = a_r x + b_r$, thus also

$$y_r - y_s = (a_r - a_s)x + (b_r - b_s),$$

where r, s denotes any combination of two distinct numbers from the range $1, 2 \ldots n$. For the combination $r = 1$, $s = 2$ it follows that the numbers y_1, y_2 [stets voneinander verschieden ausfallen], however the rational number x may be selected, because $a_1 = a_2$, but b_1 is different from b_2. For each of the remaining combinations r, s, a_r is different from a_s, and thus it follows that there is either none or only one rational number x for which $y_r = y_2$; if one excludes these possibly existing numbers x which, running through all combinations, certainly number $< \frac{1}{2}n(n-1)$, then any other rational number x certainly produces a number y which transforms into n distinct numbers y_1, y_2, …, y_n under the n permutations, which was to be proven.

From here we draw yet another important consequence. By a very well-known theorem of determinant theory, to which we will return later (in §167), the product of all of those differences $y_r - y_s$ in which $r < s$ is equal to the

determinant

$$\begin{vmatrix} y_1^{n-1} & y_1^{n-2} & \cdots & y_1 & 1 \\ y_2^{n-1} & y_2^{n-2} & \cdots & y_2 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ y_n^{n-1} & y_n^{n-2} & \cdots & y_n & 1 \end{vmatrix}$$

whose elements are the powers $(y_r)^{n-s}$, where r and s range independently through all values $1, 2, \ldots, n$. This determinant is therefore nonzero in our case. Since now $y_r = y\varphi_r$ and it follows from condition (3) that $(y_r)^{n-s} = (y^{n-s})\varphi_r$, then setting $y^{n-s} = a^{(s)}$ one gets the theorem:

If the n permutations $\varphi_1, \varphi_2, \ldots, \varphi_n$ of the same field A are all distinct, then there is a system of n numbers $a', a'', \ldots, a^{(n)}$ in A such that the determinant formed from the elements $a^{(s)}\varphi_r$ does not vanish.

§ 162. Resultants of permutations

After these considerations, which refer to permutations of one and the same field, we turn to the *composition*[v] *[Zusammensetzung]* of two permutations φ, ψ, which however is possible only if ψ is a permutation whose domain is the field $A\varphi$ that is the range of φ; following the notation's lead one may appropriately call ψ a *right neighbor* of φ, and φ a *left neighbor* of ψ. Each particular number a from the field A maps under the permutation φ into a particular number $a\varphi$ of the field $A\varphi$, and this maps under ψ into a particular number $(a\varphi)\psi$; one can thereby define a mapping π of the field A by setting $a\pi = (a\varphi)\psi$ generally. If one now considers conditions (1) and (3) of the previous section applied first to φ, then also to ψ, the reader will easily find that it follows that these same conditions hold also for this mapping π, and that the images $a\pi$ obviously do not all vanish (because e.g. $1\pi = 1$), so π is a permutation whose domain is the field A. We call this the *resultant [Resultante] of the components* φ, ψ and denote it by the symbol $\varphi\psi$, in which the influence of the *left* or *first* component φ on the *right* or *second* component ψ is well distinguished by the position. Given the above, the definition of this resultant $\varphi\psi$ consists in that the image produced from any number a contained in A is

$$a(\varphi\psi) = (a\varphi)\psi;$$

one can therefore omit the parentheses without hesitation and denote the image briefly by $a\varphi\psi$. Just as easily one can see that, if T is any part of A, the two systems $T(\varphi\psi)$ and $(T\varphi)\psi$ are completely identical and can therefore be denoted briefly by $T\varphi\psi$. From this the following theorem follows immediately:

If two fields A, A'' are conjugate to a third field A', then they are also conjugate to each other.

Because according to the hypothesis there is a permutation φ of A, and a permutation ψ of A', for which $A\varphi = A'$, and $A'\psi = A''$; therefore $A(\varphi\psi) = (A\varphi)\psi = A'\psi = A''$, which was to be proven.

[v] This is only a special case of the composition of mappings of arbitrary systems; see the conclusion in §2 of my text cited above, though the notation is different there.

Having described the composition of neighboring permutations in detail, we still highlight the following important theorems involving the notion, whose proofs the reader will find easy.

If φ is a permutation of the field A, then $\varphi\varphi^{-1}$ is the identity permutation of A. If ψ is a right neighbor of φ, then ψ^{-1} is a left neighbor of φ^{-1}, and $(\varphi\psi)^{-1} = \psi^{-1}\varphi^{-1}$. If, furthermore, ψ_1 is likewise a right neighbor of φ, and φ_1 a left neighbor of ψ, then it follows from $\varphi\psi = \varphi\psi_1$ that $\psi = \psi_1$, and from $\varphi\psi = \varphi_1\psi$ that $\varphi = \varphi_1$. If, in addition, the permutation χ is a right neighbor of ψ, then $(\varphi\psi)\chi = \varphi(\psi\chi)$, and one can therefore briefly denote the resultant by $\varphi\psi\chi$; from here there follows, if one applies the same method of proof as in §2, the completely determinate meaning of the resultant $\varphi_1\varphi_2 \dots \varphi_{n-1}\varphi_n$ of n components φ_1, φ_2 … φ_{n-1}, φ_n, each of which is a right neighbor of the preceding one; since the components may not be transposed with one another, and each can always be combined only with the immediately proceeding one in order to form a resultant, the number of distinct methods of producing this resultant is $= (n-1)(n-2)\cdots 2 \cdot 1$.

§ 163. Multiples and divisors of permutations

Besides the composition of neighboring permutations just described, we still have to consider now the equally important relations which obtain between the permutations of a field and those of its divisors. If the field A is a divisor of the field M, and π is a permutation of the latter, then a completely determined mapping φ of A is contained in π, under which for each number a contained in A (thus also contained in M) the image $a\varphi = a\pi$, and it is clear from the basic rules in §161 that this mapping φ is a permutation of A; we want to call it the *divisor of π relative to A*, and likewise π is a *multiple* of φ. Obviously φ^{-1} is at the same time a divisor of π^{-1}. If $A = M$, then naturally also $\varphi = \pi$; in every other case, i.e. if A is a proper divisor of M, one must strictly differentiate φ from π.[vi] If π is itself a divisor of a permutation ρ, then clearly φ is also a divisor of ρ. If π is the identity permutation of M, then φ is the identity permutation of A. The only permutation of the field R of rational numbers (namely the identity) is (according to §161) a common divisor of all field-permutations. Generally the following fundamental theorem applies:

If Π denotes any system of permutations π of arbitrary fields M, then the collection A of all numbers a that are one-valued in Π forms a field, which is a common divisor of the fields M; the permutations π all have one and the same divisor φ relative to A, and every common divisor ψ of the permutations π is a divisor of this permutation φ.

Since the essence of a number a that is *one-valued* in Π resides (according to §161) in the fact that the images $a\pi$ corresponding to all the permutations π have one and the same value, it therefore follows from the basic rules (in §161) that the sums, differences, products and quotients of any two such one-valued numbers u, v are likewise one-valued in Π; thus A is a field. If one further defines the mapping φ of A, in which one sets $a\varphi = a\pi$, then φ is obviously

[vi] This distinction carried no weight in §2 of the text cited above.

the divisor with respect to A of each individual permutation π. Finally, if a permutation ψ of a field B is a common divisor of the permutations π, and b is an arbitrary number in B, then $b\psi$ must agree with each of the images $b\pi$, i.e. b is a one-valued number in Π; thus B is a divisor of A, and at the same time ψ is a divisor of φ, which was to be proven.

Since this field A, which is a common divisor (although by no means always the greatest common divisor) of the fields M, is completely determined by the system Π, we want to say that A belongs to Π or it is the field belonging to Π, or we want to call A for short *the field of the system* Π, and one immediately sees that this way of speaking agrees completely with that of §161 in the case that Π consists of only one permutation. The permutation φ can without hesistation be called the greatest common divisor of the permutations π; for the sake of brevity however we want to call φ also the *remainder [Rest]* of the system Π, or of the permutations π. –

The situation with respect to the existence of a *common multiple* of given permutations is completely different; because it is clear e.g., that two *distinct* permutations of one and the same field certainly have no common multiple. A very important distinction is based hereupon: the permutations φ, ψ, ... should be called *compatible [einig]* (harmonious) or *incompatible*, according to whether they share a common multiple or not. If we restrict ourselves to the consideration of *two compatible* permutations φ, ψ of the fields A, B, and designate with ρ a common multiple of φ, ψ, then the field belonging to ρ is a common multiple of A, B and thus also of AB; further, if a denotes any number in A, b any number in B, and π the divisor of ρ with respect to AB, then $a\varphi = a\rho = a\pi$, $b\psi = b\rho = b\pi$, and therefore π is likewise a common multiple of φ, ψ. Now since any particular number m of the field AB is (according to §160) rationally representable by a finite set of numbers a, b, and the image $m\pi$ is representable in the same way (according to the basic rules of any permutation) by the images $a\pi$, $b\pi$, hence it can be derived from the numbers $a\varphi$, $b\psi$, it follows that the permutation π of the product AB is *completely* determined by the permutations φ, ψ of the factors A, B, hence it is entirely independent of the choice of the above permutation ρ. This permutation π, which is thus a divisor of any common multiple ρ of the permutations φ, ψ, can therefore be called their *least* common multiple or more briefly their *union*[vii] *[Union]*.

Conversely, if π denotes a permutation of a product AB, and φ, ψ denote the divisors with respect to A, B of π, then these permutations φ, ψ are obviously compatible, and π is their union. At the same time it is clear that $(AB)\pi = (A\pi)(B\pi) = (A\varphi)(B\psi)$, and that π^{-1} is the union of φ^{-1}, ψ^{-1}. If in addition φ_1, ψ_1 are two compatible permutations of the fields $A\varphi, B\psi$, and π_1 is their union, then one easily discerns that the resultants $\varphi\varphi_1, \psi\psi_1$ are likewise compatible, and that the resultant $\pi\pi_1$ is their union.

From these considerations, which hold just as well for systems of more than

[vii] I would prefer the word *product [Produkt]*, if the same were not already used in this sense by some writers for the composition of substitutions, for which I have chosen the equally common name *resultant* above (§ 162). [Trans. – Dedekind himself uses "product" precisely for the composition of substitutions in his 1857–8 Galois theory lectures.]

two, indeed of infinitely many, *compatible* permutations, at last we reach the following concept. A system of arbitrary (compatible or incompatible) permutations

$$\varphi_1, \varphi_2, \varphi_3 \dots$$

and a system of corresponding permutations

$$\varphi'_1, \varphi'_2, \varphi'_3 \dots$$

should be called *conjugate* systems if any two corresponding members φ_r, φ'_r are permutations of one and the same field A_r, and if at the same time the resulting permutations

$$\varphi_1^{-1}\varphi'_1, \varphi_2^{-1}\varphi'_2, \varphi_3^{-1}, \varphi'_3 \dots$$

are compatible. From the foregoing there arises immediately the theorem that two systems conjugate with a third are also conjugate with one another. The benefit which these and the previously developed concepts provide would, admittedly, become clearly recognizable only during a thorough, particularized account of algebra.

§ 164. Irreducible systems, finite fields

For the detailed investigation of the relationship between different fields–and herein lies the real subject of today's algebra–the following concept[viii] provides the most general, and at the same time the simplest, foundation:

A system T of m numbers $\omega_1, \omega_2, \dots, \omega_m$ is called *reducible [reduzibel]* over the field A, if there are m numbers $a_1, a_2, \dots, a_m$ in A which meet the condition

$$a_1\omega_1 + a_2\omega_2 + \dots + a_m\omega_m = 0$$

and which do not all vanish; in the opposite case the system T is called *irreducible* over A. According to whether the former or latter case occurs, we will also say that the m numbers $\omega_1, \omega_2, \dots, \omega_m$ are *dependent [abhängig]* on, or *independent* of, each other (over A).

If A is a divisor of the field B, then clearly each system reducible over A is also reducible over B, and every system irreducible over B is also irreducible over A. In the remarks that follow next, however, all systems T will be considered relative to one and the same field A, and it will therefore be alright to leave this relationship unmentioned.

Each irreducible system consists of several numbers distinct from one another and from zero, and a system consisting of only one number is irreducible if, and only if, this number is non-zero.

A reducible or irreducible system retains this character if the numbers are all multiplied by a common non-zero factor.

[viii] Cf. Dirichlet: *Verallgemeinerung eines Satzes aus der Lehre von den Kettenbrüchen nebst einigen Anwendungen auf die Theorie der Zahlen.* (Berliner Monatsberichte, April 1842, or Dirichlet's collected works, vol. 1, p. 633 [13].)

If one or more numbers are added to a reducible system, then the system remains reducible; each part of an irreducible system is irreducible.

The following application of the concept is of special interest. We say that a number θ is *algebraic [algebraisch]* over the field A, if it is the root of a finite algebraic equation of the form

$$\theta^n + a_1\theta^{n-1} + \cdots + a_{n-1}\theta + a_n = 0,$$

whose coefficients a_r belong to the field A. We can express this same property by saying that the $n+1$ powers $\theta^n, \theta^{n-1}, \ldots, \theta, 1$ form a reducible system over A. Among all positive exponents for which this reducibility holds, there must be a *least* n such that the system of n powers $\theta^{n-1}, \ldots, \theta, 1$ is irreducible, but becomes reducible by adding θ^n; we want to call this natural number n the *degree [Grad]* of the number θ over A, and we say for short that θ is an (algebraic) number of n^{th} degree over A. If $n = 1$ then θ is obviously contained in A, and conversely every number in the field A is algebraic of the first degree over A.

If we return now to the general case and assume that the above system of m numbers $\omega_1,\ \omega_2,\ \ldots,\ \omega_m$ (which do not all vanish) is reducible, then there is obviously a part of this system, which may consist of the n numbers $\omega_1, \omega_2, \ldots, \omega_n$ for instance, that is irreducible, while each of the $m-n$ remaining number $\omega_{n+1}, \omega_{n+2}, \ldots, \omega_m$ forms a reducible system with that part. We now want to generally denote by ω each number that is dependent on the numbers $\omega_1, \omega_2, \ldots, \omega_n$, i.e. which forms a reducible system with these numbers; it is clear that every such number ω can always (and only in a *single* way) be represented in the form

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

where the coefficients $h_1, h_2, \ldots, h_n$ denote numbers of the field A, and that conversely each number representable in this form is dependent on then n numbers $\omega_1, \omega_2, \ldots, \omega_n$. We call the collection Ω of all of these numbers ω a *family [Schar]* (over A); the system of n determinate numbers $\omega_1, \omega_2, \ldots, \omega_n$ is called an (irreducible) *basis [Basis]* of the family Ω, and these n numbers ω_r are themselves called the *members* or *elements* of this basis. To each number ω contained in Ω there belong n completely determined numbers $h_1, h_2, \ldots, h_n$ of the field A, which arise in the representation (1) of ω and should be called the *coordinates of* ω relative to this basis. The characteristic properties of such a family Ω are the following:

I. The numbers in Ω reproduce themselves by addition and subtraction, i.e. the sums and differences of any two such numbers are likewise numbers in Ω.

II. Any product of a number in Ω and a number in A is a number in Ω.

III. There exist n numbers in Ω independent of each other, but any $n+1$ such numbers are dependent.

Only the second part of this last property requires still further justification, and we may assume that it has already been proven for each similar family whose basis consists of less than n members. If one now takes $n+1$ arbitrary numbers $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_n$ from Ω, then in the case that one of them is zero, e.g. $\alpha = 0$, they are certainly dependent on each other; in the opposite case we may

suppose, e.g. that the first coordinate of the number α does not vanish; then one can obviously determine n numbers in such a way that the first coordinate of each of the n numbers

$$\alpha_1 + c_1\alpha,\ \alpha_2 + c_2\alpha, \ldots,\ \alpha_n + c_n\alpha$$

vanishes;[ix] these n numbers then belong to a family, whose basis consists of only $n-1$ numbers $\omega_2, \omega_3, \ldots, \omega_n$, and are therefore dependent on each other; there are therefore n numbers $a_1, a_2, \ldots, a_n$ in A, which do not all vanish, and which satisfy the condition

$$a_1(\alpha_1 + c_1\alpha) + a_2(\alpha_2 + c_2\alpha) + \cdots + a_n(\alpha_n + c_n\alpha) = 0,$$

and therefore the sum $a = a_1c_1 + a_2c_2 + \cdots + a_nc_n$ is contained in A, then it follows from this that the $n+1$ numbers $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_n$ really are dependent on each other, which was to be proven.

Conversely, if a number system Ω possesses the above three properties I, II, III, then it follows from the latter that, after one has selected n numbers $\omega_1, \omega_2, \ldots, \omega_n$ from Ω that are independent of each other, each number ω contained in Ω is certainly of the form (1); then it follows from II and I that each number ω of the form (1) belongs to the system Ω. Thus these three properties really are characteristic for the family Ω consisting of all numbers ω of the form (1).

At the same time it is clear from this that each irreducible system consisting of n such numbers ω can likewise be seen and used as a basis for Ω; with each transition from one basis to another there is obviously an associated transformation of the coordinates of all numbers ω, similar to analytic geometry. The following important theorem, which we will often need to use, although only later, refers to the selection of such a basis.

IV. An arbitrary system of n numbers of the family Ω is reducible or irreducible, respectively, according to whether the determinant formed out of its coordinates is zero or not.

In order to prove this, we consider an arbitrary system of n numbers α_1, α_2, $\ldots$, α_n contained in Ω, which thus are of the form

$$\alpha_r = a_{r,1}\omega_1 + a_{r,2}\omega_2 + \cdots + a_{r,n}\omega_n,$$

and denote by a the determinant formed out of the coordinates $a_{r,s}$. Now if these n numbers α_r form a reducible system, then there are n numbers x_1, x_2, $\ldots$, x_n in A which do not all vanish and which satisfy the condition

$$x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n = 0;$$

if one replaces herein the n numbers α_r with the protuberant expressions then, because the n numbers ω_s are independent of each other, the n sums

$$a_{1,s}x_1 + a_{2,s}x_2 + \cdots + a_{n,s}x_n$$

[ix] In the case $n = 1$ the statement is already proven from this alone.

contained in A must be $= 0$, and as is well known it follows from this that each of the products ax_1, ax_2, $\ldots$, ax_n, and thus also a itself, vanishes. If however the n numbers α_r form an irreducible system, thus also a new basis for Ω, then the n numbers ω_s are representable in the form

$$\omega_s = b_{1,s}\alpha_1 + b_{2,s}\alpha_2 + \cdots + b_{n,s}\alpha_n,$$

where again all coefficients $b_{r,s}$, whose determinant we denote by b, are contained in A. If one substitutes these representations of the numbers ω_s in the above expression for α_r, then it follows that each of the n^2 sums

$$a_{r,1}b_{s,1} + a_{r,2}b_{s,2} + \cdots + a_{r,n}b_{s,n}$$

contained in A is either $= 1$ or $= 0$, according to whether r, s are the same or different; by the well known theorem on the multiplication of determinants it follows from here that $ab = 1$, and therefore a is nonzero, which was to be proven.–

We turn now to the important question: When is such a family Ω, characterized by the properties I, II, III, a field? If this should be the case, then all products $\omega_r\omega_s$ of two elements from the basis must likewise be contained in Ω, hence

$$\omega_r\omega_s = a_1^{r,s}\omega_1 + a_2^{r,s}\omega_2 + \cdots + a_n^{r,s}\omega_n,$$

where all coefficients $a_m^{r,s}$ denote numbers of the field A.[x] If these conditions are fulfilled then (according to I) it is clear that the numbers ω of the family Ω reproduce themselves not only by addition and subtraction, but also by multiplication; furthermore if α is an arbitrary, but non-zero, number in Ω, then the n products $\alpha\omega_r$ certainly form an irreducible system, and they are likewise contained in Ω, so they can serve as a new basis for Ω; therefore each number ω is also representable in the form:

$$\omega = \alpha(k_1\omega_1 + k_2\omega_2 + \cdots + k_n\omega_n),$$

where the n new coordinates k_r again belong to the field A, and therefore any quotient of two numbers ω, α of the family Ω is also a number in Ω. We have therefore obtained the following theorem:

V. The necessary and sufficient conditions for a family Ω to be a field consist in the fact that all products of two elements of a basis for Ω are again contained in Ω.

We now call each basis of the family Ω also a basis of the field Ω over A. Since this field Ω certainly contains the number 1, there follows from II the theorem:

VI. If the family Ω is a field, then A is a divisor of Ω.

[x] According to the general laws $\omega_r\omega_s = \omega_s\omega_r$ and $(\omega_r\omega_s)\omega_t = \omega_r(\omega_s\omega_t)$, these coefficients must fulfill certain conditions, which however we need pursue no further here. Cf. §159 of the second edition (1871) of this work and my essay: *Zur Theorie der aus n Haupteinheiten gebildeten komplexen Größen* (Nachrichten von der Göttinger Ges. d. W. 1885, S. 141) [7].

Since, furthermore, if ω denotes an arbitrary number of this field Ω, all powers $\omega^2, \omega^3, \ldots$ are also contained in Ω, then according to III the $n+1$ numbers $\omega^n, \omega^{n-1}, \ldots, \omega, 1$ certainly form a reducible system, which we can express thus:

VII. If the family Ω is a field, then every number in it is algebraic over A and of degree at most n.

We now consider two fields A, B and assume there exist n numbers ω_1, ω_2, $\ldots$, ω_n in B which form an irreducible system over A, but any system of $n+1$ numbers of the field B is reducible; since any part of an irreducible system is likewise irreducible, there can only be one such number n; in this case we say that the field B is *finite and of degree* n over A, and we denote this by the equation[xi]

$$(B, A) = n.$$

First it is clear that the case $n = 1$ arises when and only when B is a divisor of A; the two equations

$$(B, A) = 1, \quad AB = A$$

are therefore equivalent. For an arbitrary degree n it follows that B is contained in the family Ω, which consists of all numbers ω of the form (1), and thus all products $\omega_r \omega_s$ in B are also contained in Ω, so Ω is (by V, VI) a field, and moreover a multiple of AB; since furthermore each number ω is formed rationally from numbers h_r of the field A and numbers ω_r of the field B and is thus contained in AB, it then follows that Ω is also a divisor of AB, therefore $\Omega = AB$. We can thus state the following theorem:

VIII. If B is a field of nth degree over A then

$$(AB, A) = (B, A) = n \tag{2}$$

as well, and every system of n numbers in B or AB that is irreducible over A forms a basis of the family AB over A.

At the same time it follows (from VII) that all numbers in AB, thus also all numbers in B, are algebraic over A, and of degree at most n; the fact that there also exist numbers of the n^{th} degree in B could now be proven of course, but because this will result automatically later (in §165, VI) we want to do without it for now and prove only the following converse:

IX. If θ is an algebraic number of n^{th} degree over A, and B is the field $R(\theta)$ which consists of all numbers rationally representable by θ, whereby $AB = A(\theta)$, then $(B, A) = n$ and the n powers $\theta^{n-1}, \theta^{n-2}, \ldots, \theta, 1$ form a basis for $A(\theta)$ over A.

For this we consider the family Ω of all numbers ω of the form

$$\omega = h_1 \theta^{n-1} + h_2 \theta^{n-2} + \cdots + h_{n-1}\theta + h_n,$$

[xi] I have first used the symbol (B, A) with this meaning on p.21 of the book reviews in volume 18 of Schlömilch's *Zeitschrift für Mathematik und Physik* (1873) [5]. [Trans. – This is a review of Bachmann's published lectures on the relations between circle division and number theory [4].]

whose coordinates h_r are arbitrary numbers in A. Since (by hypothesis) the power θ^n is contained in Ω, the same holds (by II, I) of $h_1\theta^n$ and of each product $\omega\theta$, thus also of all higher powers $\theta^{n+1}, \theta^{n+2}, \ldots$; therefore all products of any two members of the basis are likewise contained in Ω, and so Ω is (by V) a field. Since this field Ω is a multiple of A and contains the number θ, it is also a multiple of $A(\theta)$ and therefore $= A(\theta)$, because conversely each number ω is certainly contained in $A(\theta)$. The field $A(\theta)$ or AB is therefore of degree n over A, and thus the same holds of B also, which was to be proven.

Here we attach the following remarks. If t is a variable and we denote by $F(t), f(t), f_1(t), f_2(t), \ldots$ exclusively such polynomial functions of t whose coefficients are contained in the field A, then the sums, differences, products of the same are likewise such functions, and by division of $f_1(t)$ by $f(t)$ there arises an identity of the form $f_1(t) = f(t)f_2(t) + F(t)$, where the remainder $F(t)$ is of lower degree than $f(t)$, or is identically $= 0$ if $f_1(t)$ is divisible by $f(t)$. Now if θ has the same meaning as in the preceding theorem, then there is one and only one function of n^{th} degree

$$f(t) = t^n + a_1 t^{n-1} + \cdots + a_{n-1}t + a_n, \tag{3}$$

which has the same roots as $t - \theta$ and therefore is completely determined by the number θ (and A). If one designates with $F(t)$ any function whose degree is $< n$, then $F(\theta) = 0$ only if $F(t) = 0$ identically. Therefore if $f_1(\theta) = 0$, then $f_1(t)$ must be *divisible by* $f(t)$. The function $f(t)$ itself can be divisible by no function $F(t)$, because from $f(t) = F(t)F_1(t)$ and $f(\theta) = 0$ either $F(\theta) = 0$ or $F_1(\theta) = 0$ would follow, which is impossible. Such a function $f(t)$, whose coefficients are contained in A, and which is divisble by no similar function of lesser degree, is called *irreducible* or a *prime function [Primfunktion]* over A, and likewise the *equation* $f(\theta) = 0$ is called *irreducible*. The field $A(\theta)$ consists of all numbers ω of the form $F(\theta)$, and each such number ω can also be represented in the form $F(\theta)$ only in a single way.

Here we move on to the consideration of *three* fields A, B, C and establish the following theorem:[xii]

X. If B is finite over A and C is finite over AB, then also BC is finite over A, and

$$(BC, A) = (C, AB)(B, A). \tag{4}$$

Setting $(B, A) = n$ and $(C, AB) = p$, if the n numbers ω_r in B form an irreducible system over A and the p numbers τ_s in C form an irreducible system over AB, then the np products $\omega_r\tau_s$ form, as one can easily see, an irreducible basis for the field ABC over A, which was to be proven.

Most frequently the case arises where B is a multiple of A and at the same time a divisor of C, thus $AB = B$, $BC = C$, and therefore

$$(C, A) = (C, B)(B, A). \tag{5}$$

In addition it follows from the theorem X that each product of two or more fields finite over A is again such a field. Now if θ, η are two algebraic numbers over

[xii] Cf. the preceding citation.

A, then (by IX) the fields $R(\theta), R(\eta)$ are finite over A, and thus the same holds of their product $R(\theta, \eta)$; therefore the sum, difference, product and quotient of θ, η contained in the latter are also algebraic over A, and thus the totality of all numbers algebraic over A is a field.

It is expedient to settle on a meaning for the symbol (B, A), and set $(B, A) = 0$,[xiii] if B is not finite over A. Thereby one obtains, as the reader will easily find, that the theorems contained in the two equations (2), (4) hold for arbitrary fields A, B, C without any qualification. If one now exchanges the latter with one another, then one obtains certain reciprocities and other relations, e.g.

$$(B, C)(C, A)(A, B) = (C, B)(A, C)(B, A), \tag{6}$$

whose deeper meaning, however, can only be recognized through the following investigations.

§ 165. Permutations of finite fields

We now connect the concepts explained in the preceding sections with one another and suppose the field A is a divisor of the field M, and π is a permutation of the latter; for the sake of brevity, if ω is any number in M we denote by ω' the conjugate number $\omega\pi$. Now if the m numbers $\omega_1, \omega_2, \ldots, \omega_m$ contained in M form a reducible system T over A, thus there are m numbers $a_1, a_2, \ldots, a_m$ in A which satisfy the condition

$$a_1\omega_1 + a_2\omega_2 + \cdots + a_m\omega_m = 0$$

and which do not all vanish, then because $0' = 0$,

$$a_1'\omega_1' + a_2'\omega_2' + \cdots + a_m'\omega_m' = 0$$

also follows from this, and since a non-zero number a in A always gives rise to a non-zero number a' in $A\pi$, the system $T\pi$ contained in $M\pi$ which consists of the m numbers ω_1', ω_2', $\ldots$, ω_m' is *reducible* over $A\pi$. Furthermore, since each number ω' of the field $M\pi$ transforms into a number ω of the field M under the inverse permutation π^{-1}, then conversely the system T is certainly reducible over A if the system $T\pi$ is reducible over $A\pi$. We can thus state the following theorem:

I. If the field M is a multiple of the field A, and π is a permutation of M, then for a system T contained in M, the system $T\pi$ is reducible or irreducible according to whether T is reducible or irreducible, respectively.

If we apply this to the case where M is the product of the two fields A, B, then there follows immediately the theorem:

II. If π is a permutation of the product AB of the two fields A, B, then

$$(B, A) = (B\pi, A\pi).$$

We build on this for the proof of the following fundamental theorem:

[xiii] If one prefers it, then one may set $(B, A) = \infty$, which has essentially the same success.

III. If the field B is finite over A and φ is a permutation of A, then the degree (B, A) is the number of distinct permutations π of the product AB which are multiples of φ. At the same time, A is the field and φ is the remainder of the system Π of these permutations π.

This is immediately clear for the case $(B, A) = 1$, because then B is a divisor of A, hence $AB = A$, therefore $\pi = \varphi$ necessarily. In order to prove it generally, we apply complete induction; we assume that it has already been proven for all cases where the degree (B, A) is $< n$, and demonstrate that it then holds for $(B, A) = n$ also.

Here we must distinguish *two cases*, the *first* of which occurs if there is a third field K which is simultaneously a *proper* divisor of AB and a *proper* multiple of A. If we set $(AB, K) = p$, $(K, A) = q$, then (according to Theorems VIII and X in §164) $n = (B, A) = (AB, A) = (AB, K)(K, A) = pq$, and since K is distinct from AB and A, each of the two degrees p, q is > 1 and therefore also $< n$. Thus, given our assumption there exist q and only q distinct permutations

$$\chi_1, \chi_2, \ldots, \chi_q$$

of the field $AK = K$ which are multiples of φ, and if χ_r is any one of these permutations, there then exist p and only p distinct permutations

$$\pi_{r,1}, \ldots, \pi_{r,2}, \ldots, \pi_{r,p}$$

of the field $ABK = AB$ which are multiples of χ_r, and each of these permutations $\pi_{r,s}$ is (according to §163) simultaneously a multiple of φ. Since, furthermore, each permutation π of the field AB which is a multiple of φ always gives rise to one and only one permutation χ of K which is a divisor of π and thus likewise a multiple of φ, the n permutations $\pi_{r,s}$ given above, which correspond to the q values r and the p values s, are all distinct from one another, and except for these n permutations $\pi_{r,s}$ there could be no other permutation π of AB which is a multiple of φ. In this case, therefore, our statement concerning the *number* of permutations π is proven.

In the opposite *second* case, where there exists no field K with the above-mentioned property, we choose from B (or as well from AB) a number θ not contained in A, which is possible because $n > 1$, hence B is not a divisor of A. Then the field $A(\theta)$ produced from A by the adjunction of θ must be $= AB$, because it is simultaneously a divisor of AB and a multiple of A, but is distinct from A, and the number θ which is algebraic over A is (according to IX in § 164) certainly of degree $n = (B, A)$; the field $A(\theta)$ consists of all numbers α of the form

$$\alpha = F(\theta) = x_1\theta^{n-1} + x_2\theta^{n-2} + \cdots + x_{n-1}\theta + x_n, \tag{1}$$

where the n coefficients or coordinates x denote arbitrary numbers in A, and surely each number α is so representable in only one unique way, because the n powers $\theta^{n-1}, \ldots, \theta, 1$ form an irreducible system over A. The number θ is the root of a particular equation

$$f(\theta) = \theta^n + a_1\theta^{n-1} + a_2\theta^{n-2} + \cdots + a_{n-1}\theta + a_n = 0 \tag{2}$$

which is irreducible over A, whose coefficients a_r are at the same time the coordinates of the number $-\theta^n$.[xiv]

We now seek all potentially existing permutations π of this field $A(\theta)$ which are multiples of the given permutation φ of the field A. For the sake of simplicity, if x denotes an arbitrary number in A, we set the number produced from x by φ as

$$x\varphi = x'; \tag{3}$$

then, because π should be a multiple of φ, it must be that

$$x\pi = x' \tag{4}$$

as well, and since all numbers α of the field AB are formed rationally from numbers x and the unique number θ, the permutation π is completely determined once $\theta\pi$ is also known; if, for the sake of brevity, we set this number as

$$\theta\pi = \eta, \tag{5}$$

then it follows from (1) and (2) that each number α represented in the form (1) transforms into the appropriate number

$$\alpha\pi = \mathfrak{F}(\eta) = x'_1\eta^{n-1} + x'_2\eta^{n-2} + \cdots + x'_{n-1}\eta + x'_n \tag{6}$$

under π, and that η must be a root of the particular equation

$$\mathfrak{f}(\eta) = \eta^n + a'_1\eta^{n-1} + a'_2\eta^{n-2} + \cdots + a'_{n-1}\eta + a'_n = 0. \tag{7}$$

Conversely, if η denotes a particular root of this equation (7), then since each number α of the field $A(\theta)$ is always representable in a unique way in the form (1), a *mapping* π of this field is completely determined via rule (6), which subsumes (4) and (5) as special cases, and we now want to prove that this very same is actually a *permutation*. To this end we need (according to § 161) only to show that for any two numbers α, β of the field AB the rules

$$(\alpha+\beta)\pi = \alpha\pi + \beta\pi \tag{8}$$

$$(\alpha\beta)\pi = (\alpha\pi)(\beta\pi) \tag{9}$$

both hold. If one designates with y_r the coordinates of β, then $x_r + y_r$ are those of $\alpha+\beta$; now since φ is a permutation of A, hence $(x_r+y_r)' = x'_r + y'_r$, rule (8) results immediately from (6). Since the same naturally holds also for sums of more than two members, and since each number β is a sum of products whose factors are either $= \theta$ or contained in A, one easily recognizes that rule (9) need only be proven for the two cases where β is either an arbitrary number y of the field A or is $= \theta$. Now since the coordinates yx_r of the product αy transforms into $(yx_r)' = y'x'_r$ under the permutation φ, the first case $(\alpha y)\pi = (\alpha\pi)y'$ follows from (6), and likewise the second case $(\alpha\theta)\pi = (\alpha\pi)\eta$ follows easily, if

[xiv] It is good to note that all of the following holds for *any* such field $A(\theta)$ which arises from a number θ of degree n.

one considers that according to (2), (6), (7) it is also the case that $(\theta^n)\pi = \eta^n$. With this the proof is delivered, that each root η of the equation (7) actually gives rises to a *permutation* π of the field AB which is defined by (6) and is a multiple of φ.[xv]

At the same time it follows from theorem I that the n powers $\eta^{n-1}, \ldots, \eta, 1$ form an *irreducible* system over the field $A\pi = A\varphi$. Now according to the fundamental theorem of algebra first proved by GAUSS there generally exist n distinct roots η of the equation (7), and it is known that there are less than n only if at least one of these numbers η simultaneously satisfies the condition

$$\mathfrak{f}'(\eta) = n\eta^{n-1} + (n-1)a_1'\eta^{n-2} + (n-2)a_2'\eta^{n-3} + \cdots + a_{n-1}' = 0;$$

since this contradicts the irreducibility just proven, however, the equation (7) actually has n distinct roots η, and thus there are exactly n *distinct* permutations π of the field AB which are multiples of φ, which was to be proven.

Having herewith proved theorem III generally, insofar as it involves the *number* of permutations π, we can also easily deal with its last part. For if K denotes the *field* of the system Π, and χ denotes the *remainder*, then K consists (according to § 163) of all numbers one-valued in Π, hence is a multiple of A and divisor of AB, and its permutation χ is a multiple of φ; if one again sets $(AB, K) = p$, $(K, A) = q$, then $n = pq$, and according to the part of the theorem already proved, p is the exact number of distinct permutations of AB which are multiples of χ; but the n permutations π are certainly situated among these, and thus $p \geq n$, therefore $p = n$, $q = 1$, $K = A$, $\chi = \varphi$, which was to be proven. –

Now that the fundamental theorem III has been proven completely, we first remark that the divisors ψ with respect to B of the n permutations π are likewise distinct from one another, because conversely (according to §163) every permutation π of the product AB is completely determined by its divisors φ, ψ with respect to A,B. The field of the system Ψ of these n permutations ψ compatible with φ is, as is immediately clear, the greatest common divisor D of A, B, and the remainder of Ψ is the divisor of φ with respect to D.

If, furthermore, φ' is likewise a permutation of A, hence $\varphi^{-1}\varphi'$ is a permutation of $A\varphi$, and Π' is the system of these n permutations π' of AB which are multiples of φ', then if π denotes a particular permutation in Π, the n permutations $\pi^{-1}\pi'$ of the field $(AB)\pi$ are distinct and at the same time multiples of $\varphi^{-1}\varphi'$ (from §163), and since the field $(AB)\pi$ is of degree n over $A\varphi$ according to II, as a result of III there could be no permutation of $(AB)\pi$ which is at the same time a multiple of $\varphi^{-1}\varphi'$, other than these n permutations $\pi^{-1}\pi'$ under which $(AB)\pi$ transforms into the n fields $(AB)\pi'$; thus $A\varphi$ is the field and $\varphi^{-1}\varphi'$ is the remainder of the system $\pi^{-1}\Pi'$. –

[xv] If $f(t)$, $F(t)$, $f_1(t)$ ... denote (as in §164) polynomial functions of the variable t whose coefficients c are contained in A, and if the functions $\mathfrak{f}(t)$, $\mathfrak{F}(t)$, $\mathfrak{f}_1(t)$ ... result from replacing each coefficient c with $c' = c\varphi$, then because φ is a *permutation* of A, the identities $\mathfrak{F}(t) + \mathfrak{F}_1(t) = \mathfrak{F}_2(t)$, $\mathfrak{F}(t)\mathfrak{F}_1(t) = \mathfrak{f}(t)\mathfrak{f}_1(t) + \mathfrak{F}_3(t)$ always follow from the identities $F(t) + F_1(t) = F_2(t)$, $F(t)F_1(t) = f(t)f_1(t) + F_3(t)$. Herein lies manifest a proof of rules (8) and (9), of which that given above in the text is only a circumlocution.

Henceforth we want to consider only the special case in which φ is the *identity* permutation of A; then the *identity* permutations of AB, B are obviously also contained in the systems Π, Ψ; A is the collection of all numbers in AB which map *to themselves* under every permutation π, and just the same D is the collection of all numbers in B which map to themselves under every permutation ψ. Now if T denotes an arbitrary sequence of n numbers $\omega_1, \omega_2, \ldots, \omega_n$ contained in AB, and $\pi_1, \pi_2, \ldots, \pi_n$ are the permutations in Π in a particular ordered sequence, then we want to set the determinant formed from the n^2 elements $\omega_r \pi_s$

$$\left| \begin{array}{cccc} \omega_1\pi_1, & \omega_2\pi_1, & \ldots, & \omega_n\pi_1 \\ \omega_1\pi_2, & \omega_2\pi_2, & \ldots, & \omega_n\pi_2 \\ \vdots & \vdots & \ddots & \vdots \\ \omega_1\pi_n, & \omega_2\pi_n, & \ldots, & \omega_n\pi_n \end{array} \right| = (T) \tag{10}$$

and for brevity call it the *determinant of the system* T. Then the following theorem holds:

IV. The necessary and sufficient condition for the system T to be irreducible over A and thus form a basis of AB is that the determinant (T) does not vanish; and the quotient of any two such determinants (T) is contained in A.

For if T is *irreducible*, then every number α in the family AB can be represented in the form

$$\alpha = x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n, \tag{11}$$

where the numbers x_r denote the coordinates of α contained in A, and consequently

$$\alpha\pi_s = x_1(\omega_1\pi_s) + x_2(\omega_2\pi_s) + \cdots + x_n(\omega_n\pi_s). \tag{12}$$

at the same time.

Now if U is a system of n such numbers $\alpha_1, \alpha_2, \ldots, \alpha_n$, and $a_{r,s}$ is the s^{th} coordinate of α_r, then

$$\begin{array}{c} \alpha_r = a_{r,1}\omega_1 + a_{r,2}\omega_2 + \cdots + a_{r,n}\omega_n \\ \alpha_r\pi_s = a_{r,1}(\omega_1\pi_s) + a_{r,2}(\omega_2\pi_s) + \cdots + a_{r,n}(\omega_n\pi_s) \end{array} \tag{13}$$

and as a result of the well-known theorem of determinant-theory

$$(U) = a(T), \tag{14}$$

where a denotes the determinant

$$a = \left| \begin{array}{cccc} a_{1,1}, & a_{1,2}, & \ldots, & a_{1,n} \\ a_{2,1}, & a_{2,2}, & \ldots, & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1}, & a_{n,2}, & \ldots, & a_{n,n} \end{array} \right| \tag{15}$$

formed from the coordinates $a_{r,s}$, and thus is contained in A. Now since, according to an earlier theorem (at the end of § 161), there certainly exists a system U in AB whose determinant (U) does not vanish, it follows from (14) that (T)

is non-zero.[xvi] If, on the other hand, T is *reducible*, then there exist n numbers x_r in A which do not all vanish, for which however the sum α in (11), hence also all n sums $\alpha\pi_s$ in (12), do vanish, and from here it is known that $(T) = 0$ as well, which was to be proven.

By the *norm* with respect to A of the field B we mean the product P of the n conjugate fields $B\pi$ or $B\psi$, into which B transforms under the n permutations ψ of the system Ψ; since the identity permutation of B is found among these, the norm P is always a multiple of B. Obviously AP is at the same time the norm of AB, because $A\pi = A$, hence $(AB)\pi = A(B\psi)$, and from the proof of the foregoing theorem the following easily results:

V. If P is the norm of the field B over A, and Q is the greatest common divisor of P and A, then $(B, A) = (B, Q)$.

For if one selects from B a system T of n numbers ω_1, ω_2, ..., ω_n which is irreducible over A, then every number α of the field B is representable in the form (11); now since the determinant (T) does not vanish, and since all numbers $\alpha\pi$, $\omega_r\pi$ appearing in (12) are contained in P, the same holds of the coordinates x_r, which therefore certainly belong to the field Q; the system T, which is irreducible over A and hence also over Q, thence becomes reducible over Q by the addition of any number α contained in B, and therefore $(B, Q) = n$, which was to be proven.

If, furthermore, θ denotes an arbitrary number in AB, and T denotes the system of n powers θ^{n-1}, θ^{n-2}, ..., θ, 1, then the determinant (T) is, as we have already observed earlier (at the end of § 161), the product of all the differences $\theta\pi_r - \theta\pi_s$ where $r < s$, and therefore the system T is *irreducible* over A if and only if θ is an *n-valued* number in Π; now since every number contained in AB is (according to § 164, VIII) algebraic over A and at most of degree n, it follows from here that *every n-valued number θ, and no other, is of degree n.* Furthermore, since the system Ψ consists of n distinct permutations ψ of the field B, there exist (according to §161) infinitely many numbers θ which are n-valued in Ψ, hence also in Π, and we can thus state the following theorem:

VI. If B is a field of n^{th} degree over A, then there also exist infinitely many numbers θ of degree n over A in B, and at the same time $A(\theta) = AB$.

Conversely, if a field B consists only of numbers which are algebraic over A, and whose degrees do not exceed a finite height, then it follows without difficulty from the preceding theorems that B is *finite* over A. Another, likewise characteristic, criterion for this finiteness is that the *number* of all the distinct fields K which are simultaneously multiples of A and divisors of AB is *finite*. Here, however, we want to elaborate on only the one part of this theorem, [indem] we again suppose that B is of degree n over A and designate with Π the system of n permutations π of AB which are multiples of the *identity* permutation φ of A; if ones sets $(AB, K) = p$, $(K, A) = q$, then $n = pq$ and K is (according to VI) of the form $A(\alpha)$, where α denotes a number of degree q contained in K, hence also in AB, and conversely every number α in AB produces such a field $K = A(\alpha)$. Now there are (according to III) q distinct

[xvi] Compare this with theorem IV in §164.

permutations χ of K which are multiples of φ, and under which α transforms into q distinct values $\alpha\chi$; each particular such permutation χ is again the remainder of a system Π' of p permutations π' which produce one and the same value $\alpha\pi' = \alpha\chi$, and the system Π consists of these q complexes Π'. Now since, conversely, K is completely determined (according to §163) as the field belonging to every single complex Π', it follows easily that the number of such fields K is finite, because a finite system Π also has only a finite number of parts Π'. – For the sake of brevity we must forego the proof of the converse, which admittedly is not difficult, but does require several lemmas.

Now the complete determination of all these fields K and the investigation of their mutual relations forms the most important task of algebra, whose solution began with LAGRANGE[xvii] and finally was brought to a systematic conclusion by GALOIS[xviii] through the *theory of groups*. Although we cannot expand upon the latter ourselves, we still want to indicate from our standpoint what this reduction consists in.

§ 166. GROUPS OF PERMUTATIONS

A system Π of n different field permutations π is called a *group [Gruppe]* if any one can be composed with any other, and the resultant is always contained in Π.

From this definition it follows first that the permutations π contained in a group Π all refer to one and the same field, and that this field M maps into itself under each permutation π. If, furthermore, π' denotes a particular one of these n permutations, while we let π range over all of them, then the n resultants $\pi\pi'$ are (according to §162) all distinct, and therefore their complex is identical to Π; there exists therefore, if π', π'' are two particular permutations, always one and only one permutation π which meets the condition $\pi\pi' = \pi''$. If one takes $\pi' = \pi''$, it then follows that the identity permutation on M is also contained in Π. The following fundamental theorem is based on these properties of a group:

I. If a group Π consists of n distinct permutations π of the field M, and if A is the field of Π, then $(M, A) = n$, and the remainder of Π is the identity permutation of A.

In order to prove this, we select (according to §161) a system of n numbers α_r from M in such a way that the determinants formed from the n^2 numbers $\alpha_r\pi$ do not vanish; then, if ω denotes any determinate number in M, there exists one and only one system of n numbers x_r which satisfy the n linear equations

$$\omega\pi = x_1(\alpha_1\pi) + x_2(\alpha_2\pi) + \cdots + x_n(\alpha_n\pi); \tag{1}$$

since all numbers $\omega\pi, \alpha\pi$ appearing here are contained in M, the same also holds for these n numbers x_r, and consequently, if π' denotes a particular permutation

[xvii] *Réflexions sur la résolution algébrique des équations* (Mém. de l'Acad. de Berlin, 1770, 1771. – Œuvres de L. Tome III) [22].

[xviii] *Sur les conditions de résolubilité des équations par radicaux* (Liouvilles Journal, t. XI, 1846) [16].

in Π, there arises from the above system (1) the following:

$$\omega\pi\pi' = (x_1\pi')(\alpha_1\pi\pi') + (x_2\pi')(\alpha_2\pi\pi') + \cdots + (x_n\pi')(\alpha_n\pi\pi'),$$

which, because $\pi\pi'$ ranges over the whole system Π while π does, can also be represented in the form

$$\omega\pi = (x_1\pi')(\alpha_1\pi) + (x_2\pi')(\alpha_2\pi) + \cdots + (x_n\pi')(\alpha_n\pi);$$

in concert with (1) it results from here that $x_r\pi' = x_r$, and therefore the n numbers x_r are contained in the field A, which (according to §163) consists of all numbers that are one-valued in Π. Since the identity permutation of M is found among the permutations π, it follows from (1) that every number ω of the field M is representable in the form

$$\omega = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n,$$

where the coefficients x_r belong to the field A; hence M is finite over A, namely $(M, A) \leq n$; since there exist n *distinct* permutations π of M which are multiples of the identity permutation of A, it follows (from §165, III) that $(M, A) = n$, and that the system of the n numbers α_r is *irreducible* over A, which was to be proven.

Now if a part of the group Π likewise forms a group Π', which consists of p permutations π', then the field A' of Π' is a divisor of M and a multiple of A, because each number one-valued in Π is also one-valued in Π', and at the same time $n = pq$, where $p = (M, A')$, $q = (A', A)$; when π denotes a particular permutation in Π but π' ranges over all permutations of the group Π', if one further designates by $\Pi'\pi$ the complex of the p resultants $\pi'\pi$, and by φ' the remainder of $\Pi'\pi$, then the group Π consists of q distinct complexes $\Pi'\pi$, whose remainders φ' agree with those q permutations of the field A' which are multiples of the identity permutation of A. Conversely, if a field A' is a divisor of M and a multiple of A, one easily sees that the permutations of M which are multiples of the identity permutation of A' form a group Π' contained in Π, and A' is the field belonging to Π'. If, furthermore, Π'' is likewise a group contained in Π, and A'' is the field belonging to it, then the permutations common to both groups Π', Π'' again form a group; and the field belonging to it is the product $A'A''$.

From this one recognizes that the complete determination of all these fields $A', A'', \ldots$ and the investigation of their mutual relations is completely settled by the determination of all groups $\Pi', \Pi'', \ldots$ contained in the group Π, and this task belongs to the general[xix] theory of groups.

Now the general case (§165), where $(B, A) = n > 0$, and where it is a matter of the classification of all fields K which are simultaneously multiples of A and divisors of AB, is easily reduced to the foregoing. If φ again denotes the *identity* permutation of A, and Π the system of n permutations π of AB

[xix] Already in my Göttingen lectures (1857-1858) I taught this theory as applying to groups Π of *arbitrary elements* π.

which are multiples of φ, then we have already noted that the norm of B, i.e. the product P of the n fields $B\pi$, is a multiple of B. If now $P = B$, so B is its own norm, we should call B a *normal field [Normalkörper]* over A; this case occurs if and only[xx] if all fields $B\pi$ are identical with B, and obviously AB is also normal over A then. If now the latter is the case–which, as we still want to note, can also occur without B being normal over A–, then one can easily convince himself that Π is a *group*, and that everything said above about the field M holds for this field AB. But if AB (and hence also B) is not normal over A, nevertheless the norm P of B, and hence also AP, is normal over A; namely if χ is a particular permutation of AP, to be precise a multiple of φ, then the divisors of χ with respect to the n fields $AB\pi$ are (according to §165) of the form $\pi^{-1}\pi'$, where π' ranges over *all* permutations contained in Π simultaneously with π,[xxi] and thus $(AP)\chi = AP$, i.e. AP (and likewise P as well) is normal over A, the system X of all permutations χ is a group, φ is their remainder, and the principles above hold for the field $M = AP$.

From here, incidentally, there follows as well the important theorem that, if ω denotes an arbitrary number contained in AB, any number derived from the n numbers $\omega\pi$ in a rational and *symmetric* way is certainly contained in A, because it is obviously *one-valued* in X.

[xx] At first, admittedly, there follows only that each field $B\pi$ must be a divisor of B; however, since (according to §164) each number ω in B is algebraic over A, and since the numbers of the infinite range ω, $\omega' = \omega\pi$, $\omega'' = \omega'\pi$, $\omega''' = \omega''\pi$, ... are contained in B and are roots of one and the same irreducible (over A) equation, repetitions of the form $\omega^{(r)} = \omega^{(r+s)}$, where $s > 0$, must occur among them, and since $\alpha = \beta$ always follows from $\alpha\pi = \beta\pi$, it follows that $\omega = \omega^{(s)}$, and thus every number ω contained in B is also contained in $B\pi$, hence $B\pi = B$. – In order to set this consideration in the right light, we still note the following. If τ, τ' are two arbitrary *transcendental*, i.e. non-algebraic, numbers over A, then the field $A(\tau)$ transforms into $A(\tau')$ under infinitely many permutations which are multiples of the identity permutation of A, and among these there is a single π for which $\tau\pi = \tau'$; if one now takes e.g. $\tau' = \tau^2$, then it is readily apparent that the field $A(\tau^2)$ conjugate to $A(\tau)$ is a *proper* divisor of $A(\tau)$.

[xxi] For if one selects an arbitrary n-valued number θ from AB, then the n distinct numbers $\theta\pi$ contained in AP must also map into n distinct images $\theta\pi'$ under the permutation χ (according to §161); the permutation χ thus produces a certain permutation [Vertauschung] of the n values among themselves.

References

[1] E. Artin, *Galois Theory*, University of Notre Dame Press, 1st ed., 1942. 12

[2] J. Avigad, *Dedekind's 1871 version of the theory of ideals*, Tech. Rep. CMU-PHIL-162, Carnegie Mellon University, 2004. 16

[3] ——, *Methodology and metaphysics in the development of Dedekind's theory of ideals*, in The Architecture of Modern Mathematics, J. Ferreirós and J. Gray, eds., Oxford Univeristy Press, 2006, pp. 159–186. 16

[4] P. Bachmann, *Die Lehre von der Kreistheilung und ihre Beziehungen zur Zahlentheorie*, B. G. Teubner, 1st ed., 1872. 31

[5] R. Dedekind, *Anzeige von P. Bachmann*, Literaturzeitung der Zeitschrift für Mathematik und Physik, 18 (1873), pp. 14–24. 31

[6] ——, *Sur la Théorie des Nombres entiers algébriques*, Gauthier-Villars, 1877. 16, 42

[7] ——, *Zur Theorie der aus n Haupteinheiten gebildeten komplexen Größen*, in Nachrichten von der Göttinger Gesellschaft der Wissenschaften, 1885, pp. 141–159. 30

[8] ——, *Was sind und was sollen die Zahlen?*, Friedrich Vieweg und Sohn, 1888. 20

[9] ——, *Über die von drei Moduln erzeugte Dualgruppe*, Mathematische Annalen, 53 (1900), pp. 371–403. 4

[10] ——, *Über Zerlegungen von Zahlen durch ihre grössten gemeinsamen Teiler*, in Gesammelte mathematische Werke, vol. II, Chelsea, 1968, pp. 103–148. 4

[11] ——, *Theory of Algebraic Integers*, Cambridge University Press, 2004. Translation of [6] by John Stillwell. 16

[12] R. Dedekind and H. Weber, *Theorie der algebraischen Funktionen einer Veränderlichen*, Journal für die reine und angewandte Mathematik, 92 (1882), pp. 181–290. 18

[13] P. G. L. Dirichlet, *Verallgemeinerung eines Satzes aus der Lehre von den Kettenbrüchen nebst einigen Anwendungen auf die Theorie der Zahlen*, in G. Lejeune Dirichlet's Werke, L. Kronecker, ed., vol. I, G. Reimer, 1889, pp. 633–638. 27

[14] P. G. L. Dirichlet and R. Dedekind, *Vorlesungen über Zahlentheorie*, Friedrich Vieweg und Sohn, 4th ed., 1894. 1, 43

[15] ——, *Lectures on Number Theory*, American Mathematical Society, 1999. Translation, by John Stillwell, of the 1863 1st edition of [14]. 16

[16] É. Galois, *Sur les conditions de résolubilité des équations par radicaux*, Journal de Mathématiques Pures et Appliquées, 11 (1846), pp. 417–444. 39

[17] C. F. Gauss, *Disquisitiones Arithmeticae*, Yale University Press, 1965. English translation by Arthur A. Clarke. 2

[18] T. W. Hungerford, *Algebra*, Springer, 1974. 3

[19] B. M. Kiernan, *The development of Galois theory from Lagrange to Artin*, Archive for History of Exact Sciences, 8 (1971), pp. 40–154. 2, 13, 16

[20] L. Kronecker, *Grundzüge einer arithmetischen Theorie der algebraischen Grössen*, Journal für die reine und angewandte Mathematik, 92 (1882), pp. 1–122. 18

[21] E. Kummer, *Zur Theorie der komplexen Zahlen*, Journal für die reine und angewandte Mathematik, 35 (1847), pp. 319–326. 18

[22] J. L. Lagrange, *Réflexions sur la résolution algébrique des équations*, in Œuvres de Lagrange, Tome III, J. A. Serret, ed., Gauthier-Villars, 1867, pp. 205–421. 39