

# Algebraic Theory of Fields.

By *Ernst Steinitz*.

With two appendices by *Reinhold Baer* and *Helmut Hasse*.

**About this edition.** This volume contains Ernst Steinitz's *Algebraische Theorie der Körper*, first published in the *Journal für die reine und angewandte Mathematik*, vol. 137 (1910), pp. 167–309, in English translation; and, as Appendix A and Appendix B, the *Abriß der Galoisschen Theorie* and the *Erläuterungen* by Reinhold Baer and Helmut Hasse, which accompanied the reissue of the paper (Berlin: W. de Gruyter, 1930), likewise in English. The appendices are not by Steinitz.

The translation renders the sense in natural English and keeps close to the German; Steinitz's own terms are kept. Footnotes marked *\**), *\*\**), . . . are the authors' own: Steinitz's in the paper, Baer and Hasse's in the appendices. Numbered footnotes, signed "Trans.", give the modern term for some of Steinitz's.

A gray superscript such as <sup>E57</sup> marks a place on which an Explanatory Note (Appendix B) comments; it links to the note, and the note's number links back. Every cross-reference — Steinitz's own, and those of the two appendices — refers to this edition and is a link, as are the entries of the table of contents and the PDF bookmarks. Obvious misprints have been corrected without comment, and the table of contents, which the original prints at the end, stands at the front.

# Contents

|                                                                                                                                                                        |     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Introduction . . . . .                                                                                                                                                 | 3   |
| I. FOUNDATIONS.                                                                                                                                                        |     |
| § 1. Systems with double composition. Isomorphism. Fields. . . . .                                                                                                     | 5   |
| § 2. Subfields, extension, adjunction. . . . .                                                                                                                         | 7   |
| § 3. Domains of integrity. . . . .                                                                                                                                     | 9   |
| § 4. Prime fields. Characteristic. . . . .                                                                                                                             | 10  |
| § 5. Equivalent extensions. Simple extensions. Transcendental and algebraic elements. Adjunction of a transcendental element. Integral and rational functions. . . . . | 12  |
| § 6. Adjunction of an algebraic element. . . . .                                                                                                                       | 19  |
| II. ALGEBRAIC EXTENSIONS.                                                                                                                                              |     |
| § 7. Foundations of algebraic extensions. . . . .                                                                                                                      | 22  |
| § 8. Decomposition of an arbitrary integral function into linear factors. Normal fields and normal functions. . . . .                                                  | 26  |
| § 9. Differentiation. . . . .                                                                                                                                          | 30  |
| § 10. The multiplicity of the zeros of an integral function. . . . .                                                                                                   | 32  |
| § 11. Perfect and imperfect fields. . . . .                                                                                                                            | 36  |
| § 12. Imperfect fields: Smallest containing and greatest contained perfect field. — Root fields. . . . .                                                               | 40  |
| § 13. Imperfect fields: Algebraic extensions of the first kind. . . . .                                                                                                | 44  |
| § 14. Imperfect fields: Arbitrary algebraic extensions, theorem of primitive elements and theorem of intermediate fields. . . . .                                      | 48  |
| § 15. Finite fields. . . . .                                                                                                                                           | 54  |
| III. INFINITE ALGEBRAIC EXTENSIONS.                                                                                                                                    |     |
| § 16. The absolutely algebraic fields of prime-number characteristic. . . . .                                                                                          | 56  |
| § 17. Algebraically closed fields. . . . .                                                                                                                             | 63  |
| § 18. Relations between systems of integral functions and extension fields. . . . .                                                                                    | 64  |
| § 19. Auxiliary considerations from set theory. . . . .                                                                                                                | 68  |
| § 20. The immediate applications. . . . .                                                                                                                              | 70  |
| § 21. The fundamental theorem of algebraic extensions. . . . .                                                                                                         | 75  |
| IV. TRANSCENDENTAL EXTENSIONS.                                                                                                                                         |     |
| § 22. Transcendental extensions. Algebraic dependence between elements of an extension field. . . . .                                                                  | 81  |
| § 23. The degree of transcendence and the division of fields into classes. . . . .                                                                                     | 84  |
| § 24. Supplementary remarks of various content. . . . .                                                                                                                | 89  |
| APPENDICES                                                                                                                                                             |     |
| A. Outline of Galois Theory . . . . .                                                                                                                                  | 95  |
| B. Explanatory Notes . . . . .                                                                                                                                         | 106 |

In the present essay the concept “field” is conceived in the same abstract and general manner as in *H. Weber’s investigations on the general foundations of the Galois theory of equations*<sup>\*)</sup>, namely as a system of elements with two operations: addition and multiplication, which are subject to the associative and commutative law, are connected by the distributive law, and admit unrestricted and unique inversions<sup>\*\*)</sup>. *Weber’s* goal, however, is a general treatment of *Galois* theory, independent of the numerical meaning of the elements, whereas for us the concept of field itself stands at the centre of interest. *To obtain a survey of all possible field types*<sup>1</sup> and to establish their relations to one another in their basic features may count as the programme of this work<sup>\*\*\*)</sup>. Since the distinctions between integral and fractional quantities, which belong to arithmetic in the narrower sense, were not to be pursued further here, the title *Algebraic Theory of Fields* was chosen.

The tendency characterized here also marks out the path we have to take. We shall start from the formation of the simplest fields and then consider the methods by which one passes, by extension, from a given field to a more comprehensive one. The first task leads to the concept of the *prime field* and to a distinction of fields according to the *characteristic*. Every field contains a smallest field, or prime field; this is either of the type of the field of rational numbers (characteristic 0) or of the type of the system of residue classes of a prime number  $p$  (characteristic  $p$ ). For many questions the characteristic is without significance, but for others there is a profound difference between the fields of characteristic 0 and those of prime-number characteristic. Considering the so-called *simple* extensions, which can be obtained by adjunction of a single element, gives occasion for an analogous distinction. According as such an element satisfies an algebraic equation of the ground field or not, it is called *algebraic* or *transcendental* (with respect to the ground field). By an *algebraic extension* we understand, quite generally, any extension all of whose elements are algebraic, while every other extension is called *transcendental*. The algebraic extensions include the *finite* ones, which are characterized by the fact that a finite number of elements of the extension field suffice to represent all elements linearly and homogeneously with coefficients from the ground field. In the literature, only these extensions are usually called algebraic. The investigations belonging here form the content of *Galois* theory.<sup>E 1</sup>

Following the precedent of *Cauchy*, who showed that the introduction of the complex numbers can be circumvented by considerations of congruences with respect to the modulus  $x^2 + 1$ <sup>\*\*\*\*)</sup>, *Kronecker* has proved that any introduction of irrationalities in the treatment of algebraic problems<sup>\*\*\*\*\*)</sup> can also be avoided if one replaces the equations by congruences with respect to modular systems<sup>2</sup>. We use *Kronecker’s* idea in order first of all to prove that for a field  $\mathfrak{K}$  and a function  $\varphi(x)$  irreducible in  $\mathfrak{K}$  an extension field can be found which arises from  $\mathfrak{K}$  by adjunction of a zero of  $\varphi(x)$ . In doing so, however, we pass from the notation of *congruences* back to *equations*, by introducing a symbol by means of which we represent

\*) Math. Ann. 43, p. 521.

\*\*) Only division by zero is to be excluded.

\*\*\*) I was stimulated to undertake these general investigations in particular by *Hensel’s* Theorie der algebraischen Zahlen (Leipzig, 1908), in which the field of  $p$ -adic numbers forms the starting point, a field which is to be counted neither among the function fields nor among the number fields in the ordinary sense of the word.

\*\*\*\*) Exerc. d’anal. et de phys. math. 4 (1847), p. 87.

\*\*\*\*\*) With *Kronecker* it is always only a matter of problems which require *finite* extensions.

<sup>1</sup> In modern terms: *isomorphism type*. — Trans.

<sup>2</sup> German: *Modulsystem*. In modern terms, roughly: *ideal* of a polynomial ring. — Trans.

all elements of the extension field and which itself becomes a zero of  $\varphi(x)$ . The further investigations build synthetically on this first result. The method followed here may count as just as *purely arithmetical* as the method of congruences, to which the transition is of course always possible and, even if at times inconvenient, yet cannot possibly be missed.

In the area of finite extensions, one fact especially deserves emphasis: *Galois* theory, as we find it for the algebraic number fields, does not hold for all fields in its full extent. For a large part of that theory rests on the theorem that every equation with vanishing discriminant (multiple zeros) must be reducible. But precisely this theorem does not hold generally. This gives us occasion to divide the fields into *perfect* and *imperfect* ones.<sup>E 2</sup> All fields of characteristic 0 belong to the former; of the fields of characteristic  $p$ , only those within which the extraction of the  $p$ -th root is possible without exception do so. I have gone somewhat further into the properties of the imperfect fields — whose laws deviate in part from the ordinary *Galois* theory — than would have been absolutely necessary for the continuing investigation. The fields with only finitely many elements further required special treatment. Although in them, as in all other perfect fields, the theorems of *Galois* theory hold without restriction<sup>\*)</sup>, the proof must nevertheless in part be conducted differently.

Under the title “*a fundamental theorem of general arithmetic*” *Kronecker* has published in this Journal<sup>3</sup> an essay<sup>\*\*)</sup> which is concerned with the determination of a prime modular system<sup>4</sup> for which a given integral function<sup>5</sup> of one variable can be represented as a product of linear factors. That the existence of such a prime modular system is of fundamental significance for general arithmetic is beyond question; the reference to the fundamental theorem of algebra, by which *Kronecker* justifies the designation of his theorem as a fundamental theorem, appears, however, not entirely apt. The fundamental theorem of algebra gives more; its counterpart, in the area of general arithmetic, would be the proof of a prime modular system for which *every* function of the domain of rationality under consideration breaks up into linear factors. The treatment of this problem lay outside the circle of *Kronecker*’s investigations insofar as its settlement requires the introduction of *infinitely many* indeterminates. If we translate the problem into our mode of expression, then it is a matter of extending a given field to an *algebraically closed* one, i.e. one in which every integral function of one indeterminate breaks up into linear factors. This task belongs to the area of *infinite* algebraic extensions; it is solved in § 16 first for the case of a prime field of prime-number characteristic. The method used here is also applicable in other cases, such as the natural domains of rationality<sup>6</sup>, the only ones *Kronecker* considered; it requires no recourse to principles that would not be recognized by all mathematicians. The situation is different for the proof that our task, provided one further demands that the extension field contain no superfluous elements, has essentially<sup>\*\*\*)</sup> only *one* solution. This proof cannot, e.g., be carried out even for the field of rational numbers without use of the *principle of choice*. This principle also appears unavoidable if one wishes to carry

<sup>\*)</sup> This holds also, e.g., with regard to the questions settled by *Weber* for fields with infinitely many elements but left open for finite fields; see the end of the cited work.<sup>E 3</sup>

<sup>\*\*) Vol. 100, p. 490. = Werke III, I, p. 209.</sup>

<sup>\*\*\*)</sup> For the precise definition of this expression see § 5.

<sup>3</sup> The Journal für die reine und angewandte Mathematik (“Crelle’s Journal”), in which the present paper first appeared; so also below. — Trans.

<sup>4</sup> German: *Primmodulsystem*. In modern terms, roughly: *prime ideal* of a polynomial ring. — Trans.

<sup>5</sup> In modern terms: *polynomial*. — Trans.

<sup>6</sup> German: *natürlicher Rationalitätsbereich*. — Trans.

out the proof of the existence of an algebraically closed extension for *every arbitrary* field. The *well-ordering theorem* of Zermelo, which rests on the principle of choice, is an essential tool for this proof<sup>\*)</sup>. — Many mathematicians are still opposed to the principle of choice. With the increasing recognition *that there are questions in mathematics that cannot be decided without this principle*, resistance to it may well disappear more and more. On the other hand, it appears expedient, in the interest of the purity of the method, to avoid that principle so far as the nature of the question does not require its application. I have endeavoured to let this boundary stand out sharply.

This applies also to the discussions of the last part, which deals with the *transcendental* extensions. Among these the *purely transcendental* ones appear as the simplest. A purely transcendental extension amounts essentially to the adjunction of indeterminates, which may form a finite or also an infinite set of arbitrary power<sup>7</sup>. The well-ordering theorem leads at once to the recognition that every extension can be decomposed into a purely transcendental and an algebraic one.

From here we can easily characterize the position that the fields considered by Kronecker occupy within the totality of fields. For Kronecker the concept of field develops in three stages<sup>\*\*)</sup>. The starting point is the “*absolute domain of rationality*”<sup>8</sup>, that is, the field of rational numbers, thus a particular prime field. From it one arrives, by adjunction of a finite number of indeterminates — thus by a special purely transcendental extension — at the “*natural domain of rationality*”; from this, finally, by adjunction of an algebraic quantity, i.e. by a special algebraic extension, one arrives at the “*domain of genus*”<sup>9</sup>. — If instead one starts from an *arbitrary* prime field and carries out an *arbitrary* purely transcendental extension, followed by an *arbitrary* algebraic extension, then one thereby has a procedure by which one can reach *every* field.

The present essay treats only the *basic features* of a general theory of fields. I intend to let further-reaching investigations, as well as applications to geometry, number theory and function theory, follow in some further treatises.<sup>E 4</sup>

*Summary of contents:* I. Foundations (§§ 1—6.); II. Algebraic extensions (§§ 7—15.); III. Infinite algebraic extensions (§§ 16—21.); IV. Transcendental extensions (§§ 22—24.). — (Detailed table of contents at the beginning of the work.)

## § 1.

### Systems with double composition. Isomorphism. Fields.

If  $\mathfrak{S}$  denotes a system of elements, then by a *law of composition of the system*  $\mathfrak{S}$  we understand any stipulation that assigns to every pair  $a, b$  of elements of this system — which may also be equal — an element  $c$  of the same system. — By a *system with double composition* we understand one for which *two* laws of composition are given, which we call *addition* and *multiplication*. Addition assigns to any two elements  $a, b$  their *sum*  $a + b$ , multiplication their *product*  $a \cdot b$ .

<sup>\*)</sup> The first application of the well-ordering theorem to an arithmetical problem is found, to my knowledge, in Hamel, Mathem. Ann. 60, p. 459.

<sup>\*\*)</sup> Festschrift zu Kummers Doktorjubiläum § 1—3. This Journal. Vol. 92, p. 1. = Werke II, p. 237.

<sup>7</sup> In modern terms: *cardinality*. — Trans.

<sup>8</sup> German: *absoluter Rationalitätsbereich*. — Trans.

<sup>9</sup> German: *Gattungsbereich*. — Trans.

*Isomorphism.* Two systems  $\mathfrak{S}_1, \mathfrak{S}_2$  with double composition are called *isomorphic* or *of the same (composition) type* if it is possible to relate their elements to one another one-to-one in such a way that the sum and the product of any two elements of one system always correspond, in the other, to the sum and the product of the corresponding elements; the correspondence itself is called an isomorphic one or isomorphism.<sup>E5</sup>

*Fields.* — So far we have subjected the two laws of composition to no further condition than that of single-valuedness. If we introduce further conditions, we arrive at particular kinds of systems with double composition. Among these, of particular importance are the *domains of rationality* (Kronecker) or *fields* (Dedekind), systems which satisfy the following 7 conditions:

1. *The associative law of addition:*

$$(a + b) + c = a + (b + c),$$

2. *the commutative law of addition:*<sup>E6</sup>

$$a + b = b + a,$$

3. *the associative law of multiplication:*

$$(a \cdot b) \cdot c = a \cdot (b \cdot c),$$

4. *the commutative law of multiplication:*

$$a \cdot b = b \cdot a,$$

5. *the distributive law:*

$$a(b + c) = ab + ac,$$

6. *the law of unrestricted and unique subtraction:*

If  $a, b$  are elements of the system, then there is in it one and only one element  $x$  for which  $a + x = b$  holds. — Let this element be denoted by  $b - a$  and called the *difference* of  $a$  and  $b$ , so that in general  $a + (b - a) = b$  holds.

Before we set up the seventh and last condition, we draw some simple consequences from the preceding ones. Let  $a, b$  be any two elements of our system. If we put  $a - a = x$ ,  $b - b = y$ , then by 6. the equations:  $a + x = a$ ,  $b = b + y$  hold, and if we add these, applying 1. and 2. gives  $(a + b) + x = (a + b) + y$ , and from this, by 6.,  $x = y$ , or  $a - a = b - b$ . There is thus a distinguished element — we call it *zero* (0) —, which is represented by every difference of the form  $a - a$ . — If  $a, b$  again denote arbitrary elements of the system, then  $a \cdot b = a(b + 0) = a \cdot b + a \cdot 0$ , hence  $a \cdot 0 = a \cdot b - a \cdot b = 0$ , i.e.: *a product in which one factor is 0 is itself 0.* — We now give the last condition:

7. *the law of unrestricted and unique division:*

The system contains besides 0 at least one more element, and if  $a$  is an element different from 0,  $b$  an arbitrary element of the system, then there is in it one and only one element  $x$  for which  $a \cdot x = b$  holds.<sup>E7</sup> — We call  $x$  the *quotient* of  $b$  and  $a$ , in symbols  $x = \frac{b}{a}$  or  $= b : a$ .

If all 7 conditions are satisfied, the system is called a *field*. Examples of fields are the systems of the rational, of the real, of the complex numbers etc. The significance of the stated conditions rests on the fact that all laws prevailing in the named fields, so far as they

are expressible by equations between aggregates<sup>10</sup> that are composed rationally from their elements, appear as consequences of those conditions and are therefore found again in all fields. Without carrying this out in all details, we nevertheless wish to emphasize here some of the essential points: If  $a, b$  are two elements of a field  $\mathfrak{K}$  that are different from 0, then by 7.  $a \cdot b$  is different from  $a \cdot 0 = 0$ , i.e. *a product is equal to 0 only if at least one factor vanishes*. — If  $a$  and  $b$  are different from 0 and we determine  $x$  and  $y$  by the conditions  $a \cdot x = a$ ,  $b \cdot y = b$ , then it follows that  $(ab)x = b(ax) = ba = (by)a = (ab)y$ ,  $(ab)x = (ab)y$ , consequently by 7.  $x = y$ . If we therefore denote the solution of the equation  $ax = a$  by  $\varepsilon$ , then  $\varepsilon$  is the only element of  $\mathfrak{K}$  with the property that multiplying it by any element of  $\mathfrak{K}$  leaves that element unchanged, and it is represented by every quotient of the form  $\frac{a}{a}$  ( $a \neq 0$ ). This distinguished element we call the *unity*; we shall always denote it by  $\varepsilon$ <sup>E 8</sup>.

The fundamental theorems of the theory of determinants are also among the theorems whose proof can be carried out solely on the basis of the stated 7 conditions. In particular, the following holds for every field  $\mathfrak{K}$ :

- 1)  $n$  linear equations in  $n$  unknowns

$$\sum_{k=1}^n a_{ik}x_k = c_i, \quad (i = 1, \dots, n)$$

in which the coefficients  $a_{ik}, c_i$  are given elements from  $\mathfrak{K}$ , have, if the determinant  $|a_{ik}|$  is not 0, one and only one system of solutions in  $\mathfrak{K}$ .

- 2)  $n$  homogeneous linear equations in  $n + 1$  unknowns

$$\sum_{k=0}^n a_{ik}x_k = 0 \quad (i = 1, \dots, n)$$

have at least one system of solutions whose elements are not all <sup>E 9</sup> 0.

Finally, let us point out right here that there are also fields that have only a *finite* number of elements. Thus the  $p$  residue classes that belong to a prime number  $p$  as modulus form a system with double composition that satisfies all 7 conditions and is thus a field in our sense.<sup>E 10</sup>

## § 2.

### Subfields, extension, adjunction.

A subsystem  $\mathfrak{K}'$  of a field  $\mathfrak{K}$  can, by virtue of the laws of composition prevailing in  $\mathfrak{K}$ , again represent a field. Obviously it is necessary and sufficient for this that, if  $\alpha$  and  $\beta$  are elements of  $\mathfrak{K}'$ , then  $\alpha + \beta$ ,  $\alpha - \beta$ ,  $\alpha \cdot \beta$  and, in case  $\beta \neq 0$ ,  $\frac{\alpha}{\beta}$  also belong to  $\mathfrak{K}'$ . We then say: *the field  $\mathfrak{K}$  comprises the field  $\mathfrak{K}'$ ,  $\mathfrak{K}'$  is contained in  $\mathfrak{K}$* , and call  $\mathfrak{K}'$  a *subfield* of  $\mathfrak{K}$ ,  $\mathfrak{K}$  an *extension field* or *extension* of  $\mathfrak{K}'$ . As a rule we shall count a field itself among its sub- and extension fields; where this is not the case, it will be apparent from the mode of expression (“actual extension”<sup>11</sup>, “proper subfield”, “only a subfield”) or from the context. — One now convinces oneself at once of the validity of the following theorem:

<sup>10</sup> In modern terms: *expression*. — Trans.

<sup>11</sup> In modern terms: *proper extension*. — Trans.

1. If  $\mathfrak{S}$  denotes a system of finitely or infinitely many subfields of a field  $\mathfrak{K}$ , then there are in  $\mathfrak{K}$  elements (e.g.  $0, \varepsilon$ ) that occur in all fields of the system  $\mathfrak{S}$ . The totality of these elements again represents a field.<sup>E11</sup>

We shall call this field the *intersection* of the system of fields  $\mathfrak{S}$ . — Alongside Theorem 1. there stands a second, no less important one:

2. If  $\mathfrak{U}$  denotes a system of finitely or infinitely many fields of such a nature that any two fields  $\mathfrak{K}_1, \mathfrak{K}_2$  from  $\mathfrak{U}$  are always contained in at least one field  $\mathfrak{K}_3$  of the system  $\mathfrak{U}$ , then there is a definite (not necessarily occurring in  $\mathfrak{U}$ ) field  $\mathfrak{K}$  that has all fields of the system  $\mathfrak{U}$  as subfields and contains no other elements than those that occur in fields of  $\mathfrak{U}$ .<sup>E12</sup>

Proof: Let  $\mathfrak{K}$  denote the system of all elements that occur in fields of the system  $\mathfrak{U}$ . If one has elements from  $\mathfrak{K}$  in finite number  $a_1, a_2, \dots, a_n$  and if  $\mathfrak{K}_i$  ( $i = 1, \dots, n$ ) is a field from  $\mathfrak{U}$  that contains  $a_i$ , then there is in  $\mathfrak{U}$  a field  $\mathfrak{K}'_2$  that contains  $\mathfrak{K}_1$  and  $\mathfrak{K}_2$ , a field  $\mathfrak{K}'_3$  that contains  $\mathfrak{K}'_2$  and  $\mathfrak{K}_3$ , etc. There are thus in  $\mathfrak{U}$  fields that contain all fields  $\mathfrak{K}_i$  ( $i = 1, \dots, n$ ) and therewith all elements  $a_i$ . If now  $a, b$  are any two elements from  $\mathfrak{K}$ , and  $\mathfrak{K}'$  is any field from  $\mathfrak{U}$  that contains  $a$  and  $b$ , then  $a + b$  and  $a \cdot b$  have a definite meaning in  $\mathfrak{K}'$ . If  $\mathfrak{K}''$  is any other field belonging to  $\mathfrak{U}$  and containing  $a$  and  $b$ , then  $a + b$  and  $a \cdot b$  also have a definite meaning in this one. But that  $a + b$  and  $a \cdot b$  can denote nothing different in  $\mathfrak{K}''$  than in  $\mathfrak{K}'$  is a consequence of the hypothesis that there is a field which contains  $\mathfrak{K}'$  and  $\mathfrak{K}''$ . Thus sum and product of two elements from  $\mathfrak{K}$  are unambiguously defined, i.e.  $\mathfrak{K}$  is a system with double composition.<sup>E13</sup> From the circumstance that any two elements from  $\mathfrak{K}$  occur simultaneously in fields from  $\mathfrak{U}$ , it now follows that the laws of composition 2. and 4. of § 1 hold, further, that at least one element  $x_1$ , and if  $a \neq 0$ , at least one element  $x_2$  occurs in  $\mathfrak{K}$  for which  $a + x_1 = b$ ,  $a \cdot x_2 = b$  holds. Since also three elements from  $\mathfrak{K}$  occur in one field from  $\mathfrak{U}$ , it follows that the laws of composition 1., 3. and 5. are also satisfied. Since finally the same holds also for 4 elements  $a, b, x, y$  from  $\mathfrak{K}$ , the equations  $a + x = b$ ,  $a + y = b$  and, if  $a \neq 0$ , also the equations  $a \cdot x = b$ ,  $a \cdot y = b$  can hold only if  $x = y$ . The system  $\mathfrak{K}$  is therefore a field, and it is immediately evident that  $\mathfrak{K}$  contains all fields from  $\mathfrak{U}$  and has only such elements as occur in the fields from  $\mathfrak{U}$ ; but equally also that a field that has these two properties must necessarily be identical with  $\mathfrak{K}$ .

If the field  $\mathfrak{K}$  is contained in the field  $\mathfrak{L}$ ,  $\mathfrak{S}$  any system of elements from  $\mathfrak{L}$ , then we denote by  $\mathfrak{K}(\mathfrak{S})$  the intersection of all those fields between\*)  $\mathfrak{K}$  and  $\mathfrak{L}$  that contain all elements of the system  $\mathfrak{S}$ . Of the field  $\mathfrak{K}(\mathfrak{S})$  we say that it has arisen from  $\mathfrak{K}$  by *adjunction* of the system  $\mathfrak{S}$ .  $\mathfrak{K}(\mathfrak{S})$  can be equal to  $\mathfrak{L}$ , and is, e.g., equal to  $\mathfrak{L}$  when  $\mathfrak{S} = \mathfrak{L}$ . But  $\mathfrak{K}(\mathfrak{S})$  can also be equal to  $\mathfrak{K}$ ; this case occurs<sup>E14</sup> when all elements of  $\mathfrak{S}$  belong to  $\mathfrak{K}$ . If from a field  $\mathfrak{K}$  a second one arises by adjunction of a system  $\mathfrak{S}_1$ , from this a third by adjunction of a system  $\mathfrak{S}_2$ , etc., then, if  $\mathfrak{S}_1, \mathfrak{S}_2, \dots, \mathfrak{S}_n$  have been adjoined one after another, we denote the field obtained last by  $\mathfrak{K}(\mathfrak{S}_1, \mathfrak{S}_2, \dots, \mathfrak{S}_n)$ . As one easily sees, the order of the systems  $\mathfrak{S}$  does not matter for the final result.<sup>E15</sup> — Let the field  $\mathfrak{K}(\mathfrak{S})$  arise from a field  $\mathfrak{K}$  by adjunction of a system  $\mathfrak{S}$  of infinitely many elements. Let us denote by  $\mathfrak{U}$  the system of those fields that arise from  $\mathfrak{K}$  by adjunction of a *finite* subsystem of  $\mathfrak{S}$  in each case. Then all fields from  $\mathfrak{U}$  are contained in  $\mathfrak{K}(\mathfrak{S})$ . If  $\mathfrak{K}_1, \mathfrak{K}_2$  are any two fields from  $\mathfrak{U}$ , then one has  $\mathfrak{K}_1 = \mathfrak{K}(\mathfrak{S}_1)$ ,  $\mathfrak{K}_2 = \mathfrak{K}(\mathfrak{S}_2)$ , where  $\mathfrak{S}_1, \mathfrak{S}_2$  are finite subsystems of  $\mathfrak{S}$ . If  $\mathfrak{S}_3$  denotes that subsystem of  $\mathfrak{S}$  that contains all elements from  $\mathfrak{S}_1$  and  $\mathfrak{S}_2$ , but no other element, then  $\mathfrak{S}_3$  is also finite; the field  $\mathfrak{K}_3 = \mathfrak{K}(\mathfrak{S}_3)$ , which contains  $\mathfrak{K}_1$

\*) A field lies “between”  $\mathfrak{K}$  and  $\mathfrak{L}$  if it contains  $\mathfrak{K}$  and is contained in  $\mathfrak{L}$ .

and  $\mathfrak{K}_2$ , therefore also belongs to  $\mathfrak{U}$ . Thus the system  $\mathfrak{U}$  satisfies the hypothesis of Theorem 2.; a definite field  $\mathfrak{L}$  therefore exists that contains all fields of the system  $\mathfrak{U}$ , consequently also  $\mathfrak{K}$  and all elements from  $\mathfrak{S}$ , thus also  $\mathfrak{K}(\mathfrak{S})$ , but that also contains only such elements as occur in fields of the system  $\mathfrak{U}$ . But since all these elements already occur in  $\mathfrak{K}(\mathfrak{S})$ , the field in question is identical with  $\mathfrak{K}(\mathfrak{S})$ . We therefore obtain the theorem:

3. *If  $\mathfrak{S}$  is an infinite system, then every element of the field  $\mathfrak{K}(\mathfrak{S})$  — likewise every system of finitely many elements from  $\mathfrak{K}(\mathfrak{S})$  — occurs in a field that arises from  $\mathfrak{K}$  by adjunction of a finite subsystem of  $\mathfrak{S}$ .*

### § 3.

#### Domains of integrity.

Here, by a *domain of integrity*<sup>E16</sup> we shall understand a system with double composition that satisfies conditions 1. to 6. of § 1, does not consist only of the single element 0, has a unity, and in which the product of two elements different from 0 is always again different from 0. By unity we here understand an element  $\varepsilon$  for which the equation  $x\varepsilon = x$  holds for all elements of the system; one sees at once that not more than one unity can exist.<sup>E17</sup>

Every field is at the same time a domain of integrity, while the system of integers proves that not every domain of integrity is a field. — The considerations made in § 2 about fields can without further ado be extended to domains of integrity. A subsystem  $\mathfrak{J}'$  of a domain of integrity  $\mathfrak{J}$  represents a domain of integrity if it contains the unity, and if sum, difference, product of two elements from  $\mathfrak{J}'$  always again belong to  $\mathfrak{J}'$ . As one sees at once, Theorems 1. and 2. of § 2 hold for domains of integrity as well; we need only replace, throughout, the word (sub)field by (sub)domain of integrity. We denote *adjunction* in the case of domains of integrity by square brackets, so that  $\mathfrak{J}[\mathfrak{S}]$  represents a domain of integrity  $\bar{\mathfrak{J}}$  that comprises the domain of integrity  $\mathfrak{J}$  and the system of elements  $\mathfrak{S}$ , and is so constituted that  $\mathfrak{S}$  is not already contained in a domain of integrity other than  $\bar{\mathfrak{J}}$  lying between  $\mathfrak{J}$  and  $\bar{\mathfrak{J}} = \mathfrak{J}[\mathfrak{S}]$ . If  $\mathfrak{J}$  is a field, then accordingly one must distinguish between  $\mathfrak{J}[\mathfrak{S}]$  and  $\mathfrak{J}(\mathfrak{S})$ . — Now, as is at once evident, Theorem 3. of § 2, too, can be extended to domains of integrity.

If  $a$  and  $b$  are elements of a domain of integrity  $\mathfrak{J}$ , then we say:  *$b$  is divisible by  $a$ ,  $a$  goes into  $b$ , is a divisor of  $b$*  etc., if there is in  $\mathfrak{J}$  an element  $x$  for which the equation  $ax = b$  is satisfied. If  $b$  and  $c$  are divisible by  $a$ , then the same holds for  $b + c$ ,  $b - c$  and for  $b \cdot d$ , if  $d$  is an arbitrary element from  $\mathfrak{J}$ . The concept of divisibility is, however, a relative one, dependent on the domain of integrity considered; if the element  $b$  is not divisible by  $a$  in  $\mathfrak{J}$ , it can nevertheless become divisible by  $a$  in an extended domain.<sup>E18</sup>

*Formation of quotients:* — Let a domain of integrity  $\mathfrak{J}$  be contained in a field  $\mathfrak{L}$ . If we let single letters denote elements from  $\mathfrak{J}$ , then, by the laws valid for every field, the following holds in  $\mathfrak{L}$ :

1) if one of the equations  $a = \frac{a'}{b'}$ ,  $\frac{a'}{b'} = a$ ,  $ab' = a'$  holds, then the other two also hold,<sup>E19</sup>

2) from  $\frac{a}{b} = \frac{a'}{b'}$  it follows that  $ab' = a'b$ , and conversely,

3)  $\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}$ ,  $\frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}$ ,

4)  $\frac{a}{b} - \frac{a'}{b'} = \frac{ab' - a'b}{bb'}$ ,  $\frac{a}{b} : \frac{a'}{b'} = \frac{ab'}{a'b}$ .

Here it is of course presupposed that the denominators are different from 0, while otherwise the letters denote arbitrary elements from  $\mathfrak{J}$ . From 3) and 4) we see that those elements of

$\mathfrak{L}$  that are represented as quotients of elements from  $\mathfrak{J}$  form a field  $\mathfrak{K}$ , and from 1) — since it gives  $\frac{a}{\varepsilon} = a$  — that  $\mathfrak{K}$  comprises the domain of integrity  $\mathfrak{J}$ . We say:  $\mathfrak{K}$  arises from  $\mathfrak{J}$  by *formation of quotients*. Such a field must therefore exist as soon as  $\mathfrak{J}$  can be contained in a field  $\mathfrak{L}$  at all. To test this possibility, we therefore need only investigate whether it is permissible to define, for the expressions of the form  $\frac{a}{b}$ , the concepts *equality, sum, product* by 1), 2), 3), and whether this yields a field containing  $\mathfrak{J}$ . That this is in fact the case for every domain of integrity  $\mathfrak{J}$  follows easily. If we test, e.g., the definition of equality, then from the assumption  $\frac{a}{b} = \frac{a'}{b'}$ ,  $\frac{a'}{b'} = \frac{a''}{b''}$  the equations  $ab' = a'b$ ,  $a'b'' = a''b'$  result by 2); from these, by the laws valid in  $\mathfrak{J}$ , multiplication gives  $ab'a''b'' = a'ba''b'$ , hence, since  $b' \neq 0$ ,  $ab''a' = a''ba'$  and, if  $a' \neq 0$ ,  $ab'' = a''b$ . But if  $a' = 0$ , then it follows from  $ab' = a'b$ ,  $a'b'' = a''b'$ ,  $b \neq 0$ ,  $b' \neq 0$ , that  $a = 0$ ,  $a'' = 0$ , and consequently again  $ab'' = a''b$ . In every case it thus follows from  $\frac{a}{b} = \frac{a'}{b'}$ ,  $\frac{a'}{b'} = \frac{a''}{b''}$  that also  $\frac{a}{b} = \frac{a''}{b''}$ ; and the corresponding result also holds by 1) if, instead of 3 quotients, we consider, say, only two and a single element from  $\mathfrak{J}$ , etc. Further, it follows from  $\frac{a}{b} = \frac{a'}{b'}$  by 2) that conversely  $\frac{a'}{b'} = \frac{a}{b}$ . Finally, by 2) always  $\frac{a}{b} = \frac{a}{b}$ . As regards the definitions of sum and product, we must prove that they are single-valued, i.e. that the result does not change if we replace a summand or factor by one equal to it. Once this is done, it is proved that a system with double composition is present, and it remains to be shown that all 7 conditions stated in § 1 are satisfied. By 1) the field then contains the domain of integrity  $\mathfrak{J}$ . — All these investigations are settled in a manner similar to the proof of the legitimacy of the definition of equality given by 1), 2), so it is unnecessary to go into the details of the argument more closely.

The field  $\mathfrak{K}$  that arises from  $\mathfrak{J}$  by formation of quotients is, of course, identical with  $\mathfrak{J}$  when  $\mathfrak{J}$  is a field. This case always occurs when  $\mathfrak{J}$  contains only finitely many elements, say  $m$  of them.<sup>E 20</sup> For if  $a (\neq 0)$  and  $b$  are then elements of  $\mathfrak{J}$ , then, as  $x$  runs through all  $m$  elements of  $\mathfrak{J}$ , so does  $ax$ , which therefore becomes equal to  $b$  at some point, i.e. condition 7 of § 1 is satisfied, and  $\mathfrak{J}$  is a field. — From isomorphic domains of integrity there arise by formation of quotients, as is at once evident, isomorphic fields.

#### § 4.

##### Prime fields. Characteristic.

To gain insight into the various possible field types,<sup>E 21</sup> we must first aim at forming the simplest fields, and then investigate how new fields can be derived by extension from fields already given. The first task leads to the concept of the *prime field*. By this we understand a field that has no subfield besides itself. The following theorem holds:

1. *In every field  $\mathfrak{K}$  one and only one prime field is contained.*

For let  $\mathfrak{U}$  denote the system of all subfields of  $\mathfrak{K}$ ,  $\mathfrak{P}$  their intersection.  $\mathfrak{P}$  is itself a field belonging to  $\mathfrak{U}$ , and if  $\mathfrak{P}'$  is a subfield of  $\mathfrak{P}$ , then  $\mathfrak{P}'$  likewise belongs to  $\mathfrak{U}$ , must therefore contain  $\mathfrak{P}$ , hence be identical with  $\mathfrak{P}$ . Thus  $\mathfrak{P}$  is a prime field. If on the other hand  $\mathfrak{T}$  is a subfield of  $\mathfrak{K}$ , then  $\mathfrak{P}$  is a subfield of  $\mathfrak{T}$ ; if therefore  $\mathfrak{T}$  is to be a prime field, then  $\mathfrak{T}$  must be identical with  $\mathfrak{P}$ .

In the same way we define as a *prime domain of integrity* one that contains no domain of integrity besides itself. The intersection of all domains of integrity contained in a domain of integrity  $\mathfrak{J}$  represents the only prime domain of integrity contained in  $\mathfrak{J}$ .

Now let  $\mathfrak{K}$  be a system that we shall at first presuppose only to be a domain of integrity, and  $\alpha$  an element of  $\mathfrak{K}$ . We put

$$\alpha = 1\alpha, \alpha + \alpha = 2\alpha, 2\alpha + \alpha = 3\alpha, \dots,$$

where  $1, 2, 3, \dots$  are to be regarded as abbreviating signs, not, however, as elements of  $\mathfrak{K}$ . The elements  $\alpha, 2\alpha, 3\alpha, \dots$  are called the *natural multiples* of  $\alpha$ . If further  $-n$  denotes a negative integer, we put

$$-(n\alpha) = (-n)\alpha.$$

This defines the element  $m\alpha$  for every integer  $m$ . The elements  $m\alpha$  are called the *integral multiples* of  $\alpha$ . For  $\alpha = \varepsilon$ , if  $m, m'$  denote integers, the equations

$$(1.) \quad m\varepsilon + m'\varepsilon = (m + m')\varepsilon, \quad m\varepsilon - m'\varepsilon = (m - m')\varepsilon, \quad (m\varepsilon) \cdot (m'\varepsilon) = (mm')\varepsilon,$$

result at once, from which it follows that the integral multiples of  $\varepsilon$  form a domain of integrity  $\mathfrak{J}$ . Since every domain of integrity contained in  $\mathfrak{K}$  contains the unity  $\varepsilon$ , and hence also the integral multiples of  $\varepsilon$ ,  $\mathfrak{J}$  represents the prime domain of integrity contained in  $\mathfrak{K}$ . If  $\mathfrak{K}$  is a field and  $\mathfrak{P}$  the prime field contained in  $\mathfrak{K}$ , then  $\mathfrak{P}$  contains all elements of  $\mathfrak{J}$ , hence also all quotients of elements of  $\mathfrak{J}$ . But since these already form a field, the prime field  $\mathfrak{P}$  is exhausted by them.

*Two cases are now conceivable:* Either the integral multiples of  $\varepsilon$  are all different from one another, i.e.  $m\varepsilon = m'\varepsilon$  only if  $m = m'$ , or that equation can also hold without the latter. In the first case there is a one-to-one correspondence between  $\mathfrak{J}$  and the system of integers, which by (1.) proves to be isomorphic. If  $\mathfrak{K}$  is a field, then it follows further from this that the prime field  $\mathfrak{P}$  contained in  $\mathfrak{K}$  is isomorphic to the field of rational numbers. In the second case there are natural multiples of  $\varepsilon$  that are equal to 0. If  $p$  is the smallest natural number for which  $p \cdot \varepsilon = 0$  holds, and if  $m, m'$  are natural numbers  $< p$ , then it follows from  $m\varepsilon \neq 0, m'\varepsilon \neq 0$  that  $(mm')\varepsilon = (m\varepsilon) \cdot (m'\varepsilon) \neq 0 = p\varepsilon$ , hence  $mm' \neq p$ .  $p$  is therefore not the product of any two smaller numbers, consequently a prime number. We call  $p$  the *characteristic* of  $\mathfrak{K}$ , while in the case discussed first we ascribe to  $\mathfrak{K}$  the *characteristic* 0.<sup>E 22</sup> *Every domain of integrity accordingly has a characteristic, which is either 0 or a prime number.* If the characteristic is a prime number  $p$ , then it follows further that  $m\varepsilon = m'\varepsilon$  holds if and only if  $m \equiv m' \pmod{p}$ . This shows, in connection with the equations (1.), that here the prime domain of integrity  $\mathfrak{J}$  is isomorphic to the system of residue classes of the prime number  $p$ , and since this system is already a field, here  $\mathfrak{J} = \mathfrak{P}$ .<sup>E 23</sup> Thus we obtain:

2. *The only prime fields that exist are the fields of the type of the field of rational numbers (which we shall henceforth denote by  $\mathfrak{P}_0$ ) and those of the type of the system of residue classes of a prime number  $p$  (henceforth denoted by  $\mathfrak{P}_p$ ).*

From the preceding it follows further:

3. *All subfields of a field  $\mathfrak{K}$  have the same characteristic as  $\mathfrak{K}$ .*<sup>E 24</sup>

If  $\alpha$  is any element of a field  $\mathfrak{K}$ ,  $m$  an integer, then  $m\alpha = (m\varepsilon) \cdot \alpha$ ; if therefore  $\alpha \neq 0$ , then  $m\alpha = 0$  only if  $m\varepsilon = 0$ . Therefore:

4. *An integral multiple  $m\alpha$  of an element  $\alpha$  different from 0 in the field  $\mathfrak{K}$  is  $= 0$  if and only if either  $m = 0$  or the characteristic of  $\mathfrak{K}$  is a prime number and  $m$  is divisible by this prime number.*

Of course these theorems also hold for domains of integrity.

## §5.

**Equivalent extensions. Simple extensions. Transcendental and algebraic elements.  
Adjunction of a transcendental element. Integral and rational functions.**

If  $\mathfrak{L}$  and  $\mathfrak{L}'$  are extension fields of a field  $\mathfrak{K}$ , then we say:  $\mathfrak{L}$  and  $\mathfrak{L}'$  represent *equivalent extensions*<sup>E 25</sup> of  $\mathfrak{K}$ , if  $\mathfrak{L}$  and  $\mathfrak{L}'$  can be mapped isomorphically onto one another in such a way that every element of  $\mathfrak{K}$  corresponds to itself. — The equivalence of two extensions  $\mathfrak{L}, \mathfrak{L}'$  therefore presupposes the isomorphism; but non-equivalent extensions of a field can very well also yield isomorphic fields.<sup>E 26</sup> — If we are faced with the problem of extending a field so that the newly arisen field satisfies certain conditions, and it turns out that all extensions that satisfy the conditions set are equivalent, then we say *that the extension problem has essentially only one solution*. In this sense, e.g., the problem of extending the field  $\mathfrak{R}$  of real numbers so that every element of the new field satisfies an algebraic equation in  $\mathfrak{R}$ , but not every one is already contained in  $\mathfrak{R}$ , is essentially solvable in only one way.

The simplest extensions of a field  $\mathfrak{K}$  that present themselves are those that arise from  $\mathfrak{K}$  by adjunction of a single element. We call them *simple extensions*, and if  $\mathfrak{L}$  is such an extension, we call every element  $\alpha$  of  $\mathfrak{L}$  for which  $\mathfrak{K}(\alpha) = \mathfrak{L}$  holds a *primitive element of  $\mathfrak{L}$  with respect to  $\mathfrak{K}$* . — Let the field  $\mathfrak{K}(x)$  arise from  $\mathfrak{K}$  by adjunction of an element  $x$ . Between  $\mathfrak{K}$  and  $\mathfrak{K}(x)$  lies the domain of integrity  $\mathfrak{K}[x]$  (§ 3). It contains all elements of the form

$$c_0 + c_1x + c_2x^2 + \cdots + c_nx^n,$$

in which the coefficients  $c$  are arbitrary elements from  $\mathfrak{K}$ . For a more convenient representation we think of these elements from  $\mathfrak{K}[x]$  as written in the form of infinite series

$$(1.) \quad \sum c_k x^k$$

where of course it is always presupposed that from a definite index  $k$  on all coefficients are equal to 0. Then the equations hold:

$$(2.) \quad \begin{cases} \sum a_k x^k + \sum b_k x^k = \sum (a_k + b_k) x^k, \\ (\sum a_k x^k) \cdot (\sum b_k x^k) = \sum c_k x^k, \quad (c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0), \end{cases}$$

and

$$(3.) \quad \sum a_k x^k - \sum b_k x^k = \sum (a_k - b_k) x^k,$$

from which it follows that the elements of the form (1.) reproduce themselves under addition, subtraction, and multiplication. Since all elements from  $\mathfrak{K}$ , thus in particular also  $\varepsilon$ , are contained among the elements of the form (1.), these elements form a domain of integrity comprising  $\mathfrak{K}$ , and since it also contains  $x$ , this domain must be identical with  $\mathfrak{K}[x]$ . The field  $\mathfrak{K}(x)$  contains the domain of integrity  $\mathfrak{K}[x]$ , hence also a definite field  $\mathfrak{L}$  that arises from  $\mathfrak{K}[x]$  by formation of quotients (§ 3). But since  $\mathfrak{L}$  comprises both  $\mathfrak{K}$  and  $x$ ,  $\mathfrak{K}(x)$  is identical with  $\mathfrak{L}$ .

As in the formation of the simplest *fields*, so also in the formation of the simplest *extensions* we have to distinguish two cases. The first corresponds to the assumption that two elements  $\sum a_k x^k, \sum b_k x^k$  from  $\mathfrak{K}[x]$  are always equal to one another only if for every  $k$   $a_k = b_k$  holds, the second to the contrary one. In the first case we call the element  $x$  *transcendental*, in the second *algebraic with respect to  $\mathfrak{K}$* , and at this point we wish to introduce some further

designations that will be important for what follows: If  $\mathfrak{L}$  is an arbitrary extension field of  $\mathfrak{K}$ , then  $n$  elements  $\alpha_1, \dots, \alpha_n$  of  $\mathfrak{L}$  are called *linearly dependent* or *linearly independent with respect to  $\mathfrak{K}$* , according as a linear homogeneous relation

$$a_1\alpha_1 + \dots + a_n\alpha_n = 0,$$

in which the coefficients  $a$  are elements from  $\mathfrak{K}$  and not all equal to 0, exists or does not exist. The elements  $\alpha_1, \dots, \alpha_n$  need not all be different from one another, but it is clear that, if equal ones occur among them, they are always linearly dependent. We remark further that the elements  $\alpha_1, \dots, \alpha_n$  are linearly dependent if already a part of them is linearly dependent, and on the basis of this we arrive at an extension of our definition to systems of infinitely many elements. We call a system  $\mathfrak{S}$  of infinitely many elements from  $\mathfrak{L}$  linearly dependent or independent with respect to  $\mathfrak{K}$ , according as a *finite* subsystem of  $\mathfrak{S}$  that is linearly dependent with respect to  $\mathfrak{K}$  exists or does not exist. The distinction made above between (relatively) transcendental and algebraic elements can now also be formulated thus: *The element  $x$  is transcendental or algebraic with respect to  $\mathfrak{K}$  according as its powers*

$$\varepsilon, x, x^2, \dots, x^n, \dots$$

*are linearly independent or dependent with respect to  $\mathfrak{K}$ .* <sup>E 27</sup>

We first consider the adjunction of a *transcendental* element, which alone is to be treated in the present section. Here we have:

1. *Every field  $\mathfrak{K}$  can be extended by adjunction of a transcendental element  $x$ .*

For if we form by means of the elements of  $\mathfrak{K}$  all expressions of the form (1.), if we determine that two such expressions  $\Sigma a_k x^k, \Sigma b_k x^k$  shall count as equal only if for every  $k$   $a_k = b_k$  holds, and if we lay down the equations (2.) as definitions for addition and multiplication, then we have created a system with double composition comprising  $\mathfrak{K}$  which, as direct computation shows at once, satisfies conditions 1.—6. of § 1. If further  $\alpha = \Sigma a_k x^k$  and  $\beta = \Sigma b_k x^k$  are two elements of this system that are different from 0,  $a_m, b_n$  the last coefficients different from 0, then in the product  $\alpha \cdot \beta = \Sigma c_k x^k$  the coefficient  $c_{m+n} = a_m \cdot b_n \neq 0$ , hence  $\alpha \cdot \beta \neq 0$ . Since the system also contains a unity, it represents a domain of integrity  $\mathfrak{J}$ , and since all elements of  $\mathfrak{J}$  are formed from  $x$  and the elements of  $\mathfrak{K}$  by addition and multiplication,  $\mathfrak{J} = \mathfrak{K}[x]$ . <sup>E 28</sup> But from  $\mathfrak{J}$ , as from every domain of integrity, we obtain a field by formation of quotients, the field  $\mathfrak{K}(x)$ .

2. *All extensions of a field that arise by adjunction of a transcendental element are equivalent.*

For if  $\mathfrak{K}(x), \mathfrak{K}(y)$  are two such extensions, and if we assign to every element of  $\mathfrak{K}(x)$ , which we think of as represented in the form of a quotient of two elements of the form (1.), that element of  $\mathfrak{K}(y)$  that we obtain by replacing  $x$  by  $y$ , then it is easy to see that we have an isomorphic correspondence between  $\mathfrak{K}(x)$  and  $\mathfrak{K}(y)$  under which every element of  $\mathfrak{K}$  corresponds to itself.

We also call the elements of the field  $\mathfrak{K}(x)$  *rational*, and those of the domain of integrity  $\mathfrak{K}[x]$  *integral functions of the transcendental or indeterminate  $x$  in the field  $\mathfrak{K}$* , and for their designation we use, in the customary manner, the function signs  $f(x), g(x)$ , etc. An integral function

$$f(x) = c_0 + c_1x + \dots + c_nx^n$$

is said to be of *degree*  $n$  if  $c_n \neq 0$ , so that the integral functions of degree 0 are represented by the elements from  $\mathfrak{K}$  that are different from 0. To the element 0 we ascribe no degree; but if it is stated of an integral function that its degree lies below a certain bound, then the case in which the function is equal to 0 shall always be included.

If  $f(x)$  and  $g(x)$  are integral functions of the indeterminate  $x$  in the field  $\mathfrak{K}$  and if  $g(x) \neq 0$ ,  $n$  the degree of  $g(x)$ , then by the known division procedure in the field  $\mathfrak{K}$  we can determine two integral functions  $q(x)$  and  $r(x)$  such that firstly

$$(4.) \quad f(x) = q(x) \cdot g(x) + r(x)$$

and secondly the degree of  $r(x) < n$ . The functions  $q(x)$  and  $r(x)$  are uniquely determined by the two requirements. The equation  $r(x) = 0$  states that  $f(x)$  is divisible by  $g(x)$ . It can also be that each of the functions  $f(x), g(x)$  is divisible by the other; then they differ only by a factor of degree 0, which is therefore an element from  $\mathfrak{K}$ . Two such functions are to be regarded as essentially equal in all questions concerning divisibility. That it is immaterial for these questions (in contrast to those of irreducibility treated later) in which field  $\mathfrak{K}$  the functions are considered rests on the unique determinacy of the functions  $q(x), r(x)$  occurring in (4.); the field must only be one to which the coefficients of the functions belong as elements, while  $x$  is transcendental with respect to it. — This holds also for the question of the *greatest common divisor*  $t(x)$  of two integral functions  $f(x), g(x)$ , into which every common divisor of  $f(x)$  and  $g(x)$  goes.  $t(x)$  is equal to 0 if  $f(x) = 0, g(x) = 0$ , otherwise different from 0 and determined only up to a factor of degree 0. In order to fix  $t(x)$  uniquely, we stipulate that the coefficient of the highest power of  $x$  shall be equal to the unity, and we denote the greatest common divisor  $t(x)$  of  $f(x)$  and  $g(x)$  so determined by

$$(f(x), g(x)).$$

*Euler's* procedure<sup>E 29 12</sup> teaches how to find  $t(x)$  and to represent it in the form

$$(5.) \quad t(x) = f(x) \cdot g_1(x) + g(x) \cdot f_1(x)$$

The integral functions  $f_1(x), g_1(x)$  occurring here are uniquely determined if it is required that their degrees shall be smaller than the degrees of  $f(x)$  and  $g(x)$  respectively; like  $t(x)$  they belong to every field to which the functions  $f(x), g(x)$  belong. The equation

$$(f(x), g(x)) = \varepsilon$$

expresses that  $f(x)$  and  $g(x)$  are *relatively prime*.

Starting from *Euler's* algorithm, we go on, in a known manner, to the theorems

3. If  $f(x)$  is relatively prime to  $g(x)$ ,  $f(x) \cdot h(x)$  divisible by  $g(x)$ , then  $h(x)$  is divisible by  $g(x)$ .<sup>E 30</sup>

4. If  $f(x)$  and  $h(x)$  are relatively prime to  $g(x)$ , then  $f(x) \cdot h(x)$  is also relatively prime to  $g(x)$ .<sup>E 31</sup>

Let the field  $\mathfrak{K}$  be extended to  $\mathfrak{K}(x)$  by adjunction of a transcendental element  $x$ . Every element  $\xi$  of  $\mathfrak{K}(x)$  can then be represented in infinitely many ways as a quotient of two elements

<sup>12</sup> In modern terms: *Euclidean algorithm*. — Trans.

$f(x), g(x)$  of  $\mathfrak{K}[x]$ . By cancelling with the greatest common divisor we can bring it about that numerator and denominator are relatively prime; then by multiplication of numerator and denominator by an element from  $\mathfrak{K}$  it can be brought about that in the denominator the coefficient of the highest power becomes equal to  $\varepsilon$ . Thus we obtain a “reduced” representation of  $\xi$ , and there is only one such. For if we assume two reduced representations of  $\xi$

$$\xi = \frac{f(x)}{g(x)} = \frac{f_1(x)}{g_1(x)},$$

then it follows that

$$f(x) \cdot g_1(x) = f_1(x) \cdot g(x),$$

and from this, because  $g(x)$  is relatively prime to  $f(x)$  but goes into the product  $f(x) \cdot g_1(x)$ , that  $g(x)$  must go into  $g_1(x)$ . Likewise  $g_1(x)$  must go into  $g(x)$ , and since both functions have  $\varepsilon$  as the coefficient of the highest power, it follows that  $g(x) = g_1(x)$ ,  $f(x) \cdot g(x) = f_1(x) \cdot g(x)$ , and hence also  $f(x) = f_1(x)$ . — Let  $\xi = \frac{f(x)}{g(x)}$  again denote the reduced representation of the element  $\xi$  from  $\mathfrak{K}(x)$ . Let us assume that  $\xi$  is algebraic with respect to  $\mathfrak{K}$ . Then a relation of the form

$$(6.) \quad c_0 + c_1\xi + \cdots + c_n\xi^n = 0,$$

holds, in which the coefficients  $c$  belong to the field  $\mathfrak{K}$  and  $c_n \neq 0$  may be assumed. But we may, provided  $\xi \neq 0$ , also assume  $c_0 \neq 0$ . For if  $c_\mu$  is the first coefficient different from 0, then it follows from (6.) that

$$c_\mu + c_{\mu+1}\xi + \cdots + c_n\xi^{n-\mu} = 0,$$

in which again the term free of  $\xi$  is different from 0. If we therefore assume right away  $c_0 \neq 0$ , then we obtain from (6.), after multiplication by  $(g(x))^n$ , an equation to which we can give the forms

$$\begin{aligned} g(x)[c_0(g(x))^{n-1} + \cdots + c_{n-1}(f(x))^{n-1}] &= -c_n(f(x))^n, \\ -c_0(g(x))^n &= f(x)[c_1(g(x))^{n-1} + \cdots + c_n(f(x))^{n-1}] \end{aligned}$$

from which it is evident that  $(f(x))^n$  is divisible by  $g(x)$ ,  $(g(x))^n$  by  $f(x)$ . But since  $f(x)$  and  $g(x)$  are relatively prime, this is possible, by 4., only if  $f(x)$  and  $g(x)$  are of degree 0, hence  $\xi$  is an element of the field  $\mathfrak{K}$ . Thus the theorem holds:

5. *In the field  $\mathfrak{K}(x)$  that arises from  $\mathfrak{K}$  by adjunction of a transcendental element  $x$ , all elements except those of  $\mathfrak{K}$  itself are transcendental with respect to  $\mathfrak{K}$ .*

This theorem, which finds its counterpart in Theorem 3 of § 6, shows that the extensions that are obtained by the adjunction of a transcendental element are thoroughly different from those that the adjunction of an algebraic element yields.

In the field  $\mathfrak{K}(x)$  that arises from  $\mathfrak{K}$  by adjunction of the transcendental element  $x$ , all elements are rational functions of  $x$  or of course also of any other primitive element, while on the other hand the distinction of the elements of  $\mathfrak{K}(x)$  as *integral* and *fractional* refers to a definite element  $x$ . A concept independent of the choice of the primitive element is (as is still to be shown) the *degree of a rational function*  $R(x)$ . If  $R(x) = \frac{f(x)}{g(x)}$  is the representation of  $R(x)$  in reduced form, and if  $m$  and  $n$  are the degrees of  $f(x)$  and  $g(x)$ , then the larger of the numbers  $m$  and  $n$ , and if both are equal, the number  $m = n$ , is called the *degree* of the rational function  $R(x)$ . We prove:

6. A rational function of degree  $n$  of a rational function of degree  $\nu$  ( $n > 0, \nu > 0$ ) is a function of degree  $n \cdot \nu$ .

Let

$$(7.) \quad R(x) = \frac{f(x)}{g(x)}, \quad P(x) = \frac{\varphi(x)}{\psi(x)}$$

be rational functions of  $x$  in the field  $\mathfrak{K}$  in reduced representation,  $n$  and  $\nu$  their degrees,

$$(8.) \quad \begin{cases} f(x) = a_0x^n + \cdots + a_n, & g(x) = b_0x^n + \cdots + b_n, \\ \varphi(x) = \alpha_0x^\nu + \cdots + \alpha_\nu, & \psi(x) = \beta_0x^\nu + \cdots + \beta_\nu. \end{cases}$$

Then neither the elements  $a_0, b_0$ , nor the elements  $\alpha_0, \beta_0$  can vanish simultaneously. Since  $f(x)$  and  $g(x)$  are relatively prime, we can determine two integral functions  $f_1(x), g_1(x)$ , whose degrees are  $< n$ , such that

$$(9.) \quad f(x) \cdot g_1(x) + g(x) \cdot f_1(x) = \varepsilon$$

holds. If we put

$$(10.) \quad \gamma = a_0\alpha_0^n + a_1\alpha_0^{n-1}\beta_0 + \cdots + a_n\beta_0^n, \quad \delta = b_0\alpha_0^n + b_1\alpha_0^{n-1}\beta_0 + \cdots + b_n\beta_0^n,$$

then in the case  $\beta_0 \neq 0$

$$\gamma = f\left(\frac{\alpha_0}{\beta_0}\right)\beta_0^n, \quad \delta = g\left(\frac{\alpha_0}{\beta_0}\right)\beta_0^n,$$

hence by (9.)

$$\gamma g_1\left(\frac{\alpha_0}{\beta_0}\right) + \delta f_1\left(\frac{\alpha_0}{\beta_0}\right) = \beta_0^n \neq 0,$$

and therefore  $\gamma$  and  $\delta$  cannot both be 0. But the same is also the case if  $\beta_0 = 0$ . For then  $\alpha_0 \neq 0$ ,  $\gamma = a_0\alpha_0^n$ ,  $\delta = b_0\alpha_0^n$ , from which, because  $a_0$  and  $b_0$  do not vanish simultaneously, the assertion follows. Now, however,  $\gamma$  and  $\delta$  represent the coefficients of the  $n \cdot \nu$ -th power of  $x$  in the integral functions

$$(11.) \quad \begin{cases} \sigma(x) = a_0\varphi^n + a_1\varphi^{n-1}\psi + \cdots + a_n\psi^n, \\ \tau(x) = b_0\varphi^n + b_1\varphi^{n-1}\psi + \cdots + b_n\psi^n \end{cases}$$

(where  $\varphi$  and  $\psi$  are written for  $\varphi(x)$  and  $\psi(x)$ ). Of the functions  $\sigma(x)$  and  $\tau(x)$ , neither of which, as is evident from (11.) and (8.), exceeds the degree  $n \cdot \nu$ , at least one must therefore attain this degree. By (8.)

$$(12.) \quad \sigma(x) = f\left(\frac{\varphi}{\psi}\right)\psi^n, \quad \tau(x) = g\left(\frac{\varphi}{\psi}\right)\psi^n,$$

hence because of (7.)

$$(13.) \quad R(P(x)) = \frac{\sigma(x)}{\tau(x)}.$$

From (12.), (9.) there follows

$$(14.) \quad \sigma(x) \cdot g_1 \left( \frac{\varphi}{\psi} \right) \psi^{n-1} + \tau(x) \cdot f_1 \left( \frac{\varphi}{\psi} \right) \psi^{n-1} = \psi^{2n-1},$$

and in this  $g_1 \left( \frac{\varphi}{\psi} \right) \psi^{n-1}$  and  $f_1 \left( \frac{\varphi}{\psi} \right) \psi^{n-1}$  are integral functions of  $x$ . If we put, applying the notation for the greatest common divisor introduced above,

$$(15.) \quad (\sigma(x), \tau(x)) = t(x),$$

$$(16.) \quad (t(x), \psi(x)) = u(x),$$

then  $u(x)$  goes into  $\sigma(x), \tau(x), \psi(x)$ , hence by (11.) also into  $\varphi^n$ . But since  $\varphi(x)$  and  $\psi(x)$  are relatively prime,  $u(x) = \varepsilon$  must hold. Consequently  $t(x)$  is relatively prime to  $\psi(x)$ , hence also to  $\psi^{2n-1}$ . But from (15.), (14.) it follows that  $t(x)$  goes into  $\psi^{2n-1}$ . Accordingly  $t(x) = \varepsilon$  must hold, i.e. the functions  $\sigma(x), \tau(x)$  are relatively prime, and since at least one of them has the degree  $n \cdot \nu$ , but none a higher degree, by (13.) the degree of the rational function  $R(P(x))$  is equal to  $n \cdot \nu$ , q.e.d.

In the preceding proof we used the theorem that equations that hold between rational functions of a transcendental  $x$  in a field  $\mathfrak{K}$  remain correct if for  $x$  we substitute any element of the field  $\mathfrak{K}$ , or also of any extension field of  $\mathfrak{K}$ , provided only that this substitution introduces no vanishing denominators. This theorem is an immediate consequence of the fact that, in defining equality, sum, and product for two rational functions of a transcendental element, we made only such stipulations as hold, on the basis of the general properties of fields, for every element  $x$ , whether it be transcendental or not.

If  $y$  is an element of the field  $\mathfrak{K}(x)$ , then  $\mathfrak{K}(y)$  is a field between  $\mathfrak{K}$  and  $\mathfrak{K}(x)$ . Every element of  $\mathfrak{K}(y)$  has, considered as a rational function of  $x$  in  $\mathfrak{K}$ , a degree which by 6. is divisible by the degree  $n$  of the element  $y$ . If  $y$  is to be a primitive element of  $\mathfrak{K}(x)$  with respect to  $\mathfrak{K}$ , thus  $\mathfrak{K}(y) = \mathfrak{K}(x)$ , then the degree of the element  $x$ , that is 1, must also be divisible by  $n$ , hence  $n = 1$ . But this condition is also sufficient. For if  $y = \frac{ax+b}{cx+d}$  is of degree 1, then, as is easy to see,  $ad - bc \neq 0$ ,<sup>E 32</sup> and  $x = \frac{dy-b}{-cy+a}$ ;  $x$  therefore belongs to the field  $\mathfrak{K}(y)$ , and  $\mathfrak{K}(y) = \mathfrak{K}(x)$ . Therefore:

7. *The primitive elements of the field  $\mathfrak{K}(x)$  are the rational functions of degree 1.*<sup>E 33</sup>

If  $z$  is any element of the field  $\mathfrak{K}(x) = \mathfrak{K}(y)$ , which arises from  $\mathfrak{K}$  by adjunction of the transcendental element  $x$  or  $y$ , then  $z$  can be represented as a rational function of  $x$  or  $y$ :

$$z = R(x) = R_1(y).$$

Since  $y$ , considered as a function of  $x$ , is of degree 1, by 6. the degree of  $R(x)$  in  $x$  is equal to the degree of  $R_1(y)$  in  $y$ . Thus there results:

8. *If the field  $\mathfrak{L}$  can be obtained from  $\mathfrak{K}$  by adjunction of a transcendental element, then every element of  $\mathfrak{L}$  has a definite degree with respect to  $\mathfrak{K}$ , which is independent of the choice of the primitive element.*

We prove further the theorem:

9. If  $n$  elements  $x_1, x_2, \dots, x_n$  are adjoined one after another to a field  $\mathfrak{K}_0$ , whereby the fields

$$\mathfrak{K}_0(x_1) = \mathfrak{K}_1, \quad \mathfrak{K}_1(x_2) = \mathfrak{K}_2, \dots, \quad \mathfrak{K}_{n-1}(x_n) = \mathfrak{K}_n$$

arise, and if every element  $x_k (k = 1, \dots, n)$  is transcendental with respect to  $\mathfrak{K}_{k-1}$ , then every element  $x_k$  is transcendental with respect to the field which arises from  $\mathfrak{K}_0$  by adjunction of the remaining  $n - 1$  elements. <sup>E 34</sup>

Proof: We show first that  $x_1$  is transcendental with respect to the field  $\mathfrak{K}_0(x_2)$ . For if this were not the case, there would be a relation

$$(17.) \quad c_0 + c_1 x_1 + c_2 x_1^2 + \dots + c_m x_1^m = 0,$$

in which the coefficients  $c$  are elements from  $\mathfrak{K}_0(x_2)$  and not all equal to 0. If we think of the coefficients  $c$  as written as quotients of elements from  $\mathfrak{K}_0[x_2]$  and multiply (17.) by the denominators, we obtain a relation of the same form (17.), in which the coefficients  $c$  are now elements from  $\mathfrak{K}_0[x_2]$  and likewise not all equal to 0. Let, e.g.,

$$c_k = c_{k0} + c_{k1}x_2 + \dots + c_{kr}x_2^r \neq 0;$$

then at least one of the coefficients  $c_{k0}, c_{k1}, \dots, c_{kr}$ , which are all elements from  $\mathfrak{K}_0$ , say  $c_{kl}$ , is different from 0. If now the left side of (17.) is ordered by powers of  $x_2$ , we obtain

$$(18.) \quad C_0 + C_1 x_2 + C_2 x_2^2 + \dots + C_s x_2^s = 0,$$

where the coefficients  $C$  are elements from  $\mathfrak{K}_0[x_1]$ , hence also from  $\mathfrak{K}_0(x_1)$ , and  $C_l \neq 0$ , because the coefficient of the power  $x_1^k$  occurring in  $C_l$  is equal to  $c_{kl} \neq 0$ . But from (18.) it would follow that  $x_2$  is algebraic with respect to  $\mathfrak{K}_0(x_1) = \mathfrak{K}_1$ . Since this is contrary to the hypothesis,  $x_1$  is transcendental with respect to  $\mathfrak{K}_0(x_2)$ . — This proves Theorem 9. in the case  $n = 2$ . If  $n > 2$ , we can proceed inductively. <sup>E 35</sup> The fields  $\mathfrak{K}_2, \mathfrak{K}_3, \dots, \mathfrak{K}_n$  arise from  $\mathfrak{K}_1$  by adjoining one after another the  $n - 1$  elements  $x_2, x_3, \dots, x_n$ . Since  $x_k (k \geq 2)$  is transcendental with respect to  $\mathfrak{K}_{k-1}$ , it is to be regarded as proved that every element  $x_k (k \geq 2)$  is transcendental with respect to the field  $\mathfrak{K}'_k$  which arises from  $\mathfrak{K}_1$  by adjunction of the remaining elements of the series  $x_2, x_3, \dots, x_n$ . This field  $\mathfrak{K}'_k$  is, however, identical with the field which is obtained from  $\mathfrak{K}_0$  by adjunction of the elements  $x_1, \dots, x_n$  with the exception of  $x_k$ . Accordingly it remains only to show that  $x_1$ , too, is transcendental with respect to  $\mathfrak{K}_0(x_2, x_3, \dots, x_n)$ . If we put  $\mathfrak{K}_0(x_2) = \mathfrak{K}'_1$ , then, as has already been shown,  $x_1$  is transcendental with respect to  $\mathfrak{K}'_1$ . But from  $\mathfrak{K}'_1$  we obtain the fields  $\mathfrak{K}_2, \mathfrak{K}_3, \dots, \mathfrak{K}_n$  by adjoining  $x_1, x_3, \dots, x_n$  one after another. Since these are again only  $n - 1$  elements, it follows that  $x_1$  is transcendental with respect to  $\mathfrak{K}'_1(x_3, x_4, \dots, x_n)$ , and since  $\mathfrak{K}'_1(x_3, x_4, \dots, x_n) = \mathfrak{K}_0(x_2, x_3, \dots, x_n)$ , the assertion is proved for this case also.

Of the field  $\mathfrak{K}_n$  we say that it arises from  $\mathfrak{K}_0$  by adjunction of  $n$  transcendentals or indeterminates  $x_1, x_2, \dots, x_n$ , and we call the elements of  $\mathfrak{K}_n$  *rational*, those of the domain of integrity  $\mathfrak{K}_0[x_1, x_2, \dots, x_n]$  *integral functions* of these indeterminates. — By repeated application of Theorem 2. it follows that in general two extensions  $\mathfrak{L}$  and  $\mathfrak{M}$  of a field  $\mathfrak{K}$ , each of which is derived from  $\mathfrak{K}$  by adjunction of  $n$  transcendentals, are equivalent: If  $\mathfrak{L} = \mathfrak{K}(x_1, \dots, x_n)$ ,  $\mathfrak{M} = \mathfrak{K}(y_1, \dots, y_n)$ , then there is a definite isomorphic correspondence between  $\mathfrak{L}$  and  $\mathfrak{M}$  which assigns to the elements  $x_1, \dots, x_n$  the elements  $y_1, \dots, y_n$  and lets every element of  $\mathfrak{K}$  correspond to itself. <sup>E 36</sup>

## §6.

**Adjunction of an algebraic element.**

If  $f(x)$  is an integral function of degree  $n$  in a field  $\mathfrak{K}$ ,  $\alpha$  an element from  $\mathfrak{K}$ , then dividing by  $x - \alpha$  gives

$$(1.) \quad f(x) = (x - \alpha)q(x) + r,$$

where  $q(x)$  is a function of degree  $n - 1$  in  $\mathfrak{K}$  and  $r$  an element from  $\mathfrak{K}$ . From (1.),  $f(\alpha) = r$ ; hence, if  $\alpha$  is a zero of  $f(x)$ , i.e.  $f(\alpha) = 0$ , we get the decomposition of  $f(x)$  into  $(x - \alpha) \cdot q(x)$ , from which it follows further that an integral function of degree  $n$  in a field cannot have more than  $n$  zeros. — From the representation of the greatest common divisor  $t(x)$  of two integral functions  $f(x), g(x)$  in § 5, (5.) it follows that every common zero of  $f(x)$  and  $g(x)$  must be a zero of  $t(x)$ , and that therefore relatively prime functions have no common zero.

*Reducible and irreducible functions.* — An integral function  $f(x)$  of degree  $n \geq 1$  whose coefficients belong to a field  $\mathfrak{K}$  is called *reducible in  $\mathfrak{K}$*  if there are two integral functions of smaller degree in  $\mathfrak{K}$  whose product equals  $f(x)$ ; otherwise  $f(x)$  is called *irreducible in  $\mathfrak{K}$* . If  $\mathfrak{K}_1$  is a subfield of  $\mathfrak{K}$  and the coefficients of  $f(x)$  already belong to the field  $\mathfrak{K}_1$ , then it is clear that the function  $f(x)$ , if irreducible in  $\mathfrak{K}$ , must also be irreducible in  $\mathfrak{K}_1$ ; but  $f(x)$  can be irreducible in  $\mathfrak{K}_1$  and reducible in  $\mathfrak{K}$ . — Since a function  $\varphi(x)$  irreducible in the field  $\mathfrak{K}$  is relatively prime to every other function from  $\mathfrak{K}$  into which it does not go, it follows by § 5, 4. that the product of two integral functions  $f(x), g(x)$  from  $\mathfrak{K}$  is divisible by  $\varphi(x)$  only if at least one of the two functions  $f(x), g(x)$  is divisible by  $\varphi(x)$ . From this it follows, in the familiar way, that every integral function  $f(x)$  from  $\mathfrak{K}$  can be decomposed into irreducible factors in only one way. Here, of course, we disregard factors of degree zero<sup>\*)</sup>. E 37

If  $\varphi(x)$  is an integral function of the indeterminate  $x$  in the field  $\mathfrak{K}$ ,  $n(\geq 1)$  its degree, and if we call two elements  $g_1(x), g_2(x)$  from  $\mathfrak{K}[x]$  *congruent with respect to the modulus  $\varphi(x)$*

$$g_1(x) \equiv g_2(x) \quad \text{mod. } \varphi(x),$$

if  $g_1(x) - g_2(x)$  is divisible by  $\varphi(x)$ , then all functions that are congruent to a given one are also congruent to one another, and every function  $f(x)$  is congruent to a *reduced* function, i.e. to a function whose degree is  $< n$ . From two congruences

$$g_1(x) \equiv g_2(x), \quad h_1(x) \equiv h_2(x) \quad \text{mod. } \varphi(x)$$

there follow the congruences

$$g_1(x) + h_1(x) \equiv g_2(x) + h_2(x), \quad g_1(x) \cdot h_1(x) \equiv g_2(x) \cdot h_2(x) \quad \text{mod. } \varphi(x).$$

If we therefore combine congruent functions into a *residue class*, then two such classes  $A, B$  uniquely determine two further ones  $C, D$  in such a way that, if  $g(x)$  is any element from  $A$  and  $h(x)$  one from  $B$ , then  $g(x) + h(x)$  always belongs to  $C$  and  $g(x) \cdot h(x)$  to  $D$ . If we therefore put

$$A + B = C, \quad A \cdot B = D,$$

then the residue classes form a system with double composition, and since the domain of integrity  $\mathfrak{K}[x]$  satisfies conditions 1. to 6. of § 1, the same is easily inferred for the system of

<sup>\*)</sup> On the extension of these theorems to functions of several variables see Weber, Math. Ann. 43, p. 521 ff., § 3.

residue classes. The *zero class*<sup>E38</sup>, which may be denoted by 0, here comprises the functions divisible by  $\varphi(x)$ . If  $\varphi(x)$  is reducible, if

$$(2.) \quad g(x) \cdot h(x) = \varphi(x)$$

represents a decomposition, and if  $A$  and  $B$  denote the residue classes to which  $g(x)$  and  $h(x)$  respectively belong, then by (2.)

$$A \neq 0, \quad B \neq 0, \quad A \cdot B = 0.$$

If, on the other hand, we assume that  $\varphi(x)$  is irreducible, then the product of two functions is divisible by  $\varphi(x)$  only if at least one factor is divisible by  $\varphi(x)$ , and therefore the product of two residue classes equals 0 only if at least one factor equals 0. From this it follows further that  $A \neq 0$ ,  $AB = AC$  always give  $B = C$ . If finally  $A$  and  $B$  are two residue classes, if  $A \neq 0$ , and if  $f(x), g(x)$  denote functions from  $A$  and  $B$  respectively, then  $f(x)$  is relatively prime to  $\varphi(x)$ ; we can therefore determine two elements  $\psi(x), \chi(x)$  in  $\mathfrak{K}[x]$  such that

$$f(x) \cdot \psi(x) + \varphi(x) \cdot \chi(x) = \varepsilon,$$

hence

$$(3.) \quad f(x) \cdot (\psi(x) \cdot g(x)) \equiv g(x) \quad \text{mod. } \varphi(x)$$

holds. If  $C$  denotes the residue class to which the function  $\psi(x) \cdot g(x)$  belongs, then by (3.)

$$A \cdot C = B,$$

and thus the system of residue classes also satisfies condition 7. of § 1. We therefore obtain the theorem:

1. *The system of residue classes belonging to the integral function  $\varphi(x)$  from  $\mathfrak{K}$  represents a field if  $\varphi(x)$  is irreducible in  $\mathfrak{K}$ .*<sup>E39</sup>

Now let  $\mathfrak{K}(j)$  be a field which arises from  $\mathfrak{K}$  by adjunction of an algebraic element  $j$ . Then the powers

$$\varepsilon, j, j^2, \dots \text{ in inf.}$$

are linearly dependent, and if  $n$  is the smallest number for which

$$\varepsilon, j, j^2, \dots, j^n$$

are linearly dependent, then there holds between these powers a linear homogeneous relation with coefficients from  $\mathfrak{K}$ , the last of which is different from 0 and hence, since one can divide by it, may be assumed equal to  $\varepsilon$ . The relation thus obtained

$$(4.) \quad a_0 + a_1 j + a_2 j^2 + \dots + a_{n-1} j^{n-1} + j^n = 0$$

is uniquely determined. For if one had a second such one, one would obtain by subtraction a linear homogeneous relation between the elements  $\varepsilon, j, \dots, j^{n-1}$ , which, however, are supposed to be linearly independent. We now consider the domain of integrity  $\mathfrak{K}[j]$  contained in  $\mathfrak{K}(j)$  (which subsequently proves to be identical with  $\mathfrak{K}(j)$ ) and compare it with a domain of

integrity  $\mathfrak{K}[x]$  which arises from  $\mathfrak{K}$  by adjunction of a transcendental element  $x$ .  $\mathfrak{K}[x]$  contains the function

$$\varphi(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$

which by (4.) has the zero  $j$ . If  $g(x)$ ,  $h(x)$  are elements from  $\mathfrak{K}[x]$  and if their degrees are  $< n$ , then, since  $\varepsilon, j, \dots, j^{n-1}$  are linearly independent,  $g(j) \neq 0$ ,  $h(j) \neq 0$ , and hence

$$\varphi(j) = 0 \neq g(j) \cdot h(j)$$

and from this

$$\varphi(x) \neq g(x) \cdot h(x),$$

i.e.  $\varphi(x)$  is not the product of two functions of smaller degree in  $\mathfrak{K}$ , hence irreducible in  $\mathfrak{K}$ . By the theorems on irreducible functions stated above,  $\varphi(x)$  is the only irreducible function from  $\mathfrak{K}$  with  $j$  as a zero, apart from a factor from  $\mathfrak{K}$ , which, however, is also eliminated here by the further requirement that the coefficient of the highest power shall be equal to  $\varepsilon$ . We also call the degree  $n$  of  $\varphi(x)$  the *degree of the element  $j$  with respect to  $\mathfrak{K}$* , in symbols:

$$n = [j : \mathfrak{K}].$$

We now assign to every element  $f(x)$  from  $\mathfrak{K}[x]$  the element  $f(j)$  from  $\mathfrak{K}[j]$ . If  $f(x)$  is of degree 0, hence an element of  $\mathfrak{K}$ , then  $f(j) = f(x)$ ; the elements of  $\mathfrak{K}[j]$  that correspond to the elements of  $\mathfrak{K}[x]$  comprise all elements of the form

$$c_0 + c_1j + \cdots + c_kj^k$$

with arbitrary coefficients  $c$  from  $\mathfrak{K}$ , and therefore exhaust the domain of integrity  $\mathfrak{K}[j]$ . But infinitely many elements of  $\mathfrak{K}[x]$  correspond to every element of  $\mathfrak{K}[j]$ . For if  $f_1(x), f_2(x)$  are any two elements from  $\mathfrak{K}[x]$ , then we can write

$$(5.) \quad f_1(x) - f_2(x) = q(x) \cdot \varphi(x) + r(x)$$

where  $q(x)$ ,  $r(x)$  are elements from  $\mathfrak{K}[x]$  and the degree of  $r(x)$  is  $< n$ . From this, however, it follows that

$$f_1(j) = f_2(j) + r(j),$$

and since  $r(j)$  can equal 0 only if  $r(x) = 0$ , that is, if by (5.)  $f_1(x) \equiv f_2(x) \pmod{\varphi(x)}$ , the elements of a definite residue class mod.  $\varphi(x)$  correspond to an element from  $\mathfrak{K}[j]$ , and we therefore have a one-to-one correspondence between these residue classes and  $\mathfrak{K}[j]$ . Since it further always follows from

$$f(x) + g(x) = h(x), \quad f(x) \cdot g(x) = k(x)$$

that

$$f(j) + g(j) = h(j), \quad f(j) \cdot g(j) = k(j)$$

the correspondence is isomorphic. Since  $\varphi(x)$  is irreducible, it follows that the system of residue classes is a field; therefore the isomorphic system  $\mathfrak{K}[j]$  must also be a field; consequently  $\mathfrak{K}[j] = \mathfrak{K}(j)$ . Since every residue class contains exactly *one* function whose degree is  $< n$ , in the form

$$(6.) \quad c_0 + c_1j + \cdots + c_{n-1}j^{n-1},$$

with arbitrary elements of  $\mathfrak{K}$  taken for the coefficients  $c$ , every element of  $\mathfrak{K}(j)$  is represented exactly once.

If  $\mathfrak{K}(\bar{j})$  is a second extension of  $\mathfrak{K}$ , and if  $\bar{j}$  is a zero of the same irreducible function  $\varphi(x)$ , then we have an isomorphic correspondence between  $\mathfrak{K}(j)$  and the system of residue classes mod.  $\varphi(x)$ , and likewise between this system and  $\mathfrak{K}(\bar{j})$ . These correspondences together yield an isomorphism between  $\mathfrak{K}(j)$  and  $\mathfrak{K}(\bar{j})$  under which, as shown above, every element of  $\mathfrak{K}$  corresponds to itself. Both extensions are therefore equivalent. — On the other hand, it is easy to see that for every irreducible function  $\varphi(x)$  from  $\mathfrak{K}$  there actually exists an extension  $\mathfrak{K}(j)$  in which  $j$  is a zero of  $\varphi(x)$ . For if  $\mathfrak{L}$  denotes the residue class field belonging to  $\varphi(x)$ , then there exists an isomorphic correspondence  $\pi_0$  between  $\mathfrak{K}$  and a subfield  $\bar{\mathfrak{K}}$  of  $\mathfrak{L}$ , by which to every element  $a$  of  $\mathfrak{K}$  the residue class represented by  $a$  is assigned. We now introduce a system  $\mathfrak{S}$  of new elements, which we assign uniquely to the elements of  $\mathfrak{L}$  not belonging to  $\bar{\mathfrak{K}}$ .<sup>E 40</sup> This assignment and  $\pi_0$  yield a map  $\pi_1$  between  $\mathfrak{L}$  and the system  $\mathfrak{L} = \mathfrak{K} + \mathfrak{S}$ . If  $A, B, C, D$  are elements from  $\mathfrak{L}$ ,  $a, b, c, d$  the corresponding ones from  $\mathfrak{K}$ , and if  $A + B = C$ ,  $A \cdot B = D$ , then, when  $a$  and  $b$  belong to  $\mathfrak{K}$ ,  $a + b = c$ ,  $a \cdot b = d$ . If we decree that these equations shall hold in the other case as well, then  $\mathfrak{L}$  becomes a field isomorphic to  $\mathfrak{L}$  that represents an extension of  $\mathfrak{K}$ . If  $j$  is that element of  $\mathfrak{L}$  that in the isomorphism  $\pi_1$  corresponds to the residue class represented by  $x$ , then it follows at once from the definition of the addition and multiplication of residue classes: *An element  $g(x)$  from  $\mathfrak{K}[x]$  represents a residue class to which the element  $g(j)$  from  $\mathfrak{L}$  is assigned by  $\pi_1$ .* From this, however, it follows that  $\varphi(j) = 0$  and that the field  $\mathfrak{L}$  is exhausted by the elements of the form  $g(j)$ , consequently  $\mathfrak{L} = \mathfrak{K}(j)$ . Therefore:

2. *By every irreducible function  $\varphi(x)$  from  $\mathfrak{K}$  one and — apart from equivalent extensions — only one extension  $\mathfrak{K}(j)$  is determined in which  $j$  is a zero of  $\varphi(x)$ .*<sup>E 41</sup>

If  $\varphi(x)$  is of degree  $n$  and if  $\gamma_0, \gamma_1, \dots, \gamma_n$  are any  $n + 1$  elements from  $\mathfrak{K}(j)$ , then we can represent these in the form

$$\gamma_i = c_{i0} + c_{i1}j + \dots + c_{i,n-1}j^{n-1} \quad (i = 0, \dots, n)$$

with coefficients from  $\mathfrak{K}$ . From the theorem on linear equations mentioned in § 1 it follows that we can determine in  $\mathfrak{K}$   $n + 1$  elements  $b_0, \dots, b_n$ , which are not all 0, such that  $\sum_{i=0}^n b_i \gamma_i = 0$  holds.  $n + 1$  elements are therefore always linearly dependent. Since this holds also for the powers  $\varepsilon, \gamma, \gamma^2, \dots, \gamma^n$  of an arbitrary element of  $\mathfrak{K}(j)$ , we have the theorem:

3. *If the field  $\mathfrak{L}$  arises from  $\mathfrak{K}$  by adjunction of an algebraic element  $j$ , then all elements of  $\mathfrak{L}$  are algebraic. If  $n$  is the degree of  $j$ , then every system of more than  $n$  elements is linearly dependent.*<sup>E 42</sup>

## § 7.

### Foundations of algebraic extensions.

*Algebraic extensions; algebraically closed fields.* — After the simplest extensions, the primitive ones, have been investigated in §§ 5 and 6 and have led to a distinction of (relatively) algebraic and transcendental elements, the *algebraic* extensions shall now first be considered more closely. A field  $\mathfrak{L}$  is called *algebraic with respect to a subfield  $\mathfrak{K}$*  or an *algebraic extension of  $\mathfrak{K}$*  if every element of  $\mathfrak{L}$  is algebraic with respect to  $\mathfrak{K}$ . Every field  $\mathfrak{L}$  contains elements that

are algebraic with respect to a given subfield  $\mathfrak{K}$ . For it is clear that every element of  $\mathfrak{K}$  itself is algebraic with respect to  $\mathfrak{K}$ , namely of degree 1. Likewise one sees at once that an element of  $\mathfrak{L}$  not belonging to  $\mathfrak{K}$ , if it is algebraic with respect to  $\mathfrak{K}$ , has degree  $> 1$ , and hence is a zero of a function irreducible in  $\mathfrak{K}$  of degree higher than the first. If, therefore, an algebraic extension  $\mathfrak{L}$  of  $\mathfrak{K}$  is to exist, and specifically an actual one, i.e. one different from  $\mathfrak{K}$ , then it is necessary for this, though by § 6, 2. also sufficient, that there exist irreducible functions in  $\mathfrak{K}$  whose degree is  $> 1$ . If there are none, so that every integral function of higher degree breaks up into linear factors, then the field  $\mathfrak{K}$  is not capable of any further algebraic extension and shall therefore be called *algebraically closed*. The existence of such fields was first proved by the fundamental theorem of algebra<sup>E43</sup>, which states that the field of complex numbers is algebraically closed.

*Absolutely algebraic elements and fields.* — If an element  $\alpha$  of a field  $\mathfrak{K}$  is algebraic with respect to a subfield  $\mathfrak{K}_1$ , then it is of course also algebraic with respect to every field between  $\mathfrak{K}_1$  and  $\mathfrak{K}$ . If therefore  $\alpha$  is algebraic with respect to the prime field contained in  $\mathfrak{K}$ , then  $\alpha$  is algebraic with respect to every subfield. Such an element  $\alpha$  shall therefore be called *absolutely algebraic*. Likewise we call a field *absolutely algebraic* if it is already algebraic with respect to its prime field or, what amounts to the same, if all its elements are absolutely algebraic.

*Finite extensions.* — If  $\mathfrak{K}$  is a subfield of  $\mathfrak{L}$ , then we say:  $\mathfrak{L}$  is *finite with respect to  $\mathfrak{K}$  and of degree  $n$*  — in symbols

$$[\mathfrak{L} : \mathfrak{K}] = n$$

—, if one can specify in  $\mathfrak{L}$   $n$  elements linearly independent with respect to  $\mathfrak{K}$ , while every system of more than  $n$  elements from  $\mathfrak{L}$  is linearly dependent with respect to  $\mathfrak{K}$ .

1. *Every finite extension of a field is algebraic.*

For if  $[\mathfrak{L} : \mathfrak{K}] = n$  and  $\alpha$  is an element of  $\mathfrak{L}$ , then the elements  $\varepsilon, \alpha, \alpha^2, \dots, \alpha^n$  are linearly dependent with respect to  $\mathfrak{K}$ , i.e.  $\alpha$  is algebraic with respect to  $\mathfrak{K}$ . But there are also *infinite* (non-finite) algebraic extensions, e.g. the extension of the field of rational numbers to the field of all algebraic numbers. — One sees at once that every field  $\mathfrak{K}$  is finite with respect to itself, namely of degree 1, while every actual finite extension has a degree  $> 1$ .

*Basis of a finite extension.* — If the field  $\mathfrak{L}$  is finite with respect to its subfield  $\mathfrak{K}$ ,  $[\mathfrak{L} : \mathfrak{K}] = n$ , if the elements  $\alpha_1, \dots, \alpha_n$  from  $\mathfrak{L}$  are linearly independent with respect to  $\mathfrak{K}$ , and if  $\beta$  is any element from  $\mathfrak{L}$ , then there holds between  $\alpha_1, \dots, \alpha_n$  and  $\beta$  a linear homogeneous relation with coefficients from  $\mathfrak{K}$ ; since the coefficient of  $\beta$  is different from 0<sup>E44</sup>, this relation can be given the form

$$(1.) \quad \beta = c_1\alpha_1 + \dots + c_n\alpha_n$$

This representation is possible in only one way, because from two equations for  $\beta$  of this form a linear homogeneous relation between  $\alpha_1, \dots, \alpha_n$  would follow by subtraction. — Let us now on the other hand assume that  $\alpha_1, \dots, \alpha_n$  are elements of any extension field  $\mathfrak{L}$  of  $\mathfrak{K}$ . If we then know that every element  $\beta$  of  $\mathfrak{L}$  can be represented in *at most* one way in the form (1.), then this holds also for  $\beta = 0$ , and the expression  $c_1\alpha_1 + \dots + c_n\alpha_n$  is therefore equal to 0 only if all coefficients are 0. Therefore the extension  $\mathfrak{L}$ , if finite at all, is *at least* of degree  $n$ . If, on the other hand, we know that every element  $\beta$  of  $\mathfrak{L}$  can be represented in *at least* one way in the form (1.), then we obtain for any  $n + 1$  elements  $\beta_0, \beta_1, \dots, \beta_n$  representations of the form

$$\beta_i = c_{i1}\alpha_1 + \dots + c_{in}\alpha_n \quad (i = 0, \dots, n)$$

and can therefore, by the theorem on linear homogeneous equations cited in § 1, determine  $n + 1$  elements  $d_0, \dots, d_n$ , not all 0, in  $\mathfrak{K}$  such that  $d_0\beta_0 + \dots + d_n\beta_n = 0$  holds. The extension  $\mathfrak{L}$  is therefore finite and *at most* of degree  $n$ . — If, accordingly, the representation (1.) is to be possible for all elements of  $\mathfrak{L}$  and for each in only one way, then  $[\mathfrak{L} : \mathfrak{K}] = n$  must hold and the system  $\alpha_1, \dots, \alpha_n$  must be linearly independent. For this reason a system of  $n$  linearly independent elements of an extension field of degree  $n$  is also called a *basis* of this field (with respect to the ground field). — If the elements  $\alpha_1, \dots, \alpha_n$  form a basis for the extension field  $\mathfrak{L}$  and if  $\beta_1, \dots, \beta_n$  are any elements from  $\mathfrak{L}$  whose representation in the form (1.) may be

$$\beta_i = c_{i1}\alpha_1 + \dots + c_{in}\alpha_n \quad (i = 1, \dots, n)$$

then it is shown in the familiar way that the elements  $\beta_1, \dots, \beta_n$  form a basis for  $\mathfrak{L}$  if and only if the determinant  $|c_{ik}|$  is different from zero <sup>E 45</sup>.

In connection with this we derive some simple theorems on finite extensions:

2. *If  $\mathfrak{L}$  is an extension of  $\mathfrak{K}$ ,  $\mathfrak{M}$  one of  $\mathfrak{L}$ , then  $\mathfrak{M}$  is finite with respect to  $\mathfrak{K}$  if and only if  $\mathfrak{L}$  is finite with respect to  $\mathfrak{K}$ ,  $\mathfrak{M}$  with respect to  $\mathfrak{L}$ ; and in this case*

$$[\mathfrak{M} : \mathfrak{K}] = [\mathfrak{L} : \mathfrak{K}] \cdot [\mathfrak{M} : \mathfrak{L}]. \quad \text{E 46}$$

For if  $[\mathfrak{M} : \mathfrak{K}] = \nu$ , then there holds between  $\nu + 1$  elements from  $\mathfrak{M}$  a linear homogeneous relation with coefficients that belong to  $\mathfrak{K}$ , hence also to  $\mathfrak{L}$ . Therefore  $\mathfrak{M}$  is finite with respect to  $\mathfrak{L}$ . Likewise there holds between  $\nu + 1$  elements from  $\mathfrak{L}$ , since these belong to  $\mathfrak{M}$ , a linear homogeneous relation with coefficients from  $\mathfrak{K}$ , i.e.  $\mathfrak{L}$  is finite with respect to  $\mathfrak{K}$ . Let us, on the other hand, presuppose that

$$[\mathfrak{L} : \mathfrak{K}] = m, \quad [\mathfrak{M} : \mathfrak{L}] = n$$

holds, and let us choose a basis  $\alpha_1, \dots, \alpha_m$  of  $\mathfrak{L}$  with respect to  $\mathfrak{K}$  and a basis  $\beta_1, \dots, \beta_n$  of  $\mathfrak{M}$  with respect to  $\mathfrak{L}$ . Then the  $m \cdot n$  elements  $\alpha_i \cdot \beta_k$  ( $i = 1, \dots, m; k = 1, \dots, n$ ) are linearly independent with respect to  $\mathfrak{K}$ . For if, in a relation  $\sum_{i,k} c_{ik}\alpha_i\beta_k = 0$  in which the coefficients  $c_{ik}$  belong to the field  $\mathfrak{K}$ , we put

$$(2.) \quad \sum_{i=1}^m c_{ik}\alpha_i = \gamma_k \quad (k = 1, \dots, n)$$

then it follows that  $\sum_{k=1}^n \gamma_k\beta_k = 0$ . Since the coefficients  $\gamma_k$  belong to  $\mathfrak{L}$  and the elements  $\beta_k$  form a basis of  $\mathfrak{M}$ ,  $\gamma_1 = 0, \dots, \gamma_n = 0$  must hold. But then it follows from (2.) that all  $m \cdot n$  coefficients  $c_{ik}$  must be equal to 0, whereby the linear independence of the elements  $\alpha_i\beta_k$  is proved. If further  $\tau$  is any element from  $\mathfrak{M}$ , then we obtain

$$\tau = \sigma_1\beta_1 + \dots + \sigma_n\beta_n,$$

where the coefficients  $\sigma_k$  belong to  $\mathfrak{L}$ ,

$$\sigma_k = a_{1k}\alpha_1 + \dots + a_{mk}\alpha_m,$$

where the coefficients  $a_{ik}$  are elements from  $\mathfrak{K}$ , and from this

$$\tau = \sum_{i,k} a_{ik}\alpha_i\beta_k,$$

i.e. every element of  $\mathfrak{M}$  is expressible linearly and homogeneously, with coefficients from  $\mathfrak{K}$ , by the  $m \cdot n$  elements  $\alpha_i \beta_k$  linearly independent with respect to  $\mathfrak{K}$ ; therefore

$$[\mathfrak{M} : \mathfrak{K}] = m \cdot n.$$

3. If  $\mathfrak{L}$  and  $\mathfrak{M}$  are finite extensions of equal degree of  $\mathfrak{K}$  and if  $\mathfrak{L}$  is contained in  $\mathfrak{M}$ , then  $\mathfrak{L}$  is identical with  $\mathfrak{M}$ .

For by 2.  $[\mathfrak{M} : \mathfrak{L}] = 1$ , hence  $\mathfrak{L} = \mathfrak{M}$ .

4. If  $\mathfrak{K}(j)$  is a simple algebraic extension of  $\mathfrak{K}$ , then

$$[\mathfrak{K}(j) : \mathfrak{K}] = [j : \mathfrak{K}].^{E47}$$

For if  $[j : \mathfrak{K}] = n$ , then, as was shown in the preceding section, every element of  $\mathfrak{K}(j)$  is representable in one and only one way in the form

$$c_0 + c_1 j + \cdots + c_{n-1} j^{n-1}$$

with coefficients from  $\mathfrak{K}$ ; the elements  $\varepsilon, j, \dots, j^{n-1}$  therefore form a basis of  $\mathfrak{K}(j)$  with respect to  $\mathfrak{K}$ .

5. If the field  $\mathfrak{L}$  is finite with respect to its subfield  $\mathfrak{K}$  and of degree  $n$ , then the degree of every element of  $\mathfrak{L}$  (with respect to  $\mathfrak{K}$ ) is a divisor of  $n$ ; the extension  $\mathfrak{L}$  is simple if and only if elements of degree  $n$  occur; and these elements are then primitive, all others imprimitive.<sup>E48</sup>

For if  $j$  is any element of  $\mathfrak{L}$ , then by 2. and 4.

$$n = [\mathfrak{L} : \mathfrak{K}] = [\mathfrak{L} : \mathfrak{K}(j)] \cdot [j : \mathfrak{K}],$$

hence  $[j : \mathfrak{K}]$  is a divisor of  $n$ . If further  $j$  is to be a primitive element of  $\mathfrak{L}$ , i.e.  $\mathfrak{L} = \mathfrak{K}(j)$ , then it is necessary and sufficient that  $[\mathfrak{L} : \mathfrak{K}(j)] = 1$ , i.e. that  $[j : \mathfrak{K}] = n$ .

6. An extension is finite if and only if it can be obtained by adjunction of a finite number of (relatively) algebraic elements.<sup>E49</sup>

For if  $\mathfrak{L} = \mathfrak{K}_0(j_1, j_2, \dots, j_\nu)$ , where the elements  $j_1, j_2, \dots, j_\nu$  are algebraic with respect to  $\mathfrak{K}_0$ , and if we put

$$\mathfrak{K}_0(j_1) = \mathfrak{K}_1, \quad \mathfrak{K}_1(j_2) = \mathfrak{K}_2, \dots, \mathfrak{K}_{\nu-1}(j_\nu) = \mathfrak{K}_\nu = \mathfrak{L},$$

then every element  $j_k$  is algebraic with respect to the field  $\mathfrak{K}_{k-1}$  lying between  $\mathfrak{K}_0$  and  $\mathfrak{L}$ , hence  $\mathfrak{K}_k$  is a simple algebraic and thus finite extension of  $\mathfrak{K}_{k-1}$ . Consequently, by 2.,  $\mathfrak{K}_\nu = \mathfrak{L}$  is also a finite extension of  $\mathfrak{K}_0$ . — If conversely  $\mathfrak{L}$  is presupposed to be a finite extension of  $\mathfrak{K}_0$ :  $[\mathfrak{L} : \mathfrak{K}_0] = n$ , and if  $j_1$  denotes an element of  $\mathfrak{L}$  not belonging to  $\mathfrak{K}_0$ , further, in case  $\mathfrak{K}_1 = \mathfrak{K}_0(j_1)$  is not yet equal to  $\mathfrak{L}$ ,  $j_2$  an element of  $\mathfrak{L}$  not belonging to  $\mathfrak{K}_1$ , in case  $\mathfrak{K}_2 = \mathfrak{K}_1(j_2)$  is not yet equal to  $\mathfrak{L}$ ,  $j_3$  an element of  $\mathfrak{L}$  not belonging to  $\mathfrak{K}_2$ , etc., then the degrees  $[\mathfrak{K}_1 : \mathfrak{K}_0], [\mathfrak{K}_2 : \mathfrak{K}_0], \dots$  form a constantly increasing sequence not exceeding  $n$ , which can be continued as long as the number  $n$  has not yet been reached. Therefore after a finite number  $\nu$  of steps the number  $n$  is reached, and then  $\mathfrak{K}_0(j_1, j_2, \dots, j_\nu) = \mathfrak{K}_\nu = \mathfrak{L}$ .

These theorems are followed by some further ones that refer to *arbitrary* algebraic extensions:

7. *If the field  $\mathfrak{L} = \mathfrak{K}(\mathfrak{S})$  is obtained from its subfield  $\mathfrak{K}$  by adjunction of a system  $\mathfrak{S}$  all of whose elements are algebraic with respect to  $\mathfrak{K}$ , then  $\mathfrak{L}$  is algebraic with respect to  $\mathfrak{K}$ .*

For if  $\mathfrak{S}$  is a finite system, then by 6.  $\mathfrak{L}$  is finite with respect to  $\mathfrak{K}$ , hence algebraic. But if  $\mathfrak{S}$  is infinite, then nevertheless (§ 2, 3.) every element  $\alpha$  of  $\mathfrak{L}$  is contained in a field that arises from  $\mathfrak{K}$  by adjunction of a finite subsystem of  $\mathfrak{S}$ , and is hence, as in the preceding case, algebraic with respect to  $\mathfrak{K}$ .

8. *Those elements of a field  $\mathfrak{L}$  that are algebraic with respect to a subfield  $\mathfrak{K}$  form a field between  $\mathfrak{K}$  and  $\mathfrak{L}$ ; in particular, therefore, the absolutely algebraic elements of  $\mathfrak{L}$  form a field.*

For if  $\mathfrak{S}$  is the system of all elements of  $\mathfrak{L}$  algebraic with respect to  $\mathfrak{K}$ , then the field  $\mathfrak{K}(\mathfrak{S})$  lying between  $\mathfrak{K}$  and  $\mathfrak{L}$  contains only elements that are algebraic with respect to  $\mathfrak{K}$  (Theorem 7.), from which it follows that  $\mathfrak{S} = \mathfrak{K}(\mathfrak{S})$ .

9. *If the field  $\mathfrak{L}$  lies between the fields  $\mathfrak{K}$  and  $\mathfrak{M}$  and if  $\mathfrak{L}$  is algebraic with respect to  $\mathfrak{K}$ ,  $\mathfrak{M}$  with respect to  $\mathfrak{L}$ , then  $\mathfrak{M}$  is algebraic with respect to  $\mathfrak{K}$ .*

For let  $\beta$  be an arbitrary element of  $\mathfrak{M}$ . If then  $[\beta : \mathfrak{L}] = n$ , we have an equation

$$(3.) \quad \alpha_0 + \alpha_1\beta + \cdots + \alpha_{n-1}\beta^{n-1} + \beta^n = 0,$$

where  $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$  are elements of  $\mathfrak{L}$ . These elements are algebraic with respect to  $\mathfrak{K}$ , hence the field  $\mathfrak{K}' = \mathfrak{K}(\alpha_0, \alpha_1, \dots, \alpha_{n-1})$  is by 6. finite with respect to  $\mathfrak{K}$ . Further, by equation (3.), the element  $\beta$  is algebraic with respect to  $\mathfrak{K}'$ , hence  $\mathfrak{K}'(\beta)$  is finite with respect to  $\mathfrak{K}'$ . Consequently, by 2.,  $\mathfrak{K}'(\beta)$  is finite with respect to  $\mathfrak{K}$ , hence  $\beta$  is algebraic with respect to  $\mathfrak{K}$ ,<sup>E50</sup> which proves Theorem 9.

## § 8.

### Decomposition of an arbitrary integral function into linear factors. Normal fields and normal functions.

In § 6 it was shown that every integral function irreducible in a field has a zero in a suitable extension field. In connection with this, we can now take up the further-reaching problem: *to extend a field in such a way that an arbitrarily given function from the original field breaks up completely in the extension field, i.e. into linear factors.*<sup>E51</sup>

So let  $f(x)$  now be an arbitrary integral function in a field  $\mathfrak{K}_0$ ,  $n$  the degree of  $f(x)$ ,  $m_0$  the number of factors of  $f(x)$  irreducible in  $\mathfrak{K}_0$ . Then  $m_0 \leq n$ , with equality to  $n$  only if  $f(x)$  breaks up completely in  $\mathfrak{K}_0$ . Let us assume that  $m_0 < n$ . Then  $f(x)$  has an irreducible factor  $g_1(x)$  whose degree is  $> 1$ . We extend  $\mathfrak{K}_0$  by adjunction of an element  $j_1$  for which  $g_1(j_1) = 0$  holds (§ 6). Since in the field  $\mathfrak{K}_1 = \mathfrak{K}_0(j_1)$  the function  $g_1(x)$  is no longer irreducible, the number  $m_1$  of the factors irreducible in  $\mathfrak{K}_1$  of  $f(x) > m_0$ ; we therefore have  $m_0 < m_1 \leq n$ . If  $m_1 < n$ , then let  $g_2(x)$  be an irreducible, non-linear factor of  $f(x)$  within  $\mathfrak{K}_1$ . We adjoin a zero  $j_2$  of  $g_2(x)$ , put  $\mathfrak{K}_1(j_2) = \mathfrak{K}_2$ , and denote by  $m_2$  the number of the irreducible factors of  $f(x)$  in  $\mathfrak{K}_2$ , so that  $m_0 < m_1 < m_2 \leq n$  holds. In this manner we continue until we arrive at a field  $\mathfrak{K}_\nu$  for which  $m_\nu = n$  holds, in which therefore  $f(x)$  breaks up into linear factors. The

field  $\mathfrak{K}_\nu$  then represents a finite extension of  $\mathfrak{K}_0$ . — Let  $j_1, \dots, j_\nu$  be the successively adjoined elements,  $\mathfrak{K}_r = \mathfrak{K}_{r-1}(j_r)$  ( $r = 1, \dots, \nu$ ) the successively arising fields, and let  $g_r(x)$  be the factor irreducible in  $\mathfrak{K}_{r-1}$  of  $f(x)$  with the zero  $j_r$ . We can say that the extension  $\mathfrak{K}_\nu$  is just sufficient for the complete breaking up of  $f(x)$ .<sup>13</sup> By this we mean that no field between  $\mathfrak{K}_0$  and  $\mathfrak{K}_\nu$  other than  $\mathfrak{K}_\nu$  itself already suffices for this; and this follows from the fact that the adjoined elements  $j_1, \dots, j_\nu$  are all zeros of  $f(x)$ , and hence must occur in every subfield of  $\mathfrak{K}_\nu$  that accomplishes the decomposition.

Now let  $\bar{\mathfrak{K}}_0$  be a field isomorphic to  $\mathfrak{K}_0$ , and let  $\pi_0$  denote an isomorphic correspondence between  $\mathfrak{K}_0$  and  $\bar{\mathfrak{K}}_0$ . By  $\pi_0$  there is then also assigned to every integral function  $g(x)$  from  $\mathfrak{K}_0$  a definite function  $\bar{g}(x)$  from  $\bar{\mathfrak{K}}_0$ , obtained by replacing the coefficients of  $g(x)$  with the elements of  $\bar{\mathfrak{K}}_0$  corresponding to them. The correspondence thus obtained between  $\mathfrak{K}_0[x]$  and  $\bar{\mathfrak{K}}_0[x]$  is then evidently also isomorphic. If therefore  $\bar{f}(x)$  and  $\bar{g}_1(x)$  are the functions from  $\bar{\mathfrak{K}}_0$  assigned to the functions  $f(x)$  and  $g_1(x)$  occurring above, then  $\bar{f}(x)$  breaks up in  $\bar{\mathfrak{K}}_0$  into  $m_0$  irreducible factors, and  $\bar{g}_1(x)$  is one of them. Now let  $\mathfrak{L}$  be any extension field of  $\bar{\mathfrak{K}}_0$ <sup>E 52</sup> within which  $\bar{f}(x)$  breaks up completely. Then the extension  $\mathfrak{L}$  is either just sufficient for the complete breaking up of  $\bar{f}(x)$  or not; in every case a definite field  $\mathfrak{M}$  between  $\bar{\mathfrak{K}}_0$  and  $\mathfrak{L}$  has this property, namely the one obtained by adjoining the zeros of  $\bar{f}(x)$  within  $\mathfrak{L}$  to  $\bar{\mathfrak{K}}_0$ . Since  $\bar{f}(x)$  breaks up completely in  $\mathfrak{M}$ , the factor  $\bar{g}_1(x)$  of  $\bar{f}(x)$  has zeros in  $\mathfrak{M}$ . Let  $\bar{j}_1$  be one such, and let  $r$  denote the degree of  $g_1(x)$  and  $\bar{g}_1(x)$ . By the isomorphic correspondence that exists between  $\mathfrak{K}_0[x]$  and  $\bar{\mathfrak{K}}_0[x]$ , the functions  $g_1(x)$  and  $\bar{g}_1(x)$  are assigned to each other, and therefore the residue class fields belonging to these functions as moduli are related to each other isomorphically. These residue class fields, however, stand in isomorphic correspondence to the fields  $\mathfrak{K}_0(j_1) = \mathfrak{K}_1$  and  $\bar{\mathfrak{K}}_0(\bar{j}_1) = \bar{\mathfrak{K}}_1$ , and there thus results an isomorphic correspondence  $\pi_1$  between  $\mathfrak{K}_1$  and  $\bar{\mathfrak{K}}_1$ , by which to every element of  $\mathfrak{K}_1$ , which we think of as written in the form

$$a_0 + a_1 j_1 + \dots + a_{r-1} j_1^{r-1}$$

with coefficients  $a$  from  $\mathfrak{K}_0$ , that element

$$\bar{a}_0 + \bar{a}_1 \bar{j}_1 + \dots + \bar{a}_{r-1} \bar{j}_1^{r-1}$$

of  $\bar{\mathfrak{K}}_1$  is assigned, which is obtained by replacing  $a_k$  ( $k = 0, \dots, r-1$ ) with the element  $\bar{a}_k$  from  $\bar{\mathfrak{K}}_0$  corresponding under the correspondence  $\pi_0$ . The correspondence  $\pi_0$  is contained in the correspondence  $\pi_1$ , in that  $\pi_1$  assigns the elements of the fields  $\mathfrak{K}_0$  and  $\bar{\mathfrak{K}}_0$  to each other in the same way as  $\pi_0$ . In view of all this, we can say: between  $\mathfrak{K}_1$  and  $\bar{\mathfrak{K}}_1$  there exists an isomorphism  $\pi_1$  by which the function  $\bar{f}(x)$  from  $\bar{\mathfrak{K}}_1$  is assigned to the function  $f(x)$  from  $\mathfrak{K}_1$ ;<sup>E 53</sup> the field  $\mathfrak{M}$  represents an extension of  $\bar{\mathfrak{K}}_1$  that is just sufficient for the complete breaking up of  $\bar{f}(x)$ . We can therefore apply to  $\mathfrak{K}_1, \bar{\mathfrak{K}}_1, \pi_1, f(x), \bar{f}(x)$  the same mode of inference as just now to  $\mathfrak{K}_0, \bar{\mathfrak{K}}_0, \pi_0, f(x), \bar{f}(x)$ . If we continue in this manner, we arrive at a series of fields

$$\bar{\mathfrak{K}}_0, \bar{\mathfrak{K}}_1, \dots, \bar{\mathfrak{K}}_\nu$$

with the following properties: each preceding field is contained in the following one, and all are contained in  $\mathfrak{M}$ . Between  $\mathfrak{K}_r$  and  $\bar{\mathfrak{K}}_r$  ( $r = 0, \dots, \nu$ ) there exists an isomorphic correspondence  $\pi_r$  that comprises the correspondence  $\pi_0$ , and hence assigns the functions  $f(x)$  and  $\bar{f}(x)$  to each other. Since now  $f(x)$  breaks up into linear factors in  $\mathfrak{K}_\nu$ , the same holds for  $\bar{f}(x)$  in

<sup>13</sup> In modern terms: *splitting field*. — Trans.

$\bar{\mathfrak{K}}_\nu$ ; and since  $\bar{\mathfrak{K}}_\nu$  lies between  $\bar{\mathfrak{K}}_0$  and  $\mathfrak{M}$ , and  $\mathfrak{M}$  was supposed to be an extension of  $\bar{\mathfrak{K}}_0$  just sufficient for the complete breaking up of  $\bar{f}(x)$ , then  $\bar{\mathfrak{K}}_\nu = \mathfrak{M}$ , and we have the theorem:

1. If  $\mathfrak{K}_0$  and  $\bar{\mathfrak{K}}_0$  are isomorphic fields, if  $\pi_0$  denotes an isomorphic correspondence between them that assigns to the integral function  $f(x)$  from  $\mathfrak{K}_0$  the integral function  $\bar{f}(x)$  from  $\bar{\mathfrak{K}}_0$ , and if  $\mathfrak{N}$  and  $\bar{\mathfrak{N}}$  are extensions of  $\mathfrak{K}_0$  and  $\bar{\mathfrak{K}}_0$  respectively that are just sufficient for the complete breaking up of  $f(x)$  and  $\bar{f}(x)$  respectively, then there is an isomorphic correspondence  $\pi'$  between  $\mathfrak{N}$  and  $\bar{\mathfrak{N}}$  that also comprises the correspondence  $\pi_0$ .<sup>E 54</sup>

The hypotheses of Theorem 1. are satisfied if we take  $\bar{\mathfrak{K}}_0 = \mathfrak{K}_0$  and understand by  $\pi_0$  the correspondence that lets every element of  $\mathfrak{K}_0$  correspond to itself. Then  $\bar{f}(x) = f(x)$ , and the correspondence  $\pi'$  likewise leaves every element of  $\mathfrak{K}_0$  unchanged; i.e.  $\mathfrak{N}$  and  $\bar{\mathfrak{N}}$  are equivalent extensions. Thus we have the following result:

2. To every integral function  $f(x)$  of a field  $\mathfrak{K}_0$  there belongs one and essentially only one extension of this field that is just sufficient for the complete breaking up of  $f(x)$ .<sup>E 55</sup>

This is why all the theorems about roots of equations that concern us are independent of how we extend the ground field to solve the equations. To work this out in a little more detail, let

$$f(x) = (x - \omega_1)(x - \omega_2) \cdots (x - \omega_n)$$

be the decomposition of a function  $f(x)$  of a field  $\mathfrak{K}_0$  in an extension field  $\mathfrak{L}$ . Then the field  $\mathfrak{N} = \mathfrak{K}_0(\omega_1, \dots, \omega_n)$  lying between  $\mathfrak{K}_0$  and  $\mathfrak{L}$  represents an extension just sufficient for this decomposition. If we have a second decomposition of  $f(x)$  in another extension field  $\mathfrak{L}'$ , and if  $\bar{\mathfrak{N}}$  is the field that is obtained from  $\mathfrak{K}_0$  by adjunction of the zeros of  $f(x)$  occurring in  $\mathfrak{L}'$ , then we have an isomorphic correspondence  $\pi'$  between  $\mathfrak{N}$  and  $\bar{\mathfrak{N}}$  that leaves all elements of  $\mathfrak{K}_0$  unchanged, and the decomposition of  $f(x)$  in  $\mathfrak{L}'$  becomes

$$f(x) = (x - \bar{\omega}_1)(x - \bar{\omega}_2) \cdots (x - \bar{\omega}_n),$$

where  $\omega_i$  and  $\bar{\omega}_i$  ( $i = 1, \dots, n$ ) correspond to each other in the isomorphism  $\pi'$ . If we therefore have a rational combination of  $\omega_1, \dots, \omega_n$  with coefficients from  $\mathfrak{K}_0$ , hence an element of  $\mathfrak{N}$ , then we obtain the corresponding element from  $\bar{\mathfrak{N}}$  by replacing each  $\omega_i$  by  $\bar{\omega}_i$ . In particular it follows that if certain of the roots  $\omega_i$  are equal, the corresponding roots  $\bar{\omega}_i$  must also be equal. We can therefore speak of the *number of the simple, double, triple, ... roots* of an equation without specifying the extension field. The determination of these numbers will be carried out later (§ 10.).

*Normal extensions.*<sup>E 56</sup> — The extensions of a field  $\mathfrak{K}_0$  that just suffice for the complete decomposition of a function  $f(x)$  belong to the special kind of *normal* extensions.<sup>E 57</sup> An extension field  $\mathfrak{N}$  of  $\mathfrak{K}_0$  is called *normal with respect to  $\mathfrak{K}_0$*  if it is algebraic with respect to  $\mathfrak{K}_0$  and if moreover every integral function  $f(x)$  from  $\mathfrak{K}_0$  that is irreducible in  $\mathfrak{K}_0$  but has a zero in  $\mathfrak{N}$  breaks up into linear factors in  $\mathfrak{N}$ . Evidently every extension equivalent to a normal extension is likewise normal. — We derive some simple theorems concerning normal fields:

3. If the field  $\mathfrak{N}$  is normal with respect to its subfield  $\mathfrak{K}_0$ , then it is also normal with respect to every field  $\mathfrak{K}_1$  between  $\mathfrak{K}_0$  and  $\mathfrak{N}$ .

For, first of all,  $\mathfrak{N}$  is algebraic with respect to  $\mathfrak{K}_1$ . Now if  $\varphi(x)$  is an irreducible integral function from  $\mathfrak{K}_1$  and if  $\varphi(x)$  has a zero  $j$  in  $\mathfrak{N}$ , then  $j$  is also a zero of an irreducible function

$f(x)$  of the field  $\mathfrak{K}_0$ , and since  $\mathfrak{N}$  is normal with respect to  $\mathfrak{K}_0$ ,  $f(x)$  breaks up into linear factors in  $\mathfrak{N}$ . But since  $f(x)$  is also a function in the field  $\mathfrak{K}_1$  and has the zero  $j$  in common with the irreducible function  $\varphi(x)$  of this field,  $\varphi(x)$  is a factor of  $f(x)$ ; consequently  $\varphi(x)$  also breaks up into linear factors in  $\mathfrak{N}$ . This proves the assertion.

*Normal functions.* <sup>E58</sup> — An integral function  $f(x)$  of a field  $\mathfrak{K}_0$  shall be called *normal in*  $\mathfrak{K}_0$  if it is irreducible in  $\mathfrak{K}_0$  and moreover the extension  $\mathfrak{K}_0(j)$  that is obtained by adjunction of a zero  $j$  of  $f(x)$  is normal. — If  $f(x)$  is normal in  $\mathfrak{K}_0$ , then  $f(x)$  breaks up into linear factors in the field  $\mathfrak{K}_0(j)$  obtained by adjunction of a zero  $j$  of  $f(x)$ . This follows immediately from the definition of normal extensions and functions. But the converse also holds:

4. *If a function  $f(x)$  irreducible in a field  $\mathfrak{K}_0$  breaks up completely in the field  $\mathfrak{K}_0(j)$  arising by adjunction of a zero  $j$ , then it is normal with respect to  $\mathfrak{K}_0$ .* <sup>E59</sup>

For if  $g(x)$  is an irreducible function from  $\mathfrak{K}_0$ , and if  $g(x)$  has a zero  $\alpha$  in  $\mathfrak{K}_0(j)$ , then we can put  $\alpha = \varphi(j)$ , where  $\varphi(x)$  denotes an integral function from  $\mathfrak{K}_0$ . Now if

$$f(x) = (x - j)(x - j_1) \cdots (x - j_{n-1})$$

is the presupposed decomposition of  $f(x)$  in  $\mathfrak{K}_0(j)$ , then we conclude in the familiar way that the coefficients of the function

$$h(x) = (x - \varphi(j))(x - \varphi(j_1)) \cdots (x - \varphi(j_{n-1}))$$

become symmetric functions of  $j, j_1, \dots, j_{n-1}$ , hence elements from  $\mathfrak{K}_0$ . <sup>E60</sup>  $h(x)$  is therefore a function in  $\mathfrak{K}_0$  that has the factor  $x - \varphi(j)$  in common with the function  $g(x)$  irreducible in  $\mathfrak{K}_0$ , and is therefore divisible by  $g(x)$ . Since  $h(x)$  breaks up completely in  $\mathfrak{K}_0(j)$ , the same holds for  $g(x)$ , i.e. for every function irreducible in  $\mathfrak{K}_0$  that has a zero in  $\mathfrak{K}_0(j)$ .  $\mathfrak{K}_0(j)$  is therefore a normal extension of  $\mathfrak{K}_0$ , consequently  $f(x)$  is normal in  $\mathfrak{K}_0$ .

5. *If  $f(x)$  is a normal function of the field  $\mathfrak{K}_0$ ,  $\mathfrak{L}$  any extension of  $\mathfrak{K}_0$ , then every factor of  $f(x)$  irreducible in  $\mathfrak{L}$  is normal in  $\mathfrak{L}$ .*

For if  $g(x)$  is such a factor and if  $\mathfrak{L}$  is extended by adjunction of a zero  $j$  of  $g(x)$ , then  $\mathfrak{L}(j)$  contains the field  $\mathfrak{K}_0(j)$ , and  $j$  is a zero of  $f(x)$ . Since the function  $f(x)$  is normal in  $\mathfrak{K}_0$ , it breaks up into linear factors in  $\mathfrak{K}_0(j)$ , hence also in  $\mathfrak{L}(j)$ . Since in the field  $\mathfrak{L}$   $g(x)$  is a factor of  $f(x)$ ,  $g(x)$  also breaks up into linear factors in  $\mathfrak{L}(j)$ , hence  $g(x)$  is normal in  $\mathfrak{L}$  by Theorem 4., q.e.d.

6. *An extension  $\mathfrak{N}$  of a field  $\mathfrak{K}_0$  that just suffices to break up a function  $f(x)$  from  $\mathfrak{K}_0$  completely is normal.*

For if

$$f(x) = (x - j_1)(x - j_2) \cdots (x - j_n)$$

is the decomposition of  $f(x)$  in  $\mathfrak{N}$ ,  $g(x)$  an irreducible function of the field  $\mathfrak{K}_0$  which has a zero  $\beta$  in  $\mathfrak{N}$ , then  $\beta$  can be represented in the form

$$\beta = \psi(j_1, j_2, \dots, j_n)$$

where  $\psi(x_1, x_2, \dots, x_n)$  denotes an integral function <sup>E61</sup> from  $\mathfrak{K}_0$ . By the  $n!$  permutations of the elements  $j_1, j_2, \dots, j_n$  there arise from  $\beta$   $n!$  elements of the field  $\mathfrak{N}$ , which may be called  $\beta, \beta_1, \dots, \beta_{n!-1}$ . The function

$$\varphi(x) = (x - \beta)(x - \beta_1) \cdots (x - \beta_{n!-1})$$

is contained in the field  $\mathfrak{K}_0$ , since its coefficients are symmetric functions of  $j_1, j_2, \dots, j_n$  with coefficients from  $\mathfrak{K}_0$ ; it has the factor  $x - \beta$  in common with the function  $g(x)$  irreducible in  $\mathfrak{K}_0$ , and is therefore divisible by  $g(x)$ . Since  $\varphi(x)$  breaks up completely in  $\mathfrak{N}$ ,  $g(x)$  also breaks up completely in  $\mathfrak{N}$ . But this satisfies the conditions for the normal extension. <sup>E 62</sup>

In Theorems 1., 2., 6. of this section, the place of a single function  $f(x)$  of the field  $\mathfrak{K}_0$  can of course also be taken by a system  $S$  consisting of a *finite* number of functions of this field. For if the system  $S$  consists of the functions

$$\varphi_1(x), \varphi_2(x), \dots, \varphi_m(x)$$

and we put

$$f(x) = \varphi_1(x) \cdot \varphi_2(x) \cdots \varphi_m(x)$$

then it is clear that in an extension field  $\mathfrak{L}$  of  $\mathfrak{K}_0$  all the functions of the system  $S$  break up completely if and only if the function  $f(x)$  breaks up completely in  $\mathfrak{L}$ .

### §9.

#### Differentiation.

To determine the number of zeros of a given multiplicity, we consider the derivatives of the functions. We define, purely formally, the *derivative*, or *differential quotient*,  $\frac{d}{dx}f(x) = f'(x)$ , of an integral function

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

of an indeterminate  $x$  with respect to this indeterminate, as the expression

$$a_1 + 2a_2x + \cdots + na_nx^{n-1},$$

so that  $f'(x)$  occurs as a function in every field  $\mathfrak{K}$  in which  $f(x)$  occurs. <sup>E 63</sup> It follows immediately from this definition that if

$$g(x) = b_0 + b_1x + \cdots + b_mx^m$$

is a second function from  $\mathfrak{K}$ , then

$$\frac{d}{dx}(f(x) \pm g(x)) = \frac{d}{dx}f(x) \pm \frac{d}{dx}g(x).$$

Further,

$$\begin{aligned} \frac{d}{dx}(f(x) \cdot g(x)) &= \frac{d}{dx}\Sigma a_q b_r x^{q+r} = \Sigma(q+r)a_q b_r x^{q+r-1} \\ &= \Sigma a_q x^q \cdot r b_r x^{r-1} + \Sigma q a_q x^{q-1} b_r x^r = f(x) \frac{d}{dx}g(x) + \frac{d}{dx}f(x) \cdot g(x), \end{aligned}$$

hence

$$\frac{d}{dx}(f(x) \cdot g(x)) = f(x) \cdot g'(x) + f'(x) \cdot g(x).$$

Now let  $R(x)$  be a rational function of  $x$ . We can represent it in different ways as a quotient of integral functions

$$R(x) = \frac{u}{v} = \frac{u_1}{v_1}.$$

But then

$$(1.) \quad uv_1 = vu_1.$$

If we form the derivative on both sides, we obtain

$$uv'_1 + u'v_1 = vu'_1 + v'u_1,$$

hence

$$(2.) \quad u'v_1 - vu'_1 = v'u_1 - uv'_1.$$

If we multiply this equation by  $vv_1$ , we obtain

$$(3.) \quad v_1^2vu' - v^2v_1u'_1 = vv_1(v'u_1 - uv'_1).$$

If we multiply equation (1.) by  $vv'_1 + v'v_1$ , we obtain

$$vv_1uv'_1 + v_1^2uv' = vv_1v'u_1 + v^2u_1v'_1,$$

hence

$$(4.) \quad v_1^2uv' - v^2u_1v'_1 = vv_1(v'u_1 - uv'_1).$$

From (3.) and (4.) it follows that

$$(vu' - uv')v_1^2 = (v_1u'_1 - u_1v'_1)v^2,$$

hence

$$(5.) \quad \frac{vu' - uv'}{v^2} = \frac{v_1u'_1 - u_1v'_1}{v_1^2}.$$

Accordingly, we are justified in taking the expression  $\frac{vu' - uv'}{v^2}$  to be the derivative of a rational function  $R(x) = \frac{u}{v}$ , because this definition, as equation (5.) shows, is independent of the particular representation of  $R(x)$ , and because, in the case that  $R(x)$  equals an integral function  $u$  (which can be written in the form  $\frac{u}{\varepsilon}$ ), it agrees with the definition given earlier. By direct calculation it then follows at once that for any two rational functions  $u, v$  the laws hold:

$$(6.) \quad \frac{d}{dx}(u \pm v) = u' \pm v',$$

$$(7.) \quad \frac{d}{dx}(uv) = uv' + u'v,$$

$$(8.) \quad \frac{d}{dx}\left(\frac{u}{v}\right) = \frac{vu' - uv'}{v^2}.$$

From (7.) it further follows that

$$\frac{d}{dx}u^n = nu^{n-1}u',$$

and from this, if  $\lambda(u) = a_0 + a_1u + \cdots + a_nu^n$  is an integral function of  $u$  (in the field  $\mathfrak{K}$ ),

$$\frac{d}{dx}\lambda(u) = (a_1 + 2a_2u + \cdots + na_nu^{n-1})u' = \frac{d}{du}\lambda(u) \cdot \frac{du}{dx}.$$

The application of this equation yields, if  $\mu(x)$  likewise denotes an integral function:

$$\frac{d}{dx} \frac{\lambda(u)}{\mu(u)} = \frac{\mu(u) \frac{d}{du} \lambda(u) - \lambda(u) \frac{d}{du} \mu(u)}{(\mu(u))^2} \frac{du}{dx} = \frac{d}{du} \frac{\lambda(u)}{\mu(u)} \cdot \frac{du}{dx}.$$

In other words: If  $v$  is a rational function of  $u$ ,  $u$  a rational function of  $x$ , then

$$\frac{dv}{dx} = \frac{dv}{du} \cdot \frac{du}{dx}.$$

The concept of the differential quotient can also be extended still further, but we shall not go into this here.

### § 10.

#### The multiplicity of the zeros of an integral function.

In the questions treated so far the characteristic of the field has been of no significance; in the following investigations, however, we encounter essential differences between the fields of characteristic 0 and those of prime-number characteristic. This first shows itself in the question of the circumstances under which the derivative of a rational function vanishes.

Let a field  $\mathfrak{K}$  be given, and let

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

be an integral function of the indeterminate  $x$  in  $\mathfrak{K}$ . Then

$$f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1},$$

so that in the case of characteristic 0  $f'(x)$  vanishes only if  $a_1 = 0, a_2 = 0, \dots, a_n = 0$ , that is, if  $f(x)$  does not contain  $x$ . But if the characteristic of  $\mathfrak{K}$  is a prime number  $p$ , then the coefficient  $q \cdot a_q$  occurring in  $f'(x)$  is equal to 0 if  $a_q = 0$  or  $q$  is divisible by  $p$  (§ 4, 4.); therefore  $f'(x)$  vanishes if and only if the only powers of  $x$  that actually occur in  $f(x)$  are those whose exponent is divisible by  $p$  — in other words, if  $f(x)$  is an integral function of  $x^p$ .

— If we have a rational function in  $\mathfrak{K}$  which we represent as a quotient of two integral functions in the reduced form  $\frac{u}{v}$ , then its derivative becomes  $\frac{vu' - uv'}{v^2}$ , and is hence equal to 0 only if  $vu' = uv'$ . Since  $u$  and  $v$  are relatively prime, this equation can hold only if  $v$  goes into  $v'$ ,  $u$  into  $u'$  (§ 5, 3.). But since the degrees of  $u'$  and  $v'$  are respectively smaller than those of  $u$  and  $v$ , this is possible only if  $u' = 0, v' = 0$ , hence if  $u$  and  $v$  are free of  $x$  or, in the case of characteristic  $p$ , functions of  $x^p$ . Therefore the theorem holds:

1. For the derivative of a rational function  $R(x)$  to vanish it is necessary and sufficient that  $R(x)$  be free of  $x$  or a rational function of  $x^p$ , according as the characteristic is 0 or  $p$ .

Now let  $f(x)$  be an integral function in a field  $\mathfrak{K}$ . Within a suitable extension field  $f(x)$  breaks up into linear factors, and if  $x - \alpha$  is an  $r$ -fold factor ( $r > 0$ ), then we have

$$(1.) \quad f(x) = (x - \alpha)^r g(x),$$

where  $g(x)$  no longer contains the factor  $x - \alpha$ . From (1.) it follows that

$$(2.) \quad f'(x) = (x - \alpha)^{r-1}(r\varepsilon g(x) + (x - \alpha)g'(x)),$$

from which we see that the derivative  $f'(x)$  contains the factor  $x - \alpha$  at least  $(r - 1)$  times, and that it contains it exactly  $(r - 1)$  times if  $r\varepsilon \neq 0$ . But if  $\mathfrak{K}$  has the characteristic  $p$  and  $r$  is divisible by  $p$ , then  $r\varepsilon = 0$ , and  $f'(x) = (x - \alpha)^r g'(x)$  is divisible by  $(x - \alpha)^r$ . Therefore the theorem holds:

2. *If  $f(x)$  has an  $r$ -fold linear factor ( $r \geq 1$ ), then the derivative  $f'(x)$  has this factor at least  $(r - 1)$  times; it has it at least  $r$  times if the field  $\mathfrak{K}$  to which  $f(x)$  belongs has the characteristic  $p$  and  $r$  is divisible by the prime number  $p$ , and otherwise exactly  $(r - 1)$  times. (If the derivative vanishes, then it is divisible by every power of  $x - \alpha$ , however high, and hence in this sense contains the factor  $x - \alpha$  infinitely often).*

From 2. it follows easily, for fields of arbitrary characteristic:

3. *If  $f(x)$  has only simple factors, then the greatest common divisor*

$$(f(x), f'(x))$$

*of  $f(x)$  and  $f'(x)$  is equal to  $\varepsilon$ , and otherwise it is of at least the first degree.*

Let

$$(3.) \quad f(x) = (x - \alpha_1)^{r_1} \cdot (x - \alpha_2)^{r_2} \cdots (x - \alpha_\nu)^{r_\nu},$$

where the zeros  $\alpha_i$  are to be different from one another and the exponents  $r_i > 0$ . If the characteristic is equal to  $p$  and  $f(x)$  is the  $p$ -th power of an integral function (of the original or of an extension field), then all exponents  $r_i$  are divisible by  $p$ . Therefore by 2.  $f'(x)$  contains every factor  $x - \alpha_i$  at least as often as  $f(x)$  does, and is hence divisible by  $f(x)$ . But since the degree of  $f'(x)$  is smaller than the degree of  $f(x)$ , this is only possible if  $f'(x) = 0$ . This also follows immediately from the fact that differentiating an equation of the form  $f(x) = [\varphi(x)]^p$  gives  $f'(x) = p[\varphi(x)]^{p-1} \cdot \varphi'(x)$ , hence  $f'(x) = 0$  in the case of characteristic  $p$ . But from this it follows that  $f(x)$  is an integral function of  $x^p$ . If conversely  $f(x)$  is presupposed to be an integral function of  $x^p$ , then  $f'(x)$  vanishes, and from 2. it follows that all exponents  $r_i$  are divisible by  $p$ . Therefore there holds:

4. *If in the case of characteristic  $p$   $f(x)$  is an integral function of  $x^p$ , then  $f(x)$  is the  $p$ -th power of an integral function, and conversely.*

We can also derive this result in another way: If  $a$  and  $b$  are any two elements of a field  $\mathfrak{K}$  of characteristic  $p$ , then the binomial expansion yields

$$(a + b)^p = a^p + b^p,$$

because all other terms of the expansion have a numerical coefficient divisible by  $p$ , and hence vanish. Raising the preceding equation to the  $p$ -th power gives

$$(a + b)^{p^2} = (a^p + b^p)^p = a^{p^2} + b^{p^2}$$

and, continuing in this way, in general

$$(4.) \quad (a + b)^{p^f} = a^{p^f} + b^{p^f}$$

for every natural number  $f$ . Likewise there holds

$$(5.) \quad (a - b)^{p^f} = a^{p^f} - b^{p^f}.$$

This follows for odd  $p$  by the same expansion. But if  $p = 2$ , then  $2b = 0$ ,  $2b^{p^f} = 0$ , hence  $-b = b$ ,  $-b^{p^f} = b^{p^f}$ ,<sup>E 65</sup> and the formulas (4.) and (5.) become identical. From (4.) it follows immediately that

$$(4'.) \quad (a_1 + a_2 + \cdots + a_n)^{p^f} = a_1^{p^f} + a_2^{p^f} + \cdots + a_n^{p^f}.$$

We can also apply this equation to integral functions of an indeterminate  $x$  in the field  $\mathfrak{K}$ , since these belong to the field  $\mathfrak{K}(x)$ , which after all also has the characteristic  $p$  (§ 4, 3.). Then one sees at once that the  $p^f$ -th power of such a function is an integral function of  $x^{p^f}$ . If conversely  $f(x)$  is an integral function of  $x^{p^f}$ :

$$f(x) = c_0 + c_1 x^{p^f} + c_2 x^{2p^f} + \cdots + c_n x^{np^f}$$

and if we extend the field  $\mathfrak{K}$  to a field  $\mathfrak{L}$  within which the functions  $x^{p^f} - c_0, x^{p^f} - c_1, \dots, x^{p^f} - c_n$  break up into linear factors, then one can determine the elements  $\gamma_0, \gamma_1, \dots, \gamma_n$  in  $\mathfrak{L}$  such that  $\gamma_k^{p^f} = c_k$  holds. But it then follows that

$$f(x) = (\gamma_0 + \gamma_1 x + \gamma_2 x^2 + \cdots + \gamma_n x^n)^{p^f}.$$

This proves Theorem 4. again, only in a somewhat more general formulation:

4<sup>a</sup>. *If in the case of characteristic  $p$   $f(x)$  is an integral function of  $x^{p^f}$ , then  $f(x)$  is the  $p^f$ -th power of an integral function of  $x$ , and conversely.*<sup>E 64</sup>

Let  $F(x)$  be an integral function of the indeterminate  $x$  in a field  $\mathfrak{K}$  of arbitrary characteristic, let the coefficient of the highest power of  $x$  be equal to  $\varepsilon$ , and let

$$(6.) \quad F(x) = (x - \alpha_1)^{r_1} \cdots (x - \alpha_\nu)^{r_\nu}$$

represent the decomposition of  $F(x)$  in a suitable extension field ( $\alpha_1, \dots, \alpha_\nu$  presupposed to be different). We denote by  $f_m(x)$ , for every natural number  $m$ , the product of those linear factors, taken singly, of  $F(x)$  which occur  $m$ -fold in  $F(x)$ . If there are none, then we put  $f_m(x) = \varepsilon$ . Accordingly,

$$(7.) \quad F(x) = f_1(x) \cdot (f_2(x))^2 \cdot (f_3(x))^3 \cdots$$

We now wish to prove the following theorems:

5. *If the characteristic of  $\mathfrak{K}$  is equal to 0, then each of the functions  $f_m(x)$  belongs to the field  $\mathfrak{K}$  and can be determined rationally.*

6. *If the characteristic of  $\mathfrak{K}$  is equal to  $p$ ,  $m$  not divisible by  $p$ , then  $f_m(x)$  belongs to the field  $\mathfrak{K}$  and can be determined rationally.*

7. If the characteristic of  $\mathfrak{K}$  is equal to  $p$ ,  $\pi = p^f$  the highest power of  $p$  contained in  $m$ , then  $(f_m(x))^\pi$  belongs to the field  $\mathfrak{K}$  and can be determined rationally. <sup>E 66, 67, 68</sup>

For if  $F'(x)$  denotes the derivative of  $F(x)$  with respect to  $x$ , then it follows from 2. that the function belonging to the field  $\mathfrak{K}$

$$\varphi(x) = \frac{F(x)}{(F(x), F'(x))}$$

is, in the case of characteristic 0, equal to the product of *all*, in the case of characteristic  $p$  equal to the product of *those* linear factors  $x - \alpha_k$ , taken singly, for which the exponent  $r_k$  in equation (6.) is not divisible by  $p$ . Let us now consider the expression

$$\chi_m(x) = \frac{((\varphi(x))^m, F(x))}{((\varphi(x))^{m-1}, F(x))}. \quad (m \geq 1)$$

It is an integral function composed of factors  $x - \alpha_k$  and can, in the case of characteristic  $p$ , contain only such factors  $x - \alpha_k$  for which  $r_k$  is not divisible by  $p$ . If we presuppose this about  $r_k$  in the case of characteristic  $p$ , then for  $r_k < m$  both the numerator and the denominator of the expression  $\chi_m(x)$  contain the factor  $x - \alpha_k$  exactly  $r_k$  times. If  $r_k \geq m$ , then  $x - \alpha_k$  is contained  $m$  times in the numerator,  $(m - 1)$  times in the denominator.  $\chi_m(x)$  therefore represents the product of those linear factors  $x - \alpha_k$  for which  $r_k \geq m$  and, in the case of characteristic  $p$ , is not divisible by  $p$ . From this it follows that

$$\frac{\chi_m(x)}{\chi_{m+1}(x)} = f_m(x)$$

holds, unless the characteristic is equal to  $p$  and  $m$  is divisible by  $p$ .

This proves Theorems 5. and 6. In the case  $f = 0$ , Theorem 7. coincides with Theorem 6. We prove Theorem 7. by induction, assuming that it has been proved for every  $m$  that contains the prime number  $p$  fewer than  $f$  times as a factor. Then those factors  $(f_m(x))^m$  in which  $m$  is not divisible by  $\pi = p^f$  are to be regarded as having been proved to belong to the field  $\mathfrak{K}$  and as determined. If we therefore divide both sides of (7.) by these factors, we obtain an equation of the form

$$(8.) \quad \Phi(x) = (f_\pi(x))^\pi \cdot (f_{2\pi}(x))^{2\pi} \cdots,$$

where  $\Phi(x)$  is a known function from  $\mathfrak{K}$ . Let

$$(9.) \quad \Phi(x) = (x - \beta_1)^{\varrho_1\pi} \cdot (x - \beta_2)^{\varrho_2\pi} \cdots (x - \beta_\lambda)^{\varrho_\lambda\pi}$$

be the decomposition of  $\Phi(x)$  into powers of different linear factors, and  $m = \mu \cdot \pi$ , where  $\mu$  no longer contains the factor  $p$ . The functions  $(f_{k\pi}(x))^\pi$  are integral functions of  $x^\pi$  (Theorem 4<sup>a</sup>.), hence the same holds for  $\Phi(x)$ . If we now put

$$x^\pi = y, \quad \beta_i^\pi = \gamma_i, \quad (f_{k\pi}(x))^\pi = g_k(y), \quad \Phi(x) = G(y),$$

then the equations (8.), (9.) go over into

$$(10.) \quad G(y) = g_1(y) \cdot (g_2(y))^2 \cdot (g_3(y))^3 \cdots,$$

$$(11.) \quad G(y) = (y - \gamma_1)^{e_1} \cdot (y - \gamma_2)^{e_2} \cdots (y - \gamma_\lambda)^{e_\lambda},$$

where  $G(y)$  is a known function from  $\mathfrak{K}$ . The zeros  $\gamma_1, \gamma_2, \dots, \gamma_\lambda$  are different; for from  $\gamma_k = \gamma_l$  it would follow that

$$\begin{aligned} 0 &= \gamma_k - \gamma_l = \beta_k^\pi - \beta_l^\pi = (\beta_k - \beta_l)^\pi, \\ 0 &= \beta_k - \beta_l, \quad \beta_k = \beta_l, \end{aligned}$$

<sup>E 69</sup> while  $\beta_1, \beta_2, \dots, \beta_\lambda$  were presupposed to be different.  $g_\mu(y)$  is the product of those factors  $y - \gamma_l$ , linear with respect to  $y$  and taken singly, for which  $e_l = \mu$ . Since by hypothesis  $\mu$  is not divisible by  $p$ , it follows by 6. that  $g_\mu(y)$  is a function in  $\mathfrak{K}$  that can be determined rationally. If we substitute  $x^\pi$  for  $y$  again in  $g_\mu(y)$ , we obtain, since  $m = \mu\pi$ ,

$$g_\mu(y) = (f_m(x))^\pi,$$

whereby 7. is proved.

Accordingly, in all cases  $(f_m(x))^m$  is a function in  $\mathfrak{K}$  that can be determined rationally. If we divide the degree of this function by  $m$ , we have the number of the  $m$ -fold zeros of the function  $F(x)$ .

## § 11.

### Perfect and imperfect fields.

In § 7 it was shown that a number of theorems of *Galois* theory hold in every field. But if this theory is to remain valid unchanged, in all its essential features, in a field  $\mathfrak{K}$ , we also need the theorem that an integral function irreducible in  $\mathfrak{K}$  can have only simple zeros. This theorem, however, does not hold in full generality, and so we are forced to make a distinction, which we express in the following definition:

*A field  $\mathfrak{K}$  shall be called perfect if every integral function  $f(x)$  from  $\mathfrak{K}$  that has multiple zeros (in a suitable extension field) is reducible in  $\mathfrak{K}$ ; it shall be called imperfect, on the other hand, if there are irreducible functions in  $\mathfrak{K}$  with multiple zeros.*

We obtain the simple criteria:

1. *Every field of characteristic 0 is perfect.*
2. *Among the fields whose characteristic is a prime number  $p$  there are perfect and imperfect ones; such a field is perfect if the extraction of the  $p$ -th root (which here proves to be a unique operation) can be carried out in it without exception, and otherwise imperfect.* <sup>E 70</sup>

For the proof we note first that in a field  $\mathfrak{K}$  of characteristic  $p$  there can never be more than one  $p$ -th root, and hence also never more than one  $p^f$ -th root, of an element  $\gamma$ . For if two elements  $\alpha, \beta$  satisfy  $\alpha^p = \beta^p = \gamma$ , then it follows (cf. the computation  $0 = \gamma_k - \gamma_l = (\beta_k - \beta_l)^\pi$  on p. 36) that  $0 = \alpha^p - \beta^p = (\alpha - \beta)^p$ , and therefore  $\alpha - \beta = 0$ ,  $\alpha = \beta$ . No extension of  $\mathfrak{K}$  can change this either, since the characteristic remains  $p$  after all. The function  $x^{p^f} - \gamma$  is therefore, in  $\mathfrak{K}$  or in an extension field in which it breaks up completely, the  $p^f$ -th power of a linear factor:

$$x^{p^f} - \gamma = (x - \delta)^{p^f},$$

which, incidentally, also follows from § 10, 4<sup>a</sup>. The prime field  $\mathfrak{P}_p$  (§ 4) provides the simplest example <sup>E 71</sup> of a field in which the extraction of the  $p$ -th root can be carried out without

restriction. For by *Fermat's theorem*<sup>E72</sup> the equation  $a^p = a$  holds for every element of  $\mathfrak{P}_p$ , and hence also  $\sqrt[p]{a} = a$ . Now let  $\mathfrak{K}$  be any field of characteristic  $p$ ; we extend it, by adjoining a transcendental element  $u$ , to  $\mathfrak{L} = \mathfrak{K}(u)$ . If  $\alpha$  is an element of  $\mathfrak{L}$ , then either  $\alpha$  is an element of  $\mathfrak{K}$ , and then so is  $\alpha^p$ , or  $\alpha$  does not belong to  $\mathfrak{K}$ ; in that case  $\alpha$ , regarded as a rational function of  $u$ , has a definite degree  $> 0$ , and the degree of  $\alpha^p$  is  $p$  times this degree (§ 5, 6.). In no case can  $\alpha^p = u$  hold; thus the element  $u$  of the field  $\mathfrak{L}$  has no  $p$ -th root in  $\mathfrak{L}$ .<sup>E73</sup> — Now let  $\mathfrak{K}$  again be any field of characteristic  $p$  and  $\gamma$  any element of  $\mathfrak{K}$ ; then the function  $x^{p^f} - \gamma$  has, either in  $\mathfrak{K}$  itself or in an extension field, the decomposition

$$(1.) \quad x^{p^f} - \gamma = (x - \delta)^{p^f}.$$

So if we decompose  $x^{p^f} - \gamma$  in  $\mathfrak{K}$  itself into irreducible factors, then all these factors are powers of  $x - \delta$ , and they must all have the same exponent, since otherwise a factor with a larger exponent would be divisible by the one with a smaller exponent, and so would not be irreducible. The factor irreducible in  $\mathfrak{K}$  therefore has the form

$$(2.) \quad (x - \delta)^{p^r} = x^{p^r} - \delta^{p^r},$$

where  $0 \leq r \leq f$ . The case  $r = 0$  occurs when  $\delta$ , i.e. the  $p^f$ -th root of  $\gamma$ , belongs to the field  $\mathfrak{K}$ . But if the  $p$ -th root (and hence also the  $p^f$ -th root) of  $\gamma$  does not exist in  $\mathfrak{K}$ , then  $r > 0$ , and  $x^{p^r} - \delta^{p^r}$  is then a function irreducible in  $\mathfrak{K}$  with  $p^r > 1$  equal zeros. The field  $\mathfrak{K}$  is therefore imperfect.

Let us now assume that  $\mathfrak{K}$  either has characteristic 0, or that  $\mathfrak{K}$  has characteristic  $p$  but that for every element of  $\mathfrak{K}$  its  $p$ -th root is contained in  $\mathfrak{K}$  itself. If  $f(x)$  is then an integral function of degree  $n$  in  $\mathfrak{K}$  that has multiple zeros, then

$$(f(x), f'(x))$$

is of degree at least 1. If  $f'(x)$  is different from 0, then the degree of  $(f(x), f'(x))$ , like that of  $f'(x)$ , is less than  $n$ , so  $f(x)$  is reducible. But if  $f'(x) = 0$ , which can happen only when the characteristic is a prime number  $p$ ,<sup>E74</sup> then  $f(x)$  is an integral function of  $x^p$ :

$$f(x) = a_0 + a_1 x^p + \cdots + a_\nu x^{\nu p} \quad (\nu p = n),$$

and it follows that

$$f(x) = (\sqrt[p]{a_0} + \sqrt[p]{a_1} x + \cdots + \sqrt[p]{a_\nu} x^\nu)^p,$$

where, by our hypothesis, the elements  $\sqrt[p]{a_0}, \sqrt[p]{a_1}, \dots, \sqrt[p]{a_\nu}$  belong to the field  $\mathfrak{K}$ ; hence in this case, too,  $f(x)$  is reducible in  $\mathfrak{K}$ . — This proves Theorems 1. and 2.

Among the theorems of ordinary *Galois* theory that do not hold without exception in all fields, we single out two which, as will be shown later, are most closely connected with each other, and which may be called the *theorem of primitive elements*<sup>E75</sup> and the *theorem of intermediate fields*. The first states that every finite extension is simple, the second that between a field  $\mathfrak{K}$  and a finite extension  $\mathfrak{L}$  of it there always lie only finitely many fields. The converse of the latter theorem, as is easy to see, holds without exception:

3. If only finitely many fields lie between a field  $\mathfrak{K}$  and its extension field  $\mathfrak{L}$ , then  $\mathfrak{L}$  is finite with respect to  $\mathfrak{K}$ .

For, to begin with,  $\mathfrak{L}$  cannot contain any element  $x$  that is transcendental with respect to  $\mathfrak{K}$ ; for otherwise we would have infinitely many fields

$$\mathfrak{K}(x), \mathfrak{K}(x^2), \mathfrak{K}(x^3), \dots, \mathfrak{K}(x^n), \dots,$$

which, as one sees at once (e.g. from § 5, 6.), are all different from one another and lie between  $\mathfrak{K}$  and  $\mathfrak{L}$ . By § 2, 3., every element of  $\mathfrak{L}$  belongs to a field  $\mathfrak{K}_i$  between  $\mathfrak{K}$  and  $\mathfrak{L}$  that arises from  $\mathfrak{K}$  by adjunction of a system  $\mathfrak{S}_i$  of finitely many elements.<sup>E 76</sup> By hypothesis, however, there are only finitely many of these fields. If we denote them by  $\mathfrak{K}_1, \mathfrak{K}_2, \dots, \mathfrak{K}_n$ , denote by  $\mathfrak{S}_i$  ( $i = 1, \dots, n$ ) a finite system of elements such that  $\mathfrak{K}(\mathfrak{S}_i) = \mathfrak{K}_i$ , and denote by  $\mathfrak{S}$  the finite system comprising all the elements of the systems  $\mathfrak{S}_i$ , then  $\mathfrak{K}(\mathfrak{S})$  contains all the fields  $\mathfrak{K}_i$ , and therefore  $\mathfrak{K}(\mathfrak{S}) = \mathfrak{L}$ <sup>E 77</sup>. Since, moreover, the elements of  $\mathfrak{S}$  are finite in number and, as we saw, algebraic with respect to  $\mathfrak{K}$ , it follows (§ 7, 6.) that  $\mathfrak{K}(\mathfrak{S}) = \mathfrak{L}$  is finite with respect to  $\mathfrak{K}$ .

The theorem of primitive elements in ordinary *Galois* theory rests on the following theorem, which holds for all fields:

4. *If the field  $\mathfrak{L}$  arises from its subfield  $\mathfrak{K}$  by adjoining finitely many elements  $\alpha, \beta, \gamma, \dots$ , each of which satisfies in  $\mathfrak{K}$  an equation with only simple roots, then  $\mathfrak{L}$  is simple with respect to  $\mathfrak{K}$  and can also be obtained from  $\mathfrak{K}$  by adjoining one element that likewise satisfies in  $\mathfrak{K}$  an equation with only simple roots.*

It is of course only necessary to carry out the proof for the case where  $\mathfrak{L}$  is derived from  $\mathfrak{K}$  by first adjoining two elements  $\alpha, \beta$ ; by repeating the same mode of inference, the same result then follows for any arbitrary finite number. — *We carry out the proof here under the hypothesis that  $\mathfrak{K}$  contains infinitely many elements; for the case of a field with finitely many elements a different proof will follow below (§ 15, 9.).* — So now let  $f(x)$  and  $g(x)$  be integral functions from  $\mathfrak{K}$  that vanish for  $x = \alpha$  and  $x = \beta$  respectively and that break up, in a suitable extension field  $\mathfrak{M}$ , into linear factors that are all different. Let the decompositions be

$$\begin{aligned} f(x) &= (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_m), \\ g(x) &= (x - \beta_1)(x - \beta_2) \cdots (x - \beta_n), \end{aligned}$$

where  $\alpha_1$  and  $\beta_1$  are put for  $\alpha$  and  $\beta$ . By our hypothesis, the elements  $\alpha_1, \alpha_2, \dots, \alpha_m$  are all different from one another, and likewise  $\beta_1, \beta_2, \dots, \beta_n$ . If  $\mu$  is any element of  $\mathfrak{K}$ , then  $\alpha + \mu\beta$  is an element of  $\mathfrak{K}(\alpha, \beta) = \mathfrak{L}$ . Let us now consider the  $m \cdot n$  elements  $\alpha_i + \mu\beta_k$ . If two of them,  $\alpha_i + \mu\beta_k$  and  $\alpha_r + \mu\beta_s$ , are equal to one another without  $i = r, k = s$  holding at the same time, then  $\beta_k \neq \beta_s$ , since otherwise  $k = s, \alpha_i = \alpha_r, i = r$  would follow. In this case we therefore obtain

$$(3.) \quad \mu = \frac{\alpha_r - \alpha_i}{\beta_k - \beta_s}.$$

But since only a finite number of elements is represented in this form, while  $\mathfrak{K}$  contains infinitely many, we can and will choose from  $\mathfrak{K}$  an element  $\mu$  that does not have the form (3.), and we keep it fixed in what follows.<sup>E 78</sup> Now let  $\delta = \delta_1$  be an arbitrary element from  $\mathfrak{K}(\alpha, \beta)$ , hence an integral function  $\chi(\alpha, \beta) = \chi(\alpha_1, \beta_1)$  of  $\alpha$  and  $\beta$  with coefficients from  $\mathfrak{K}$ . We denote by

$$\begin{aligned} \gamma_1, \gamma_2, \dots, \gamma_{mn}, \\ \delta_1, \delta_2, \dots, \delta_{mn} \end{aligned}$$

those elements of  $\mathfrak{M}$  that arise from

$$\gamma = \gamma_1 = \alpha + \mu\beta, \quad \delta = \delta_1 = \chi(\alpha, \beta)$$

when all possible combinations  $\alpha_i, \beta_k$  are put for  $\alpha, \beta$ , and we form the function

$$h(x) = (x - \gamma_1)(x - \gamma_2) \cdots (x - \gamma_{mn}).$$

Since by the foregoing the elements  $\gamma_1, \gamma_2, \dots, \gamma_{mn}$  are all different,

$$\frac{h(x)}{x - \gamma_1}, \frac{h(x)}{x - \gamma_2}, \dots, \frac{h(x)}{x - \gamma_{mn}}$$

are integral functions of  $x$ , the first of which takes for  $x = \gamma_1$  the value  $h'(\gamma_1)$  different from 0 (if  $h'(x)$  denotes the derivative of  $h(x)$ ), while the others vanish for  $x = \gamma_1$ . The function  $h(x)$  is symmetric in  $\alpha_1, \dots, \alpha_m$  and in  $\beta_1, \dots, \beta_n$ , hence a function in  $\mathfrak{K}$ ; therefore  $h'(x)$  is also a function in  $\mathfrak{K}$ . Finally the function

$$(4.) \quad \varphi(x) = \frac{h(x)}{x - \gamma_1} \delta_1 + \frac{h(x)}{x - \gamma_2} \delta_2 + \cdots + \frac{h(x)}{x - \gamma_{mn}} \delta_{mn}$$

is also symmetric in  $\alpha_1, \dots, \alpha_m$  and in  $\beta_1, \dots, \beta_n$ , hence a function in  $\mathfrak{K}$ . If we put  $x = \gamma_1 = \gamma$  in (4.), we obtain

$$\varphi(\gamma) = h'(\gamma) \cdot \delta, \quad \delta = \frac{\varphi(\gamma)}{h'(\gamma)},$$

from which we see that  $\delta$  belongs to the field  $\mathfrak{K}(\gamma)$ . Since  $\gamma$  belongs to the field  $\mathfrak{K}(\alpha, \beta)$  and  $\delta$  is an arbitrary element of  $\mathfrak{K}(\alpha, \beta)$ , it follows that

$$\mathfrak{K}(\alpha, \beta) = \mathfrak{K}(\gamma).$$

Further, the equation  $h(x) = 0$ , which  $\gamma$  satisfies in  $\mathfrak{K}$ , has only simple roots; thus 4. is proved.

If  $\mathfrak{K}$  is a perfect field, then the equations irreducible in  $\mathfrak{K}$  that are satisfied by  $\alpha$  and  $\beta$  have only simple zeros; the hypotheses made about  $\alpha$  and  $\beta$  in Theorem 4. are therefore always fulfilled here. From this it follows by § 7, 6.:

5. *Every finite extension of a perfect field is simple.*

Now in order to show that neither the theorem of primitive elements nor the theorem of intermediate fields has unrestricted validity, we prove right here the following theorem, which we shall need later in the more thorough investigations on this subject:

6. *If  $\mathfrak{K}$  is a field of characteristic  $p$ ,  $\mathfrak{L}$  an extension of  $\mathfrak{K}$ , if the  $p$ -th power of every element of  $\mathfrak{L}$  is contained in  $\mathfrak{K}$ , but  $[\mathfrak{L} : \mathfrak{K}] > p$  (in so far as  $\mathfrak{L}$  is finite at all with respect to  $\mathfrak{K}$ ), then  $\mathfrak{L}$  is not a simple extension, and infinitely many fields lie between  $\mathfrak{K}$  and  $\mathfrak{L}$ .*

Proof: The first assertion is immediately evident; for the degree of a primitive element would have to be equal to  $[\mathfrak{L} : \mathfrak{K}] > p$ , while from the hypothesis it follows that every element of  $\mathfrak{L}$  satisfies an equation of degree  $p$  in  $\mathfrak{K}$ . — As regards the second assertion, it follows from the hypothesis first that  $\mathfrak{K}$  is an imperfect field; for otherwise the elements of  $\mathfrak{L}$ , which are indeed  $p$ -th roots of elements of  $\mathfrak{K}$ , would all belong to  $\mathfrak{K}$ , so  $[\mathfrak{L} : \mathfrak{K}] = 1$  would hold. From this it follows further that  $\mathfrak{K}$  contains infinitely many elements, because all fields with only

finitely many elements are perfect (see § 12, 2.).<sup>E 79</sup> Now let  $\alpha$  be any element contained in  $\mathfrak{L}$  but not in  $\mathfrak{K}$ . Then  $\alpha$  is a zero of the function  $x^p - \alpha^p$  of the field  $\mathfrak{K}$ , which is irreducible in this field.  $\mathfrak{K}(\alpha)$  is a field between  $\mathfrak{K}$  and  $\mathfrak{L}$  and different from  $\mathfrak{L}$ , because  $[\mathfrak{K}(\alpha) : \mathfrak{K}] = p$ . Let  $\beta$  be an element belonging to  $\mathfrak{L}$  but not to  $\mathfrak{K}(\alpha)$ ; then also  $[\mathfrak{K}(\beta) : \mathfrak{K}] = p$ , and  $\mathfrak{K}(\alpha)$  and  $\mathfrak{K}(\beta)$  are different. Now if  $\mu_1, \mu_2, \dots, \mu_k, \dots$  are infinitely many elements from  $\mathfrak{K}$  different from one another and from 0, then all the elements  $\omega_k = \alpha + \mu_k \beta$  belong to the field  $\mathfrak{L}$ , but none to the field  $\mathfrak{K}$ . For if  $\omega_k$  belonged to  $\mathfrak{K}$ , then  $\alpha = \omega_k - \mu_k \beta$  would belong to  $\mathfrak{K}(\beta)$ , which cannot be the case, because  $\alpha$  and  $\beta$  are of the same degree with respect to  $\mathfrak{K}$  and  $\mathfrak{K}(\alpha)$  and  $\mathfrak{K}(\beta)$  are different. The fields  $\mathfrak{K}(\omega_k)$  all lie between  $\mathfrak{K}$  and  $\mathfrak{L}$ , are of degree  $p$  with respect to  $\mathfrak{K}$ , and are all different from one another. For from  $\mathfrak{K}(\omega_k) = \mathfrak{K}(\omega_l)$  it would follow that

$$\alpha = \frac{\mu_l \omega_k - \mu_k \omega_l}{\mu_l - \mu_k} \quad \text{and} \quad \beta = \frac{\omega_l - \omega_k}{\mu_l - \mu_k}$$

would belong to the field  $\mathfrak{K}(\omega_k) = \mathfrak{K}(\omega_l)$ , and hence would be, with respect to  $\mathfrak{K}$ , primitive elements of this field. But then  $\mathfrak{K}(\alpha) = \mathfrak{K}(\omega_k) = \mathfrak{K}(\beta)$  would hold, while  $\mathfrak{K}(\alpha)$  and  $\mathfrak{K}(\beta)$  were already shown to be different. Thus infinitely many fields  $\mathfrak{K}(\omega_k)$  lie between  $\mathfrak{K}$  and  $\mathfrak{L}$ . This completely proves 6.

We can now easily show that the hypotheses of Theorem 6. can be realized by finite extensions. For this purpose we adjoin to an arbitrary field  $\mathfrak{M}$  of characteristic  $p$  two transcendental elements  $t, u$  and consider, besides the field  $\mathfrak{L} = \mathfrak{M}(t, u)$ , also the fields  $\mathfrak{K} = \mathfrak{M}(t^p, u^p)$ ,  $\mathfrak{K}' = \mathfrak{M}(t, u^p)$ . Then  $t$  does not occur in  $\mathfrak{K}$ , nor  $u$  in  $\mathfrak{K}'$ , and therefore the function  $x^p - t^p$  becomes irreducible in  $\mathfrak{K}$ , the function  $x^p - u^p$  in  $\mathfrak{K}'$ , from which

$$[\mathfrak{L} : \mathfrak{K}] = [\mathfrak{K}' : \mathfrak{K}] \cdot [\mathfrak{L} : \mathfrak{K}'] = [t : \mathfrak{K}] \cdot [u : \mathfrak{K}'] = p^2$$

follows. If on the other hand  $v$  is any element from  $\mathfrak{L} = \mathfrak{M}(t, u)$  and we represent it in the form  $v = \frac{v_1}{v_2}$ , where  $v_1$  and  $v_2$  belong to the domain of integrity  $\mathfrak{M}[t, u]$ , then  $v_1$  and  $v_2$  are represented as sums of terms of the form  $ct^m u^n$ , where  $c$  is an element of  $\mathfrak{M}$ . But then  $v_1^p, v_2^p$  become sums of terms of the form  $c^p t^{mp} u^{np}$  (§ 10, (4')), and so belong to the domain of integrity  $\mathfrak{M}[t^p, u^p]$ . Therefore  $v^p = \frac{v_1^p}{v_2^p}$  is an element of the field  $\mathfrak{K} = \mathfrak{M}(t^p, u^p)$ , and thus the extension  $\mathfrak{L}$  of the field  $\mathfrak{K}$ , although finite, is nevertheless not simple, and infinitely many fields lie between  $\mathfrak{K}$  and  $\mathfrak{L}$ .

## § 12.

### Imperfect fields: Smallest containing and greatest contained perfect field. — Root fields.

If  $\mathfrak{K}$  is a field of characteristic  $p$  and  $a$  and  $b$  are elements of  $\mathfrak{K}$ , then the following equations hold:<sup>E 80</sup>

$$(1.) \quad \begin{cases} a^p + b^p = (a + b)^p, & a^p - b^p = (a - b)^p, \\ a^p \cdot b^p = (a \cdot b)^p, & a^p : b^p = (a : b)^p. \end{cases}$$

From these equations we read off the following result:

1. The  $p$ -th powers of all elements of a field  $\mathfrak{K}$  of characteristic  $p$  form a field  $\mathfrak{K}^p$ . If the field  $\mathfrak{K}$  is perfect, then  $\mathfrak{K}^p$  is identical with  $\mathfrak{K}$ , otherwise only a part of  $\mathfrak{K}$  (§ 11, 2.).

Assigning to each element of  $\mathfrak{K}$  its  $p$ -th power gives an isomorphic correspondence between  $\mathfrak{K}$  and  $\mathfrak{K}^p$ .

Since the isomorphic correspondence between  $\mathfrak{K}$  and  $\mathfrak{K}^p$  is one-to-one,  $\mathfrak{K}^p = \mathfrak{K}$  must hold if  $\mathfrak{K}$  has only finitely many elements.<sup>E 81</sup> Thus:

2. *Every field that has only finitely many elements is perfect.*

Starting from a field  $\mathfrak{K}$  of characteristic  $p$ , we form the infinite sequence of fields

$$\mathfrak{K} = \mathfrak{K}^{p^0}, \mathfrak{K}^p, \mathfrak{K}^{p^2}, \dots, \mathfrak{K}^{p^f}, \dots,$$

in which in general  $\mathfrak{K}^{p^f}$  denotes the field that consists of the  $p$ -th powers of the elements of  $\mathfrak{K}^{p^{f-1}}$ , hence of the  $p^f$ -th powers of the elements of  $\mathfrak{K}$ . All these fields are isomorphic, therefore either all perfect or all imperfect; in the first case  $\mathfrak{K} = \mathfrak{K}^p = \mathfrak{K}^{p^2} = \dots$ , in the second, which alone interests us here, each following field is only a part of the preceding one. We can also continue this sequence in the opposite direction. To do this, we must first extend the field  $\mathfrak{K}$  to a field  $\mathfrak{K}^{p^{-1}}$  such that  $\mathfrak{K}$  consists of the  $p$ -th powers of all elements of  $\mathfrak{K}^{p^{-1}}$ . To this end we remark first that every element of  $\mathfrak{K}$  can be written in the form  $\sqrt[p]{a}$ , where  $a$  is an element of  $\mathfrak{K}$ . Now if  $\sqrt[p]{a}$  and  $\sqrt[p]{b}$  are any two elements of  $\mathfrak{K}$ , then, as one sees at once from (1.):

- 1)  $\sqrt[p]{a}$  is equal to  $\sqrt[p]{b}$  if and only if  $a = b$ ,
- 2)  $\sqrt[p]{a} + \sqrt[p]{b} = \sqrt[p]{a+b}$ ,
- 3)  $\sqrt[p]{a} \cdot \sqrt[p]{b} = \sqrt[p]{a \cdot b}$ .

We now form a system  $\mathfrak{K}^{p^{-1}}$  by adding to  $\mathfrak{K}$  all symbols of the form  $\sqrt[p]{a}$  in which  $a$  denotes an element belonging to  $\mathfrak{K}$  but not to  $\mathfrak{K}^p$ , without, however, for the present giving such a symbol the meaning of a  $p$ -th root of  $a$ . We stipulate further that the statements made under 1), 2), 3) shall hold for equality, sum and product also when the elements  $a, b$  of  $\mathfrak{K}$  do not belong to  $\mathfrak{K}^p$ , or when one of these elements does not belong to  $\mathfrak{K}^p$ . By this we have made  $\mathfrak{K}^{p^{-1}}$  into a system with double composition. But from 1), 2), 3) it follows further that we obtain an isomorphic correspondence between  $\mathfrak{K}$  and  $\mathfrak{K}^{p^{-1}}$  if we assign to each element  $a$  of  $\mathfrak{K}$  the element  $\sqrt[p]{a}$  of  $\mathfrak{K}^{p^{-1}}$ ; consequently  $\mathfrak{K}^{p^{-1}}$ , like  $\mathfrak{K}$ , is a field. If we now apply the rules of calculation valid in every field, we obtain, with reference to 3):

$$(\sqrt[p]{a})^p = \sqrt[p]{a^p}.$$

But since the element  $a^p$  belongs to  $\mathfrak{K}^p$ ,  $\sqrt[p]{a^p}$  already has the meaning of a  $p$ -th root of  $a^p$ , and so  $\sqrt[p]{a^p} = a$ , therefore

$$(\sqrt[p]{a})^p = a,$$

whereby the meaning of  $\sqrt[p]{a}$  as a  $p$ -th root of  $a$  is established in general, and at the same time that  $\mathfrak{K}$  consists of the  $p$ -th powers of the elements of  $\mathfrak{K}^{p^{-1}}$ .<sup>E 82</sup> If we apply repeatedly the step that led us from  $\mathfrak{K}$  to  $\mathfrak{K}^{p^{-1}}$ , we obtain a sequence of fields  $\mathfrak{K}^{p^{-1}}, \mathfrak{K}^{p^{-2}}, \dots$ , and thus  $\mathfrak{K}^{p^n}$  is defined for every integral  $n$ .

3. *All the elements that occur in the fields  $\mathfrak{K}^{p^n}$  belonging to a field  $\mathfrak{K}$  of characteristic  $p$  form a field  $\mathfrak{C}$ ; likewise the fields  $\mathfrak{K}^{p^n}$  have as intersection a field  $\mathfrak{D}$ . Both fields  $\mathfrak{C}$  and  $\mathfrak{D}$  are perfect, and indeed  $\mathfrak{D}$  represents the greatest perfect field contained in  $\mathfrak{K}$ , while  $\mathfrak{C}$  proves to be a smallest perfect extension field of  $\mathfrak{K}$ .*

For since, of any two of the fields  $\mathfrak{K}^{p^n}$  ( $n \leq 0$ ), one is always contained in the other,<sup>E 83</sup> the totality of all elements occurring in these fields yields a field (§ 2, 2.). If  $a$  is an element of

this field  $\mathfrak{C}$  and  $a$  occurs, say, in  $\mathfrak{K}^{p^n}$ , then a  $p$ -th root of  $a$  exists in  $\mathfrak{K}^{p^{n-1}}$ , and consequently in  $\mathfrak{C}$ . The field  $\mathfrak{C}$  is therefore perfect. If we call it a *smallest* perfect extension field of  $\mathfrak{K}$ , this is to mean that no field between  $\mathfrak{K}$  and  $\mathfrak{C}$  other than  $\mathfrak{C}$  itself is perfect. For if  $\mathfrak{C}'$  is a field between  $\mathfrak{K}$  and  $\mathfrak{C}$ ,  $a$  an element of  $\mathfrak{C}$  not contained in  $\mathfrak{C}'$ ,  $n$  the smallest natural number such that  $a$  occurs in  $\mathfrak{K}^{p^n}$ , then  $a^{p^n}$  is an element of  $\mathfrak{K}$ , hence also of  $\mathfrak{C}'$ . Now if  $a^{p^m}$  is the first among the elements  $a^p, a^{p^2}, a^{p^3}, \dots$  that is contained in  $\mathfrak{C}'$ , then  $a^{p^m}$  has no  $p$ -th root in  $\mathfrak{C}'$ ; the field  $\mathfrak{C}'$  is therefore imperfect. — If further  $a$  is an element of the intersection field  $\mathfrak{D}$ ,  $n$  an arbitrary integer, then  $a$  occurs in  $\mathfrak{K}^{p^{n+1}}$ , therefore  $\sqrt[p]{a}$  in  $\mathfrak{K}^{p^n}$ , i.e. in every field of the sequence  $\mathfrak{K}^{p^n}$ , and consequently in  $\mathfrak{D}$ . The field  $\mathfrak{D}$  is therefore perfect. If finally  $\mathfrak{D}'$  is any perfect field contained in  $\mathfrak{K}$ ,  $a$  an arbitrary element of  $\mathfrak{D}'$ ,  $n$  an arbitrarily large natural number, then  $a$  has a  $p^n$ -th root  $b$  in  $\mathfrak{D}'$ . Then  $b$  belongs to  $\mathfrak{K}$ , and consequently  $a = b^{p^n}$  to  $\mathfrak{K}^{p^n}$ , i.e. to all fields of our sequence, hence to  $\mathfrak{D}$ .  $\mathfrak{D}'$  is therefore contained in  $\mathfrak{D}$ , and  $\mathfrak{D}$  is the greatest perfect field contained in  $\mathfrak{K}$ .

Let  $\mathfrak{K}$  be an arbitrary field of characteristic  $p$ ,  $a$  an element of  $\mathfrak{K}$ . This element determines a sequence of elements

$$a, a^p, a^{p^2}, \dots,$$

in which each element is the  $p$ -th root of the following one. If a  $p$ -th root of  $a$  exists in  $\mathfrak{K}$ , we can continue this sequence in the opposite direction without extending the field. Either there exists for every natural number  $n$ , however large, a  $p^n$ -th root of  $a$ , which we denote by  $a^{p^{-n}}$ , or there is a greatest number  $n$  such that  $a^{p^{-n}}$  still exists but no longer has a  $p$ -th root. In the first case we obtain a sequence of elements extending to infinity in two directions, in the second it has an initial element. The perfect fields are characterized by having only sequences of the first kind. The elements of a sequence  $a^{p^n}$  are either all different from one another, or they repeat periodically, in which case the sequence is of course of the first kind. Here the following simple theorem holds:

4. *The sequence of elements  $a^{p^n}$  determined by an element  $a$  of a field  $\mathfrak{K}$  of characteristic  $p$  is periodic if and only if the element  $a$  is absolutely algebraic. The number of elements of the period is equal to the absolute degree (=degree with respect to the prime field) of  $a$ , and the elements of the period are all the roots of one and the same irreducible equation in the prime field  $\mathfrak{P}_p$ .*

For if the sequence of elements belonging to  $a$  is periodic and consists of  $n$  different elements, then each element is equal to its  $p^n$ -th power, hence a solution of the equation  $x^{p^n} - x = 0$ , whose coefficients belong to the prime field  $\mathfrak{P}_p$  contained in  $\mathfrak{K}$ , and consequently absolutely algebraic. If conversely  $a$  is an absolutely algebraic element of  $\mathfrak{K}$  and

$$(2.) \quad \varphi(x) = x^m + a_1 x^{m-1} + \dots + a_m = 0$$

the irreducible equation of the prime field that is satisfied by  $a$ , then

$$a^m + a_1 a^{m-1} + \dots + a_m = 0.$$

If we raise this equation to the  $p$ -th power and take into account that every element of the prime field is equal to its  $p$ -th power, we obtain

$$a^{pm} + a_1 a^{p(m-1)} + \dots + a_m = 0,$$

i.e. the equation (2.) is also satisfied by  $a^p$ . In the same way we recognize that the elements  $a^{p^2}, a^{p^3}, \dots$  must be solutions of the equation (2.), so that there are at most  $m$  different ones among them. Let us assume that there are  $n$  different ones, hence that  $a, a^p, a^{p^2}, \dots, a^{p^{n-1}}$  are different, while  $a^{p^n} = a$  holds; then  $\varphi(x)$  is divisible by

$$(3.) \quad (x - a)(x - a^p) \cdots (x - a^{p^{n-1}}) = x^n + b_1 x^{n-1} + \cdots + b_n = \psi(x)$$

If we raise to the  $p$ -th power and then replace  $x^p$  by  $x$  (which is permissible because  $x^p$  is transcendental with respect to  $\mathfrak{K}$ ), the factors of the left side of (3.) undergo only a cyclic permutation. We therefore obtain

$$\psi(x) = x^n + b_1^p x^{n-1} + \cdots + b_n^p$$

and thus  $b_1^p = b_1, \dots, b_n^p = b_n$ . Now the equation  $x^p = x$  is satisfied by the  $p$  elements of the prime field, and since it cannot have more than  $p$  solutions, it follows that the coefficients of  $\psi(x)$  belong to the prime field. But since  $\varphi(x)$  is divisible by  $\psi(x)$  and irreducible in the prime field,  $\varphi(x) = \psi(x)$  must hold. This completely proves Theorem 4.

If the field  $\mathfrak{K}$  is absolutely algebraic, then every element of  $\mathfrak{K}$  belongs to a periodic sequence and therefore has a  $p$ -th root. We thus obtain the following theorem, of which 2. is a special case:

5. *Every absolutely algebraic field is perfect.*

*Root elements and root fields.* — If  $\mathfrak{K}$  is a field of characteristic  $p$ ,  $\mathfrak{L}$  an extension of  $\mathfrak{K}$ , then an element  $a$  of  $\mathfrak{L}$  shall be called a *root element with respect to  $\mathfrak{K}$*  if for sufficiently large  $n$   $a^{p^n}$  belongs to  $\mathfrak{K}$ .<sup>E 84</sup> In that case we call the smallest number  $n \geq 0$  for which  $a^{p^n}$  becomes an element of  $\mathfrak{K}$  the *exponent of  $a$  with respect to  $\mathfrak{K}$* . If this is equal to  $f$ , then, as is easy to see (see p. 37),  $x^{p^f} - a^{p^f} = 0$  is the irreducible equation in  $\mathfrak{K}$  that is satisfied by  $a$ . We call the field  $\mathfrak{L}$  a *root field with respect to  $\mathfrak{K}$*  if all its elements are root elements. Among the root elements are all elements of  $\mathfrak{K}$  itself; they are characterized by the exponent 0. If  $a$  and  $b$  are root elements and their exponents do not exceed the natural number  $f$ , then  $a^{p^f}, b^{p^f}$  are elements of  $\mathfrak{K}$ , and the same therefore holds for  $(a \pm b)^{p^f} = a^{p^f} \pm b^{p^f}$  as well as for  $(a \cdot b)^{p^f}$  and  $(\frac{a}{b})^{p^f}$ . The elements  $a \pm b, a \cdot b, \frac{a}{b}$  are therefore also root elements, and their exponents are  $\leq f$ . Therefore those root elements contained in  $\mathfrak{L}$  whose exponent does not exceed the number  $f$  form a field between  $\mathfrak{K}$  and  $\mathfrak{L}$ , and the same holds for the totality of all root elements contained in  $\mathfrak{L}$ , as follows at once from this. It further follows that an extension  $\mathfrak{L}$  that arises by adjoining a (finite or infinite) system  $\mathfrak{S}$  of root elements represents a root field. For, since it contains  $\mathfrak{K}$  and the system  $\mathfrak{S}$ , the field formed by the root elements is identical with the field  $\mathfrak{K}(\mathfrak{S}) = \mathfrak{L}$ . — From the definitions given it follows further at once that, if the field  $\mathfrak{L}$  lies between  $\mathfrak{K}$  and  $\mathfrak{M}$ , and  $\mathfrak{L}$  is a root field with respect to  $\mathfrak{K}$  while  $\mathfrak{M}$  is a root field with respect to  $\mathfrak{L}$ , then  $\mathfrak{M}$  also represents a root field with respect to  $\mathfrak{K}$ . — Let us now assume that the extension field  $\mathfrak{L}$  itself, or more generally any field  $\mathfrak{T}$  between  $\mathfrak{K}$  and  $\mathfrak{L}$ , is perfect,<sup>E 85</sup> and let us denote by  $\mathfrak{C}$  the field of all root elements contained in  $\mathfrak{L}$  (with respect to  $\mathfrak{K}$ ). If then  $a$  is an element of  $\mathfrak{C}$ ,  $f$  its exponent, then  $a^{p^f}$  belongs to  $\mathfrak{K}$ , hence also to  $\mathfrak{T}$ . But  $a$  itself must already belong to  $\mathfrak{T}$ ; for otherwise, if we denoted by  $n$  the smallest number for which  $a^{p^n}$  belongs to  $\mathfrak{T}$ , then  $a^{p^n}$  would have no  $p$ -th root within  $\mathfrak{T}$ , although  $\mathfrak{T}$  was supposed to be a perfect field. Thus  $a$  belongs to  $\mathfrak{T}$ , and so the field  $\mathfrak{C}$  is contained

in  $\mathfrak{T}$ . On the other hand  $\mathfrak{C}$  is itself a perfect field. For if  $a$  again denotes an element of  $\mathfrak{C}$  and  $f$  its exponent, then  $a$ , as an element of  $\mathfrak{T}$ , has a  $p$ -th root  $\sqrt[p]{a} = b$  within this perfect field, and  $b^{p^{f+1}} = a^{p^f}$  becomes an element of  $\mathfrak{K}$ . The element  $\sqrt[p]{a}$  is therefore a root element, and consequently belongs to  $\mathfrak{C}$ . Thus every extension field  $\mathfrak{L}$  of  $\mathfrak{K}$ , if it is perfect, contains a *smallest* field of this kind, and this is formed by all the root elements contained in  $\mathfrak{L}$ . — Now let  $\mathfrak{C}$  be a smallest perfect extension field of  $\mathfrak{K}$  (hence a root field), and let  $\mathfrak{K}_f$  ( $f \geq 0$ ) denote the field of those elements of  $\mathfrak{C}$  whose exponent is  $\leq f$ . Then  $\mathfrak{K}_0 = \mathfrak{K}$ . If  $a$  is an element of  $\mathfrak{K}_f$ , then the exponent of  $\sqrt[p]{a}$  cannot be  $> f + 1$ , i.e.  $\sqrt[p]{a}$  belongs to  $\mathfrak{K}_{f+1}$ ; if  $\sqrt[p]{a}$  belongs to  $\mathfrak{K}_{f+1}$ , we can conclude conversely that  $a$  is an element of  $\mathfrak{K}_f$ . Thus  $\mathfrak{K}_{f+1}^p = \mathfrak{K}_f$ . If  $\overline{\mathfrak{K}}$  denotes a field of the same type as  $\mathfrak{K}$ ,  $\pi_0$  an isomorphic correspondence between  $\mathfrak{K}$  and  $\overline{\mathfrak{K}}$ ,  $\overline{\mathfrak{C}}$  a smallest perfect extension field of  $\overline{\mathfrak{K}}$ ,  $\overline{\mathfrak{K}}_f$  the field of those elements of  $\overline{\mathfrak{C}}$  whose exponent with respect to  $\overline{\mathfrak{K}}$  is  $\leq f$ , then we have on the one hand between  $\mathfrak{K}_1$  and  $\mathfrak{K} = \mathfrak{K}_0$ , on the other hand between  $\overline{\mathfrak{K}}_1$  and  $\overline{\mathfrak{K}}_0$ , an isomorphic correspondence if we assign to each element of  $\mathfrak{K}_1$  or  $\overline{\mathfrak{K}}_1$  respectively its  $p$ -th power. Combining these two isomorphisms with  $\pi_0$  yields an isomorphic correspondence  $\pi_1$  between  $\mathfrak{K}_1$  and  $\overline{\mathfrak{K}}_1$  that comprises  $\pi_0$ . In the same way we arrive at a correspondence  $\pi_2$  between  $\mathfrak{K}_2$  and  $\overline{\mathfrak{K}}_2$  that comprises  $\pi_1$ , etc. The totality of these isomorphisms  $\pi_0, \pi_1, \pi_2, \dots$  establishes an isomorphism between  $\mathfrak{C}$  and  $\overline{\mathfrak{C}}$ . Here we can again let  $\mathfrak{K}$  coincide with  $\overline{\mathfrak{K}}$  and presuppose that  $\pi_0$  relates every element of  $\mathfrak{K}$  to itself. Then we obtain:

6. *Every imperfect field can be extended in essentially only one way to a smallest possible perfect field; and thus every imperfect type is assigned a definite perfect one.*

### § 13.

#### Imperfect fields: Algebraic extensions of the first kind.

Let  $\mathfrak{K}$  be an arbitrary field.<sup>E 86</sup> An irreducible function in  $\mathfrak{K}$  shall be called *of the first kind*<sup>14</sup> if it has only simple zeros. An element  $\gamma$  algebraic with respect to  $\mathfrak{K}$  shall be called of the first kind if the function irreducible in  $\mathfrak{K}$  that has the zero  $\gamma$  is of the first kind. An algebraic extension shall be called of the first kind if all elements of the extension field are of the first kind.

For perfect fields, thus in particular for all fields of characteristic 0, there are only functions, algebraic elements and algebraic extensions of the first kind.

Let the field  $\mathfrak{K}$  have the characteristic  $p$ , and let  $g(x)$  be an irreducible function in  $\mathfrak{K}$ . We can then determine a non-negative integer  $f$  such that  $g(x)$  is an integral rational function of  $x^{p^f}$ , but no longer of  $x^{p^{f+1}}$ .  $g(x)$  then has the form

$$g(x) = x^{np^f} + a_1 x^{(n-1)p^f} + \dots + a_n,$$

and at least one term whose exponent is not divisible by  $p^{f+1}$  actually occurs. We call the number  $n$  the *reduced degree*,  $f$  (in generalization of a designation introduced in the preceding section) the *exponent* of the irreducible function  $g(x)$ , and we transfer this designation also to the zeros of the function<sup>\*</sup>).

<sup>\*</sup>) The designation “reduced degree” is justified by the fact that, as can easily be shown by means of the following theorems, the reduced degree of an element with respect to  $\mathfrak{K}$  is equal to the degree that the element has with respect to the smallest perfect field containing  $\mathfrak{K}$ .

<sup>14</sup> In modern terms: *separable*. — Trans.

Two special cases are particularly noteworthy. For, first, if the reduced degree has its smallest value 1, then  $g(x)$  takes the form  $x^{p^f} - \alpha$  and has nothing but equal zeros; the algebraic elements of reduced degree 1 are thus the root elements considered in the preceding section. Second, if the exponent  $f$  has its smallest value 0, then  $g(x)$  is no longer an integral rational function of  $x^p$ , the derivative  $g'(x)$  does not vanish, hence can have no common factor with  $g(x)$ , consequently the function  $g(x)$  has nothing but simple zeros; it is of the first kind. On the other hand, in the case  $f > 0$   $g(x)$  is the  $p$ -th power of another integral function, hence has only multiple zeros<sup>E87</sup>. In this section we shall be concerned chiefly with the case  $f = 0$ .

We now prove a series of theorems that refer to a field  $\mathfrak{K}$  of characteristic  $p$ ; some of these theorems are of significance only if  $\mathfrak{K}$  is imperfect.

1. *If  $\gamma$  is an element algebraic with respect to  $\mathfrak{K}$ , of exponent  $f$ ,  $f > 0$ , then  $\gamma^p$  is of exponent  $f - 1$  with respect to  $\mathfrak{K}$ , and  $[\mathfrak{K}(\gamma) : \mathfrak{K}(\gamma^p)] = p$ .*

For if  $\gamma$  is a zero of the irreducible function

$$(1.) \quad g(x) = x^{np^f} + a_1 x^{(n-1)p^f} + \cdots + a_n$$

then  $\gamma^p$  is a zero of

$$h(x) = x^{np^{f-1}} + a_1 x^{(n-1)p^{f-1}} + \cdots + a_n.$$

$h(x)$  is irreducible in  $\mathfrak{K}$ , because from  $h(x) = \varphi(x) \cdot \psi(x)$  there would follow

$$g(x) = h(x^p) = \varphi(x^p) \cdot \psi(x^p),$$

whereas  $g(x)$  is irreducible. Consequently  $f - 1$  is the exponent of  $\gamma^p$ , and since  $[\gamma : \mathfrak{K}] = n \cdot p^f$ ,  $[\gamma^p : \mathfrak{K}] = np^{f-1}$ , it follows that  $[\mathfrak{K}(\gamma) : \mathfrak{K}(\gamma^p)] = p$ .

2. *If*

$$(2.) \quad \varphi(x) = x^n + a_1 x^{n-1} + \cdots + a_n$$

*is an irreducible function of the first kind in  $\mathfrak{K}$ , then*

$$(3.) \quad \psi(x) = x^n + a_1^p x^{n-1} + \cdots + a_n^p$$

*(more generally  $x^n + a_1^{p^f} x^{n-1} + \cdots + a_n^{p^f}$ ) is also irreducible and of the first kind.*

Proof: If  $h(x)$  denotes a factor of  $\psi(x)$  belonging to  $\mathfrak{K}$  whose degree is greater than 0, then  $h(x^p)$  is a factor of  $\psi(x^p) = (\varphi(x))^p$ , hence, because  $\varphi(x)$  is irreducible, a power of  $\varphi(x)$ . We thus obtain:

$$(4.) \quad h(x^p) = (\varphi(x))^r \quad (0 < r \leq p).$$

Now, however, by hypothesis  $\varphi(x)$  has only simple zeros,  $(\varphi(x))^r$  therefore only  $r$ -fold zeros; and since  $h(x^p)$  is the  $p$ -th power of an integral function (of an extension field), hence has every zero at least  $p$ -fold, it follows from (4.) that  $r = p$ ,

$$h(x^p) = (\varphi(x))^p = \psi(x^p),$$

consequently

$$h(x) = \psi(x)$$

holds.  $\psi(x)$  is therefore irreducible. Since  $\varphi(x)$  actually contains at least *one* power of  $x$  whose exponent is not divisible by  $p$ , the same follows from (2.), (3.) for  $\psi(x)$ .  $\psi(x)$  is therefore of the first kind.

3. *If*

$$(2.) \quad \varphi(x) = x^n + a_1 x^{n-1} + \cdots + a_n$$

*is an irreducible function of the first kind in  $\mathfrak{K}$ ,  $\mathfrak{L}$  an extension field of  $\mathfrak{K}$  that contains the  $p$ -th roots of the coefficients of  $\varphi(x)$  and a zero  $\gamma$  of  $\varphi(x)$ , then  $\mathfrak{L}$  also contains the  $p$ -th root of  $\gamma$ .*

Proof: By hypothesis  $\mathfrak{L}$  contains the two functions

$$\chi(x) = x^n + \sqrt[p]{a_1} x^{n-1} + \cdots + \sqrt[p]{a_n}, \quad x^p - \gamma = (x - \sqrt[p]{\gamma})^p,$$

hence also their greatest common divisor  $t(x)$ . Since  $\gamma$  is a zero of  $\varphi(x)$ ,  $\sqrt[p]{\gamma}$  is a zero of  $\varphi(x^p) = (\chi(x))^p$ , hence a zero of  $\chi(x)$ , and indeed a simple zero, because the zeros of  $\chi(x)$  are the  $p$ -th roots of the zeros of  $\varphi(x)$ , and hence, like these, different from one another. Since  $\sqrt[p]{\gamma}$  is the only zero of  $x^p - \gamma$ , it follows that  $t(x) = x - \sqrt[p]{\gamma}$ , and consequently  $\sqrt[p]{\gamma}$  is an element of  $\mathfrak{L}$ .

4. *Every algebraic extension of a perfect field is a perfect field.*

Proof: <sup>E 88</sup> Let  $\mathfrak{K}$  be a perfect field of characteristic  $p$  — for in the case of characteristic 0 the theorem is self-evident —,  $\mathfrak{L}$  an algebraic extension of  $\mathfrak{K}$ ,  $\gamma$  an element from  $\mathfrak{L}$ , and  $\varphi(x)$  the irreducible function from  $\mathfrak{K}$  with the zero  $\gamma$ . Since  $\mathfrak{K}$  is perfect,  $\varphi(x)$  is of the first kind, and for the same reason  $\mathfrak{K}(\gamma)$ , like  $\mathfrak{K}$  already, contains the  $p$ -th roots of the coefficients of  $\varphi(x)$ , but besides this also  $\gamma$ , hence by 3. also  $\sqrt[p]{\gamma}$ . Since  $\mathfrak{K}(\gamma)$  is a subfield of  $\mathfrak{L}$ , the  $p$ -th root of every element  $\gamma$  of  $\mathfrak{L}$  is thus contained in  $\mathfrak{L}$ , hence  $\mathfrak{L}$  is a perfect field. — The hypothesis of Theorem 4. is satisfied if  $\mathfrak{K}$  is a prime field, so that  $\mathfrak{L}$  is an absolutely algebraic field, whereby the theorem of § 12, 5. is proved again.

5. *If  $\gamma$  is algebraic with respect to  $\mathfrak{K}$  and of the first kind, then  $\mathfrak{K}(\gamma^p) = \mathfrak{K}(\gamma)$ .* <sup>E 89</sup>

For if  $\gamma$  is a zero of the irreducible function  $\varphi(x) = x^n + a_1 x^{n-1} + \cdots + a_n$  in  $\mathfrak{K}$ , then  $\gamma^p$  is a zero of the function  $\psi(x) = x^n + a_1^p x^{n-1} + \cdots + a_n^p$ , which by 2. is likewise irreducible. Therefore  $n = [\gamma : \mathfrak{K}] = [\gamma^p : \mathfrak{K}]$ , from which the assertion follows. — Conversely, that  $\gamma$  is of the first kind whenever  $\mathfrak{K}(\gamma^p) = \mathfrak{K}(\gamma)$  is already stated by Theorem 1.

6. *If the element  $\gamma$  is algebraic with respect to  $\mathfrak{K}$  and of the first kind, then  $\mathfrak{K}(\gamma)$  is an algebraic extension of the first kind.*

Proof: Let  $\alpha$  be an arbitrary element of  $\mathfrak{K}(\gamma)$ ; if we then put

$$(5.) \quad \begin{cases} [\mathfrak{K}(\alpha) : \mathfrak{K}] = m_1, & [\mathfrak{K}(\gamma) : \mathfrak{K}(\alpha)] = m_2, \\ [\mathfrak{K}(\alpha^p) : \mathfrak{K}] = n_1, & [\mathfrak{K}(\gamma) : \mathfrak{K}(\alpha^p)] = n_2, \end{cases}$$

then

$$(6.) \quad m_1 \cdot m_2 = n_1 \cdot n_2 = [\mathfrak{K}(\gamma) : \mathfrak{K}],$$

and, because  $\mathfrak{K}(\alpha^p)$  is a subfield of  $\mathfrak{K}(\alpha)$ ,

$$(7.) \quad m_1 \geq n_1, \quad m_2 \leq n_2.$$

If now  $\chi(x) = x^{m_2} + b_1x^{m_2-1} + \cdots + b_{m_2}$  is the irreducible function of the field  $\mathfrak{K}(\alpha)$  that has  $\gamma$  as a zero, then  $\gamma^p$  is a zero of  $x^{m_2} + b_1^p x^{m_2-1} + \cdots + b_{m_2}^p$ , and the coefficients of this function belong, as is easy to see, to the field  $\mathfrak{K}(\alpha^p)$ . Hence

$$n_2 = [\mathfrak{K}(\gamma) : \mathfrak{K}(\alpha^p)] = [\mathfrak{K}(\gamma^p) : \mathfrak{K}(\alpha^p)] \leq m_2,$$

hence on account of (7.), (6.)  $m_2 = n_2$ ,  $m_1 = n_1$ . The elements  $\alpha$  and  $\alpha^p$  are therefore of the same degree with respect to  $\mathfrak{K}$ . Therefore  $\mathfrak{K}(\alpha^p) = \mathfrak{K}(\alpha)$ , hence  $\alpha$  is an element of the first kind, q.e.d.

7. *Every finite extension of the first kind is simple.* <sup>E 90</sup>

For if  $\mathfrak{L}$  is a finite extension of the first kind of  $\mathfrak{K}$ , then we can put  $\mathfrak{L} = \mathfrak{K}(\mathfrak{S})$ , where  $\mathfrak{S}$  contains only finitely many elements (§ 7, 6.), and since these are all of the first kind,  $\mathfrak{L}$  is simple with respect to  $\mathfrak{K}$  by § 11, 4.

8. *A field  $\mathfrak{K}(\mathfrak{S})$  that arises from  $\mathfrak{K}$  by adjunction of a system  $\mathfrak{S}$  of algebraic elements of the first kind is an extension of the first kind.*

For if  $\mathfrak{S}$  is a finite system, this follows from § 11, 4. and Theorem 6. of this section; but if  $\mathfrak{S}$  is infinite, the same follows with the addition of § 2, 3.

9. *If the field  $\mathfrak{L}$  lies between  $\mathfrak{K}$  and  $\mathfrak{M}$  and if  $\mathfrak{L}$  is of the first kind with respect to  $\mathfrak{K}$ ,  $\mathfrak{M}$  with respect to  $\mathfrak{L}$ , then  $\mathfrak{M}$  is of the first kind with respect to  $\mathfrak{K}$ .*

Proof: Let  $\delta$  be an arbitrary element of  $\mathfrak{M}$ . By § 7, 9.  $\delta$  is algebraic with respect to  $\mathfrak{K}$ . To prove 9., we have only to show that  $\delta$  is of the first kind, hence of exponent 0 with respect to  $\mathfrak{K}$ . If we first denote the exponent in question by  $f$ , then by 1.  $\delta^{p^f}$  is of exponent 0 with respect to  $\mathfrak{K}$ . With respect to  $\mathfrak{L}$ ,  $\delta$  is by hypothesis of the first kind, from which by 5.  $\mathfrak{L}(\delta) = \mathfrak{L}(\delta^p) = \mathfrak{L}(\delta^{p^2}) = \cdots$ , hence  $\mathfrak{L}(\delta) = \mathfrak{L}(\delta^{p^f})$  follows. The field  $\mathfrak{L}(\delta^{p^f})$  is obtained from  $\mathfrak{K}$  by adjoining all elements of  $\mathfrak{L}$  as well as  $\delta^{p^f}$ . But since these elements are all of the first kind with respect to  $\mathfrak{K}$ , by Theorem 8. the same holds for all elements of the field  $\mathfrak{L}(\delta^{p^f}) = \mathfrak{L}(\delta)$ , hence also for  $\delta$ , q.e.d.

Let  $\mathfrak{K}$  be an arbitrary field,  $\mathfrak{L}$  a finite extension of the first kind of  $\mathfrak{K}$ . Then the extension is simple, and any primitive element  $\alpha$  of  $\mathfrak{L}$  is a zero of a function  $\varphi(x)$  that is irreducible in  $\mathfrak{K}$  and of the first kind. It may be that  $\varphi(x)$  already breaks up completely in  $\mathfrak{L}$ ; then we put  $\mathfrak{L} = \mathfrak{N}$ . Otherwise we denote by  $\mathfrak{N}$  an extension of  $\mathfrak{L}$  that just suffices to decompose  $\varphi(x)$  completely. Then  $\mathfrak{N}$  arises from  $\mathfrak{L}$ , and, since  $\mathfrak{L} = \mathfrak{K}(\alpha)$ , also from  $\mathfrak{K}$  alone by adjunction of zeros of the function  $\varphi(x)$ , is therefore a finite extension of the first kind of  $\mathfrak{K}$  and moreover normal with respect to  $\mathfrak{K}$  (§ 8, 6.). If therefore  $j_1$  is a primitive element of  $\mathfrak{N}$  (with respect to  $\mathfrak{K}$ ) and  $g(x)$  the irreducible function from  $\mathfrak{K}$  with the zero  $j_1$ , then in  $\mathfrak{N}$  we have a decomposition

$$g(x) = (x - j_1) \cdot (x - j_2) \cdots (x - j_n).$$

Here the elements  $j_1, j_2, \dots, j_n$  are different from one another, and

$$\mathfrak{N} = \mathfrak{K}(j_1) = \mathfrak{K}(j_2) = \cdots = \mathfrak{K}(j_n); \quad [\mathfrak{N} : \mathfrak{K}] = n.$$

Since  $j_1, j_2, \dots, j_n$  are zeros of the same irreducible function from  $\mathfrak{K}$ , one obtains an isomorphic correspondence  $\pi_k$  ( $k = 1, \dots, n$ ) of  $\mathfrak{N}$  with respect to itself, in which every element of  $\mathfrak{K}$  remains unchanged, if in every element of  $\mathfrak{N}$  that one imagines written in the form

$$(8.) \quad c_0 + c_1 j_1 + \cdots + c_{n-1} j_1^{n-1}$$

with coefficients from  $\mathfrak{K}$ , one replaces  $j_1$  by  $j_k$  (§ 6). Let the system of these  $n$  isomorphisms (the *Galois* group) be denoted by  $\mathfrak{G}$ .<sup>E91</sup> Now let  $\mathfrak{M}$  be any field between  $\mathfrak{K}$  and  $\mathfrak{N}$ ,  $[\mathfrak{M} : \mathfrak{K}] = m$ ,  $\beta = \psi(j_1)$  a primitive element of  $\mathfrak{M}$ , represented in the form (8.), and  $h(x)$  the irreducible function from  $\mathfrak{K}$  with the zero  $\beta$ . Since the isomorphisms  $\pi_k$  leave the element 0 unchanged and carry  $\beta = \psi(j_1)$  into  $\psi(j_k)$ , it follows from  $0 = h(\beta) = h(\psi(j_1))$  that also  $h(\psi(j_k)) = 0$ . The function

$$f(x) = (x - \psi(j_1)) \cdot (x - \psi(j_2)) \cdots (x - \psi(j_n))$$

belongs to the field  $\mathfrak{K}$ , since its coefficients are symmetric in the zeros  $j_k$  of  $g(x)$ , and its zeros are, by what precedes, all zeros of the irreducible function  $h(x)$ . Therefore  $f(x)$  can have in  $\mathfrak{K}$  no irreducible factor except  $h(x)$ , and, in view of the degrees of  $f(x)$  and  $h(x)$ ,

$$f(x) = h(x)^{\frac{n}{m}}.$$

Hence among the elements  $\psi(j_k)$  exactly  $\frac{n}{m}$  are equal to  $\beta = \psi(j_1)$ ; there are thus among the isomorphisms  $\pi_k$  exactly  $\frac{n}{m}$  that leave the element  $\beta$ , and consequently every element of  $\mathfrak{K}(\beta) = \mathfrak{M}$ , unchanged. Let  $\mathfrak{H}$  be the system of these  $\frac{n}{m}$  isomorphisms. — If  $\mathfrak{M}'$  is a second field between  $\mathfrak{K}$  and  $\mathfrak{N}$ , then to  $\mathfrak{M}'$  there belongs a system  $\mathfrak{H}'$ , consisting of all those isomorphisms  $\pi_k$  that leave all elements of  $\mathfrak{M}'$  unchanged. Let us assume that  $\mathfrak{H}'$  is identical with  $\mathfrak{H}$ . If then  $\delta$  is an element of  $\mathfrak{M}'$ , the isomorphisms belonging to  $\mathfrak{H}$  leave all elements of  $\mathfrak{M}$  as well as  $\delta$ , hence also all elements of the field  $\mathfrak{M}(\delta)$ , unchanged. If we put

$$[\mathfrak{M}(\delta) : \mathfrak{M}] = \mu$$

then  $[\mathfrak{M}(\delta) : \mathfrak{K}] = m \cdot \mu$ . By what precedes, therefore, the number of isomorphisms  $\pi_k$  that leave all elements of  $\mathfrak{M}(\delta)$  unchanged is equal to  $\frac{n}{m \cdot \mu}$ , and since all  $\frac{n}{m}$  isomorphisms from  $\mathfrak{H}$  belong to them, it must be that  $\mu = 1$ ,  $\mathfrak{M}(\delta) = \mathfrak{M}$ , hence  $\delta$  is an element of  $\mathfrak{M}$ . Since  $\delta$  denoted an arbitrary element of  $\mathfrak{M}'$ ,  $\mathfrak{M}'$  is accordingly a part of  $\mathfrak{M}$ , and, since the converse can be proved in the same way,  $\mathfrak{M} = \mathfrak{M}'$ . Accordingly, different fields  $\mathfrak{M}$  between  $\mathfrak{K}$  and  $\mathfrak{N}$  have different subsystems  $\mathfrak{H}$  of the system  $\mathfrak{G}$ ;<sup>E92</sup> but the number of subsystems of  $\mathfrak{G}$  is finite, so only finitely many fields lie between  $\mathfrak{K}$  and  $\mathfrak{N}$ , and hence also between  $\mathfrak{K}$  and  $\mathfrak{L}$ . I.e.

10. *Between a field  $\mathfrak{K}$  and a finite extension  $\mathfrak{L}$  of the first kind there lie only finitely many fields.*

Since, further, all algebraic extensions of a perfect field are of the first kind, it follows that:

11. *Between a perfect field and a finite extension of it there lie only finitely many fields.*

#### § 14.

#### Imperfect fields: Arbitrary algebraic extensions, theorem of primitive elements and theorem of intermediate fields.

The theorems named in the heading hold, by § 11, 5. and § 13, 11., for every perfect field.<sup>E93</sup> There are, however, certain imperfect fields in which these theorems still hold as well. To investigate more closely the questions connected with this, we must now, having examined in § 12 and § 13 two special kinds of algebraic extension, namely the root fields and

the extensions of the first kind, consider arbitrary algebraic extensions. First it turns out that every such extension is composed in a definite way of two special ones:

1. *If  $\mathfrak{L}$  is an algebraic extension of the imperfect field  $\mathfrak{K}$ , then there is between  $\mathfrak{K}$  and  $\mathfrak{L}$  a definite field  $\mathfrak{L}_0$  of such a nature that  $\mathfrak{L}_0$  is of the first kind with respect to  $\mathfrak{K}$ ,  $\mathfrak{L}$  a root field with respect to  $\mathfrak{L}_0$ .  $\mathfrak{L}_0$  consists of all elements of  $\mathfrak{L}$  that are of the first kind with respect to  $\mathfrak{K}$ .*

For if  $\mathfrak{L}_0$  denotes the system of all elements of the first kind from  $\mathfrak{L}$ , then the field  $\mathfrak{K}(\mathfrak{L}_0)$  contains, by § 13, 8., only elements of the first kind, and is therefore identical with  $\mathfrak{L}_0$ ;  $\mathfrak{L}_0$  is consequently a field between  $\mathfrak{K}$  and  $\mathfrak{L}$ . If further  $\delta$  is any element from  $\mathfrak{L}$ ,  $f$  its exponent with respect to  $\mathfrak{K}$ , then  $\delta^{p^f}$  is of the first kind, hence an element of  $\mathfrak{L}_0$ , and consequently  $\delta$  is a root element of  $\mathfrak{L}_0$ . This field  $\mathfrak{L}_0$  is the only one that has the properties required under 1. For if  $\mathfrak{L}'_0$  has these properties, and the element  $\delta$  of  $\mathfrak{L}$  is of the first kind with respect to  $\mathfrak{K}$ , then  $\delta$  is also of the first kind with respect to  $\mathfrak{L}'_0$ , and since  $\delta$  is at the same time to be a root element of  $\mathfrak{L}'_0$ ,  $\delta$  itself must belong to the field  $\mathfrak{L}'_0$ .  $\mathfrak{L}'_0$  must therefore comprise all elements of the first kind, hence be identical with  $\mathfrak{L}_0$ .

2. *If  $\mathfrak{L}$  is an algebraic extension of the imperfect field  $\mathfrak{K}$ ,  $f$  an integer  $\geq 0$ , then the system  $\mathfrak{L}_f$  of those elements of  $\mathfrak{L}$  whose exponent is  $\leq f$  is a field (between  $\mathfrak{K}$  and  $\mathfrak{L}$ ).*

First, this is the case for  $\mathfrak{L}_0$  by Theorem 1. Next, the requirement that the exponent of an element  $a$  of  $\mathfrak{L}$  be  $\leq f$  is equivalent to the requirement that  $a^{p^f}$  have exponent 0,<sup>E 94</sup> hence be an element of  $\mathfrak{L}_0$ . If therefore  $a$  and  $b$  are elements of  $\mathfrak{L}_f$ , then  $a^{p^f}$  and  $b^{p^f}$ , and consequently also the sum, difference, product and quotient of  $a^{p^f}$  and  $b^{p^f}$ , are elements of  $\mathfrak{L}_0$ . These combinations, however, are the  $p^f$ -th powers of  $a + b$ ,  $a - b$ ,  $a \cdot b$ ,  $\frac{a}{b}$ . Therefore these four elements again belong to the system  $\mathfrak{L}_f$ , and this is a field.

3. *If one adjoins to an imperfect field  $\mathfrak{K}$  a system  $\mathfrak{S}$  of algebraic elements whose exponents do not exceed the number  $f$ , then the exponents of all elements of  $\mathfrak{K}(\mathfrak{S})$  are  $\leq f$ .*

For if  $\mathfrak{S}'$  denotes the system of all elements of  $\mathfrak{K}(\mathfrak{S})$  whose exponents are  $\leq f$ , then  $\mathfrak{S}'$  is a field by 2., and since all elements of  $\mathfrak{K}$  and  $\mathfrak{S}$  occur in  $\mathfrak{S}'$ ,  $\mathfrak{S}' = \mathfrak{K}(\mathfrak{S})$ .

*Exponent and reduced degree of a finite extension.*<sup>E 95</sup> — Let  $\mathfrak{L}$  be a finite extension of an imperfect field  $\mathfrak{K}$ . Then there is an integer  $f \geq 0$  such that  $\mathfrak{L}$  contains elements of exponent  $f$ , but none of greater exponent.<sup>E 96</sup> We call the number  $f$  the *exponent of  $\mathfrak{L}$  (with respect to  $\mathfrak{K}$ )*. If further  $\mathfrak{L}_0$  is the subfield of  $\mathfrak{L}$  that is formed by the elements of the first kind, and if  $[\mathfrak{L}_0 : \mathfrak{K}] = n$ , then we call the number  $n$  the *reduced degree of  $\mathfrak{L}$  (with respect to  $\mathfrak{K}$ )*. — If now  $\delta$  is an element from  $\mathfrak{L}$  of exponent  $f$ , then of the powers

$$\delta, \delta^p, \delta^{p^2}, \dots, \delta^{p^f}$$

only the last is of exponent 0, hence an element of  $\mathfrak{L}_0$ . Therefore  $[\mathfrak{L}_0(\delta) : \mathfrak{K}] = n \cdot p^f$ , hence  $n \cdot p^f$  is a divisor of  $[\mathfrak{L} : \mathfrak{K}]$ .<sup>E 97</sup> If further  $\eta$  is an arbitrary element of  $\mathfrak{L}$ ,  $n_1$  its reduced degree,  $f_1$  its exponent, then  $f_1 \leq f$ ,  $\eta^{p^{f_1}}$  is an element of  $\mathfrak{L}_0$ ,  $n_1$  is equal to the degree of  $\eta^{p^{f_1}}$ , hence a divisor of  $n$ . Since  $n_1 \cdot p^{f_1}$  is the degree of  $\eta$ , it follows:

4. *If  $\mathfrak{L}$  is a finite extension of the imperfect field  $\mathfrak{K}$ ,  $n$  its reduced degree,  $f$  its exponent, then the degree of  $\mathfrak{L}$  (with respect to  $\mathfrak{K}$ ) is a multiple, the degree of every element of  $\mathfrak{L}$  a divisor, of the number  $n \cdot p^f$ .*

If  $\mathfrak{L}$  is a simple extension, then the primitive elements have the same degree as  $\mathfrak{L}$  itself; this degree must therefore by 4. be equal to  $n \cdot p^f$ , and then  $f$  represents the exponent,  $n$  the reduced degree, of each primitive element.

As before, let  $\mathfrak{L}$  denote a finite, not necessarily simple, extension of the imperfect field  $\mathfrak{K}$ , and let  $\mathfrak{L}_0, n, f$  retain their earlier meaning. In  $\mathfrak{L}$  there are elements of exponent  $f$ , likewise elements of reduced degree  $n$ ; for the field  $\mathfrak{L}_0$  is of the first kind, hence has primitive elements. The degree of such an element is  $n$ , and since it is of the first kind,  $n$  is also its reduced degree. The question arises, however, whether one can always find in  $\mathfrak{L}$  an element that is at the same time of exponent  $f$  and of reduced degree  $n$ . For an understanding of the structure of finite extensions it is important to show that there always are such elements. We therefore now want to prove, in supplement to 4., the theorem:

5. *If  $\mathfrak{L}$  is a finite extension of the imperfect field  $\mathfrak{K}$ ,  $n$  its reduced degree,  $f$  its exponent, then there are in  $\mathfrak{L}$  elements of degree  $n \cdot p^f$ .*

We first remark that the field  $\mathfrak{K}$ , because it is imperfect, has infinitely many elements. In such a field  $\mathfrak{K}$ , however, the theorem holds that for an integral function  $F$ , different from 0, of  $n$  indeterminates  $t_0, t_1, \dots, t_{n-1}$ , one can substitute for these indeterminates such elements of  $\mathfrak{K}$  that the resulting element of  $\mathfrak{K}$  is likewise  $\neq 0$ . One shows this in a known manner first for  $n = 1$ , where one relies on the fact that infinitely many values are available, but the number of zeros is at most equal to the degree of the function; then in general by the inference from  $n$  to  $n + 1$ . — We now make use of this fact. Taking up again the earlier designations, we choose from the field  $\mathfrak{L}_0$  a primitive element  $\gamma$ , from the field  $\mathfrak{L}$  an element  $\delta$  of exponent  $f$  (in case  $f = 0$ , <sup>E 98</sup> any element  $\delta$  different from 0), and put  $\delta^{p^f} = \eta$ .

Of the powers

$$(1.) \quad \delta, \delta^p, \dots, \delta^{p^f} = \eta$$

the last is then the only one that belongs to  $\mathfrak{L}_0$ . The elements

$$(2.) \quad \varepsilon, \gamma, \gamma^2, \dots, \gamma^{n-1}$$

form a basis of  $\mathfrak{L}_0$ , and since  $\gamma$  is of the first kind, so that  $\mathfrak{L}_0 = \mathfrak{K}(\gamma) = \mathfrak{K}(\gamma^p) = \mathfrak{K}(\gamma^{p^2}) = \dots = \mathfrak{K}(\gamma^{p^f})$ , <sup>E 99</sup> and hence  $\gamma^{p^f}$  is a primitive element of  $\mathfrak{L}_0$ , and since  $\eta \neq 0$ , the elements

$$(3.) \quad \eta, \quad \eta \cdot \gamma^{p^f}, \quad \eta \cdot \gamma^{2p^f}, \quad \dots \quad \eta \cdot \gamma^{(n-1)p^f}$$

also form a basis of  $\mathfrak{L}_0$ . We now introduce  $2n$  indeterminates  $t_0, \dots, t_{n-1}; u_0, \dots, u_{n-1}$  and form the two linear forms:

$$(4.) \quad \xi = t_0 + \gamma t_1 + \gamma^2 t_2 + \dots + \gamma^{n-1} t_{n-1},$$

$$(5.) \quad \zeta = \eta u_0 + \eta \gamma^{p^f} u_1 + \eta \gamma^{2p^f} u_2 + \dots + \eta \gamma^{(n-1)p^f} u_{n-1}.$$

Then  $\xi$  as well as  $\zeta$  represents every element of  $\mathfrak{L}_0$  once, if we substitute for the  $t$ 's or  $u$ 's respectively all elements of  $\mathfrak{K}$ . For every non-negative integer  $k$ ,  $\zeta^k$  represents an integral homogeneous function of the indeterminates  $u$  with coefficients from  $\mathfrak{L}_0$ . If we express these

coefficients in terms of the basis (3.) and then arrange the expression according to the elements of this basis, we obtain

$$(6.) \quad \zeta^k = \eta A_{k0} + \eta \gamma^{p^f} A_{k1} + \cdots + \eta \gamma^{(n-1)p^f} A_{k, n-1}.$$

Here the  $A$  are integral homogeneous functions of the  $u$  with coefficients from  $\mathfrak{K}$ , and the same holds for the determinant

$$|A_{kl}| \quad (k, l = 0, \dots, n-1).$$

If we substitute for the indeterminates  $u$  any elements of  $\mathfrak{K}$ , then  $\zeta$  becomes an element of  $\mathfrak{L}_0$ ,  $|A_{kl}|$  an element of  $\mathfrak{K}$ , and indeed equal to 0 only if the elements

$$\varepsilon, \zeta, \zeta^2, \dots, \zeta^{n-1}$$

become linearly dependent (with respect to  $\mathfrak{K}$ ). But since we can choose the  $u$  such that  $\zeta$  becomes primitive,  $|A_{kl}|$ , regarded as a function of the indeterminates  $u$ , is different from 0. Therefore  $|A_{kl}|$  passes into a function  $\Delta$ , different from 0, of the indeterminates  $t_0, \dots, t_{n-1}$  if we replace  $u_0, \dots, u_{n-1}$  by  $t_0^{p^f}, \dots, t_{n-1}^{p^f}$ . After this substitution, as is evident from (4.), (5.),

$$(7.) \quad \zeta = \eta \xi^{p^f}.$$

If we now substitute for  $t_0, \dots, t_{n-1}$  elements of  $\mathfrak{K}$  such that  $\Delta \neq 0$  (and, in the case  $n = 1$ , we assume  $t_0 \neq 0$ ), <sup>E 100</sup> then  $\zeta = \eta \xi^{p^f}$  becomes a primitive, and  $\xi$  an element, different from 0, of  $\mathfrak{L}_0$ . The element  $\delta \cdot \xi$  of  $\mathfrak{L}$  has exponent  $f$ ; for since of the elements (1.) only the last belongs to the field  $\mathfrak{L}_0$ , but  $\xi$  is an element of  $\mathfrak{L}_0$ , it likewise follows that of the powers

$$(8.) \quad \delta \xi, \delta^p \xi^p, \dots, \delta^{p^f} \xi^{p^f} = \eta \xi^{p^f}$$

only the last is an element of  $\mathfrak{L}_0$ , hence of the first kind. Further, the elements (8.) all have the same reduced degree, and since  $\eta \xi^{p^f}$  is a primitive element of  $\mathfrak{L}_0$ , the reduced degree of  $\delta \xi$  is equal to  $n$ . Accordingly, the degree of  $\delta \xi$  is equal to  $n \cdot p^f$ , and this proves 5.

From 5. and § 7, 5. it follows immediately:

I. A finite extension  $\mathfrak{L}$  of an imperfect field  $\mathfrak{K}$  is simple if and only if  $[\mathfrak{L} : \mathfrak{K}] = n \cdot p^f$ , where  $n$  denotes the reduced degree,  $f$  the exponent, of  $\mathfrak{L}$ .

Again let  $\mathfrak{L}$  be an arbitrary finite extension of the imperfect field  $\mathfrak{K}$ , and  $\mathfrak{M}$  a field between  $\mathfrak{K}$  and  $\mathfrak{L}$ ; let  $n$  and  $m$  denote the reduced degrees of the fields  $\mathfrak{L}$  and  $\mathfrak{M}$ , and  $f$  and  $g$  their exponents. Then  $g \leq f$ ,

$$(9.) \quad [\mathfrak{M} : \mathfrak{K}] \geq m p^g.$$

Further, for every non-negative integer  $r$  let  $\mathfrak{L}_r$ , respectively  $\mathfrak{M}_r$ , denote the field of those elements of  $\mathfrak{L}$ , respectively  $\mathfrak{M}$ , whose exponents are  $\leq r$ , so that

$$\begin{aligned} \mathfrak{L}_f &= \mathfrak{L}, & \mathfrak{M}_g &= \mathfrak{M}, \\ [\mathfrak{L}_0 : \mathfrak{K}] &= n, & [\mathfrak{M}_0 : \mathfrak{K}] &= m \end{aligned}$$

and every field  $\mathfrak{M}_r$  becomes a subfield of  $\mathfrak{L}_r$ <sup>E101</sup>.  $\mathfrak{L}_0$  is of the first kind with respect to  $\mathfrak{K}$ , hence also with respect to  $\mathfrak{M}_0$ , consequently simple. A primitive element  $\gamma$  of  $\mathfrak{L}_0$  is hence a zero of an irreducible function  $\varphi(x)$  from  $\mathfrak{M}_0$ , of degree  $\frac{n}{m}$  and of the first kind. But  $\varphi(x)$  is also irreducible in the field  $\mathfrak{M} = \mathfrak{M}_g$ . For suppose that in  $\mathfrak{M}$  we had a decomposition

$$(10.) \quad \varphi(x) = \chi(x) \cdot \psi(x),$$

and let  $\overline{\varphi}(x), \overline{\chi}(x), \overline{\psi}(x)$  denote the functions that arise from  $\varphi(x), \chi(x), \psi(x)$  by replacing each coefficient with its  $p^g$ -th power; then from (10.) the equation

$$(11.) \quad \overline{\varphi}(x) = \overline{\chi}(x) \cdot \overline{\psi}(x)$$

would follow. Now since the exponent of every element of  $\mathfrak{M}$  is  $\leq g$ , so that its  $p^g$ -th power is contained in  $\mathfrak{M}_0$ , by (11.)  $\overline{\varphi}(x)$  would be reducible in the field  $\mathfrak{M}_0$ . But this contradicts the theorem of § 13, 2. Thus  $\varphi(x)$  is also irreducible in  $\mathfrak{M}$ , consequently  $[\gamma : \mathfrak{M}] = \frac{n}{m}$ , and by (9.)

$$(12.) \quad [\mathfrak{M}(\gamma) : \mathfrak{K}] = \frac{n}{m} [\mathfrak{M} : \mathfrak{K}] \geq n \cdot p^g.$$

Since  $\mathfrak{M}$  is of exponent  $g$  and  $\gamma$  of exponent 0, by 3.  $\mathfrak{M}(\gamma)$  is of exponent  $g$ , hence a part of the field  $\mathfrak{L}_g$ , which comprises all elements of  $\mathfrak{L}$  whose exponents are  $\leq g$ . — The field  $\mathfrak{L}$  contains elements of exponent  $f$ , hence elements of every exponent  $\leq f$  (§ 13, 1.). Consequently, of the fields

$$\mathfrak{L}_0, \mathfrak{L}_1, \dots, \mathfrak{L}_f = \mathfrak{L}$$

each is only a part of the next.

Let us now assume that  $\mathfrak{L}$  is simple with respect to  $\mathfrak{K}$ . Then by I  $[\mathfrak{L} : \mathfrak{K}] = n \cdot p^f$ ,  $[\mathfrak{L} : \mathfrak{L}_0] = p^f$ , hence

$$(13.) \quad \begin{aligned} [\mathfrak{L}_{r+1} : \mathfrak{L}_r] &= p, & (r = 0, \dots, f-1) \\ [\mathfrak{L}_g : \mathfrak{K}] &= n \cdot p^g. \end{aligned}$$

But since  $\mathfrak{M}(\gamma)$  is a subfield of  $\mathfrak{L}_g$ , it follows from (12.), (13.):

$$\mathfrak{M}(\gamma) = \mathfrak{L}_g, \quad \frac{n}{m} [\mathfrak{M} : \mathfrak{K}] = n \cdot p^g, \quad [\mathfrak{M} : \mathfrak{K}] = m \cdot p^g.$$

By I, however, this states that  $\mathfrak{M}$  is a simple extension of  $\mathfrak{K}$ . Hence we have the theorem:

II. *If  $\mathfrak{L}$  is a simple algebraic<sup>\*)</sup> extension of  $\mathfrak{K}$ , then every field between  $\mathfrak{K}$  and  $\mathfrak{L}$  is also simple with respect to  $\mathfrak{K}$ .*

The field  $\mathfrak{M}$  contains only such elements of  $\mathfrak{L}$  whose  $p^g$ -th power belongs to  $\mathfrak{M}_0$ , but it must also contain all these elements. For, to begin with, these elements form a field  $\mathfrak{M}'$  (see Theorem 2.) between  $\mathfrak{M}$  and  $\mathfrak{L}$ ; by II  $\mathfrak{M}'$  must contain a primitive element  $\delta$ . Since then  $\delta^{p^g}$  belongs to  $\mathfrak{M}_0$ ,  $[\mathfrak{M}' : \mathfrak{K}] = [\delta : \mathfrak{M}_0] \cdot [\mathfrak{M}_0 : \mathfrak{K}] \leq p^g \cdot m$ , hence  $\mathfrak{M}' = \mathfrak{M}$ . Every field  $\mathfrak{M}$  between  $\mathfrak{K}$  and  $\mathfrak{L}$  is thus uniquely determined by the field  $\mathfrak{M}_0$  of its elements of the first kind contained in it and by its exponent  $g$ . Now  $g \leq f$ ; and since  $\mathfrak{M}_0$  lies between  $\mathfrak{K}$  and  $\mathfrak{L}_0$ , and  $\mathfrak{L}_0$  is an extension of the first kind, by § 13, 10. only finitely many fields come into question for  $\mathfrak{M}_0$  as well; consequently there can be only finitely many fields between  $\mathfrak{K}$  and  $\mathfrak{L}$ .

<sup>\*)</sup> Exactly the same holds, however, also for simple transcendental extensions (theorem of Lüroth, see § 24).

We now drop the hypothesis that the finite extension  $\mathfrak{L}$  is simple, but assume instead that the number of fields between  $\mathfrak{K}$  and  $\mathfrak{L}$  is finite. Since the  $p$ -th power of every element of  $\mathfrak{L}_r$  ( $0 < r \leq f$ ) belongs to  $\mathfrak{L}_{r-1}$ ,  $[\mathfrak{L}_r : \mathfrak{L}_{r-1}]$  cannot be  $> p$ , because otherwise infinitely many fields would already lie between  $\mathfrak{L}_{r-1}$  and  $\mathfrak{L}_r$ , contrary to our hypothesis (§ 11, 6.). Since, on the other hand,  $\mathfrak{L}_{r-1}$  is only a part of  $\mathfrak{L}_r$ ,  $[\mathfrak{L}_r : \mathfrak{L}_{r-1}] = p$ , hence

$$[\mathfrak{L} : \mathfrak{K}] = [\mathfrak{L}_f : \mathfrak{L}_0] \cdot [\mathfrak{L}_0 : \mathfrak{K}] = n \cdot p^f,$$

which states that  $\mathfrak{L}$  is simple with respect to  $\mathfrak{K}$ . Together with the earlier results (§ 11, 3., § 11, 5., § 13, 11.)<sup>E 102</sup>, this proves:

III. *In order that only finitely many fields lie between an arbitrary field  $\mathfrak{K}$  and an extension  $\mathfrak{L}$  of it, it is necessary and sufficient that  $\mathfrak{L}$  be algebraic and simple with respect to  $\mathfrak{K}$ .*

In conclusion we prove further:

IV. *The theorem of primitive elements and the theorem of intermediate fields (§ 11) hold, besides for perfect fields, also for those imperfect fields  $\mathfrak{K}$  of characteristic  $p$  that are finite and of degree  $p$  with respect to  $\mathfrak{K}^p$ . For the other imperfect fields they do not hold.*<sup>E 103</sup>

For, first, let us assume that the stated theorems hold for the imperfect field  $\mathfrak{K}$  of characteristic  $p$ , and let us form, as in § 12, the extension field  $\mathfrak{L} = \mathfrak{K}^{p^{-1}}$ , so that  $\mathfrak{L}^p = \mathfrak{K}$ . If then  $a$  is an element not belonging to  $\mathfrak{K}$ , and  $b$  an arbitrary element, both of  $\mathfrak{L}$ , then  $[\mathfrak{K}(a) : \mathfrak{K}] = p$ , but also  $[\mathfrak{K}(a, b) : \mathfrak{K}] = p$ . For if  $[\mathfrak{K}(a, b) : \mathfrak{K}] > p$ , then, because the  $p$ -th powers of all elements of  $\mathfrak{K}(a, b)$  belong to  $\mathfrak{K}$ , by § 11, 6. infinitely many fields would lie between  $\mathfrak{K}$  and  $\mathfrak{K}(a, b)$ , and the extension would not be simple. Since this contradicts our assumption,  $[\mathfrak{K}(a, b) : \mathfrak{K}] = p = [\mathfrak{K}(a) : \mathfrak{K}]$ ; the element  $b$  hence belongs to  $\mathfrak{K}(a)$ , and since  $b$  was an arbitrary element of  $\mathfrak{L}$ ,  $\mathfrak{L} = \mathfrak{K}(a)$ , hence  $[\mathfrak{L} : \mathfrak{L}^p] = [\mathfrak{K}(a) : \mathfrak{K}] = p$ , and, because  $\mathfrak{L}$  is isomorphic to  $\mathfrak{K}$ , also  $[\mathfrak{K} : \mathfrak{K}^p] = p$ .

Second, let us assume that  $[\mathfrak{K} : \mathfrak{K}^p] = p$ , and let us denote by  $\mathfrak{L}$  any finite extension of  $\mathfrak{K}$ , by  $f$  its exponent, by  $n$  its reduced degree. If then  $\mathfrak{L}_r$  has the earlier meaning, and if we let every element of  $\mathfrak{L}_r$  correspond to its  $p$ -th power in  $\mathfrak{L}_r^p$ , then we obtain an isomorphic correspondence between  $\mathfrak{L}_r$  and  $\mathfrak{L}_r^p$  in which  $\mathfrak{K}$  is mapped isomorphically onto  $\mathfrak{K}^p$ . From this it follows, as one sees at once,

$$[\mathfrak{L}_r : \mathfrak{K}] = [\mathfrak{L}_r^p : \mathfrak{K}^p]$$

and from that

$$[\mathfrak{L}_r : \mathfrak{L}_r^p] \cdot [\mathfrak{L}_r : \mathfrak{K}] = [\mathfrak{L}_r : \mathfrak{L}_r^p] \cdot [\mathfrak{L}_r^p : \mathfrak{K}^p] = [\mathfrak{L}_r : \mathfrak{K}^p] = [\mathfrak{L}_r : \mathfrak{K}] \cdot [\mathfrak{K} : \mathfrak{K}^p] = p[\mathfrak{L}_r : \mathfrak{K}],$$

hence

$$(14.) \quad [\mathfrak{L}_r : \mathfrak{L}_r^p] = p.$$

Now let  $0 < r \leq f$ . Then  $\mathfrak{L}_{r-1}$  is only a part of  $\mathfrak{L}_r$ ; on the other hand the  $p$ -th power of every element of  $\mathfrak{L}_r$  belongs to  $\mathfrak{L}_{r-1}$ , i.e.  $\mathfrak{L}_{r-1}$  lies between  $\mathfrak{L}_r^p$  and  $\mathfrak{L}_r$ , and from (14.) it follows that  $\mathfrak{L}_{r-1} = \mathfrak{L}_r^p$  and thus

$$[\mathfrak{L}_r : \mathfrak{L}_{r-1}] = p.$$

From this, however, it follows further that

$$[\mathfrak{L} : \mathfrak{K}] = [\mathfrak{L}_f : \mathfrak{L}_0] \cdot [\mathfrak{L}_0 : \mathfrak{K}] = np^f.$$

This equation, however, expresses that  $\mathfrak{L}$  is simple with respect to  $\mathfrak{K}$ , q.e.d.

## § 15.

**Finite fields.**

By a *finite field* we understand a field of finitely many elements.<sup>E 104</sup> If  $\mathfrak{K}$  is a finite field, then the prime field  $\mathfrak{P}$  contained in  $\mathfrak{K}$  is also finite, the characteristic of  $\mathfrak{K}$  therefore a prime number. Further,  $\mathfrak{K}$  must be finite with respect to its prime field. If, on the other hand,  $\mathfrak{K}$  has the characteristic  $p$ , and if  $\mathfrak{K}$  is finite with respect to its prime field  $\mathfrak{P}_p = \mathfrak{P}$ ,  $[\mathfrak{K} : \mathfrak{P}] = n$ , and if the elements  $a_1, \dots, a_n$  form a basis of  $\mathfrak{K}$  with respect to  $\mathfrak{P}$ , then every element of  $\mathfrak{K}$  is represented once in the form

$$c_1 a_1 + c_2 a_2 + \dots + c_n a_n$$

if we let  $c_1, \dots, c_n$  range over all elements of the prime field.  $\mathfrak{K}$  therefore consists of  $p^n$  elements. Accordingly the number of elements of a finite field is always a prime-number power. If, again, an arbitrary prime-number power  $p^n$  is given, and if we make an extension of the prime field  $\mathfrak{P}_p$  that just suffices to decompose the function  $x^{p^n} - x$  completely, then the following results: In the extension field  $\mathfrak{K}$  the function  $x^{p^n} - x$  has  $p^n$  distinct zeros, because its derivative is  $p^n x^{p^n-1} - \varepsilon = -\varepsilon$  and hence relatively prime to  $x^{p^n} - x$ . If further  $a$  and  $b$  are any two zeros of  $x^{p^n} - x$ , then it follows from  $a^{p^n} = a$ ,  $b^{p^n} = b$  that  $(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n} = a \pm b$ , likewise  $(a \cdot b)^{p^n} = a \cdot b$ ,  $(\frac{a}{b})^{p^n} = \frac{a}{b}$  holds, which says that the zeros of  $x^{p^n} - x$  form a field of  $p^n$  elements. If, on the other hand,  $\mathfrak{K}$  is a finite field of  $p^n$  elements, then  $p$  is its characteristic,  $n$  its degree with respect to the prime field.  $\mathfrak{K}$  is absolutely algebraic, and likewise every element  $a$  of  $\mathfrak{K}$  is absolutely algebraic, its absolute degree  $m$  a divisor of  $n$ . By § 12, 4. the sequence

$$a, a^p, a^{p^2}, \dots$$

consists of a period of  $m$  distinct elements; therefore for every exponent  $f$  divisible by  $m$  we have  $a^{p^f} = a$ , hence also  $a^{p^n} = a$ . Consequently the  $p^n$  elements of  $\mathfrak{K}$  are the zeros of the function  $x^{p^n} - x$ , and  $\mathfrak{K}$  represents an extension of the prime field that just suffices to decompose the function  $x^{p^n} - x$  completely. But since all extensions of a field that just suffice for the complete breaking up of a given function are equivalent, all fields of  $p^n$  elements are isomorphic. Thus we obtain:

1. *The number of elements of a finite field is a prime-number power, and every prime-number power  $p^n$  is the number of elements of one and only\*) one field type;  $p$  is its characteristic,  $n$  its absolute degree.*

We will denote this type by  $\mathfrak{E}_{p,n}$ .

In order for a field  $\mathfrak{E}_{p,n}$  to be contained in a field  $\mathfrak{K}$  of characteristic  $p$ , it is necessary and sufficient, by what precedes, that the function  $x^{p^n} - x$  break up into linear factors in  $\mathfrak{K}$ . The  $p^n$  zeros of  $x^{p^n} - x$  then form the field. From this we obtain first:

2. *A field cannot contain more than one subfield of the type  $\mathfrak{E}_{p,n}$  (for given  $n$ ).*

If  $d$  is a divisor of  $n$ , then  $p^d - 1$  is a divisor of  $p^n - 1$ ,<sup>E 105</sup> therefore  $x^{p^d} - x = x(x^{p^d-1} - \varepsilon)$  is a divisor of  $x^{p^n} - x = x(x^{p^n-1} - \varepsilon)$ . So if the field  $\mathfrak{K}$  contains a field  $\mathfrak{E}_{p,n}$ , then the function  $x^{p^n} - x$ , and hence also the function  $x^{p^d} - x$ , breaks up into linear factors in  $\mathfrak{K}$ . Hence we have the theorem:

---

\*) This was probably first stated and proved by *Moore* (Math. Papers read at the intern. math. congress, Chicago 1893, (New York 1896), p. 210ff.).

3. If a field  $\mathfrak{K}$  contains a field  $\mathfrak{E}_{p,n}$ , then it also contains fields of all types  $\mathfrak{E}_{p,d}$ , where  $d$  denotes a divisor of  $n$ .

A further consequence of 2. and 3. is:

4. A field  $\mathfrak{E}_{p,n}$  has as many subfields as the number  $n$  has divisors, every divisor of  $n$  denotes the degree of a subfield;<sup>E 106</sup>

further:

5. If the field  $\mathfrak{K}$  contains a field  $\mathfrak{E}_{p,n}$ , then this consists of all those absolutely algebraic elements of  $\mathfrak{K}$  whose degree is a divisor of  $n$ .

For, first, every element of  $\mathfrak{E}_{p,n}$  is absolutely algebraic and its degree a divisor of  $n$ . If, on the other hand,  $a$  is an absolutely algebraic element of  $\mathfrak{K}$  and its degree  $d$  a divisor of  $n$ , then the field  $\mathfrak{P}_p(a)$  contained in  $\mathfrak{K}$  is of the type  $\mathfrak{E}_{p,d}$  and, since  $\mathfrak{K}$  contains only *one* field of this type, is identical with the one that  $\mathfrak{E}_{p,n}$  also contains. Hence  $a$  is an element of  $\mathfrak{E}_{p,n}$ .

Let  $\mathfrak{K}$  be an arbitrary field of characteristic  $p$ ; let  $a$  and  $b$  be absolutely algebraic elements of  $\mathfrak{K}$ ,  $m$  and  $n$  their degrees,  $m$  relatively prime to  $n$ ,  $t$  the degree of  $a + b$ . Then (§ 12, 4.)

$$a + b = (a + b)^{p^{tn}} = a^{p^{tn}} + b^{p^{tn}} = a^{p^{tn}} + b,$$

hence

$$a = a^{p^{tn}},$$

from which it follows that  $m$  goes into  $tn$ , hence also into  $t$ . We show likewise that  $n$  goes into  $t$ , and that  $t$  is consequently divisible by  $m \cdot n$ . On the other hand

$$(a + b)^{p^{mn}} = a^{p^{mn}} + b^{p^{mn}} = a + b,$$

hence  $mn$  is divisible by  $t$ , consequently  $t = mn$ . This result can at once be extended to sums of more than two elements, and thus we obtain:

6. If  $a_1, a_2, \dots, a_\nu$  are absolutely algebraic elements of a field of prime-number characteristic, and if their degrees are relatively prime to one another, then the degree of  $a_1 + a_2 + \dots + a_\nu$  is equal to the product of these degrees.

From this we draw some simple consequences: If

$$(1.) \quad n = q_1^{r_1} \cdot q_2^{r_2} \cdots q_\nu^{r_\nu}$$

represents the decomposition of the natural number  $n$  into powers of distinct prime numbers, then a field of the type  $\mathfrak{E}_{p,n}$  contains a subfield  $\mathfrak{A}$  of absolute degree  $q_i^{r_i}$  ( $i = 1, \dots, \nu$ ), and this in turn a subfield  $\mathfrak{B}$  of degree  $q_i^{r_i-1}$ . If  $a_i$  is an element contained in  $\mathfrak{A}$  but not in  $\mathfrak{B}$ , then the degree of  $a_i$  is a divisor of  $q_i^{r_i}$  but by 5. not a divisor of  $q_i^{r_i-1}$ , consequently equal to  $q_i^{r_i}$ . We can therefore take  $\nu$  elements  $a_1, a_2, \dots, a_\nu$  of the degrees  $q_1^{r_1}, q_2^{r_2}, \dots, q_\nu^{r_\nu}$  from the field  $\mathfrak{E}_{p,n}$ . The element  $a_1 + a_2 + \dots + a_\nu$  is then of degree  $n$ , hence primitive, and thus it is proved:

7. Every finite field is simple with respect to its prime field, and therefore the prime field contains irreducible functions of every degree  $n$ .

Let the field  $\mathfrak{K}$  of characteristic  $p$  contain the fields  $\mathfrak{E}_{p,n_1}$  and  $\mathfrak{E}_{p,n_2}$ , let  $n$  be the least common multiple of  $n_1$  and  $n_2$ , and let equation (1.) represent the decomposition of  $n$  into

prime-number powers. Then  $q_i^{r_i}$  ( $i = 1, \dots, \nu$ ) goes into at least one of the numbers  $n_1, n_2$ ,  $\mathfrak{K}$  therefore contains a finite field of degree  $q_i^{r_i}$ , hence also an element  $a_i$  of this degree. If we determine one such element for each  $i = 1, \dots, \nu$ , then  $a = a_1 + a_2 + \dots + a_\nu$  is an element, and  $\mathfrak{P}_p(a)$  a field of absolute degree  $n$ .<sup>E107</sup> Hence:

8. *If the field  $\mathfrak{K}$  contains finite fields of the (absolute) degrees  $n_1, n_2$  and if  $n$  is the least common multiple of  $n_1$  and  $n_2$ , then  $\mathfrak{K}$  also contains a field of degree  $n$ .*

On the basis of Theorem 7. we can fill the gap that remained in the proof of § 11, 4., where the case of a finite field had been excluded. For if we extend a finite field  $\mathfrak{K}$  by adjunction of finitely many algebraic elements  $\alpha, \beta, \gamma, \dots$  to a field  $\mathfrak{L}$ , then  $\mathfrak{L}$  is finite with respect to  $\mathfrak{K}$ , hence also with respect to the prime field, consequently a finite field. By 7. there are elements  $\xi$  in  $\mathfrak{L}$  such that  $\mathfrak{P}_p(\xi) = \mathfrak{L}$ , and hence also  $\mathfrak{K}(\xi) = \mathfrak{L}$ .  $\mathfrak{L}$  is therefore simple with respect to  $\mathfrak{K}$ , and since  $\mathfrak{K}$  is a perfect field,<sup>E108</sup>  $\xi$  is a zero of an irreducible function of  $\mathfrak{K}$  with simple zeros. Hence:

9. *The theorem § 11, 4. holds also for finite fields.*<sup>E109</sup>

Every element of the field  $\mathfrak{E}_{p,n}$  satisfies, in the prime field  $\mathfrak{P}_p = \mathfrak{E}_{p,1}$ , an irreducible equation  $g(x) = 0$  whose degree is a divisor of  $n$ . So if we decompose the function  $x^{p^n} - x$ , whose zeros are all the elements of  $\mathfrak{E}_{p,n}$ , into irreducible factors in  $\mathfrak{P}_p$ , then these are all distinct, and their degrees are divisors of  $n$ . But conversely, every irreducible function  $g(x)$  from  $\mathfrak{P}_p$  whose degree  $d$  goes into  $n$  must also be contained among the factors of  $x^{p^n} - x$ . For if  $\mathfrak{L}$  denotes an extension of  $\mathfrak{P}_p$  that just suffices for the breaking up of  $g(x)$ , and if  $a$  is a zero of  $g(x)$  in  $\mathfrak{L}$ , then  $\mathfrak{P}_p(a)$  is a field  $\mathfrak{E}_{p,d}$  and contains by 5. all elements of  $\mathfrak{L}$  whose degree is a divisor of  $d$ , hence also all zeros of  $g(x)$ . From this it follows that  $\mathfrak{P}_p(a) = \mathfrak{L}$ , and the function  $x^{p^d} - x$ , which has all the elements of  $\mathfrak{P}_p(a) = \mathfrak{E}_{p,d} = \mathfrak{L}$  as zeros, must be divisible by  $g(x)$ .  $g(x)$  therefore also goes into  $x^{p^n} - x$ , and we obtain the theorem:

10. *The function  $x^{p^n} - x$  represents the product of all irreducible functions of the prime field  $\mathfrak{P}_p$  whose degree is a divisor of  $n$ .*

## § 16.

### The absolutely algebraic fields of prime-number characteristic.

Let  $p$  be an arbitrary prime number, but one fixed once and for all for the discussion that follows. — We now wish to consider the *absolutely algebraic fields of characteristic  $p$* . To these belong all *finite* fields of characteristic  $p$ , which are characterized by being finite with respect to the prime field  $\mathfrak{P}$ . In the more comprehensive area of all absolutely algebraic fields of characteristic  $p$ , the same laws are found, in the main, as in the narrower area of finite fields. To bring this out more clearly, we denote all the prime numbers in their natural sequence by  $q_1, q_2, q_3, \dots$ , so that

$$q_1 = 2, q_2 = 3, q_3 = 5, \dots$$

holds. Then every natural number is represented in one way in the form

$$(1.) \quad \prod_{i=1}^{\infty} q_i^{z_i}$$

where the exponents  $\varkappa_i$  are integral non-negative numbers of which only a finite number are different from 0. We now wish to consider more generally all (symbolic) expressions of the form (1.) in which for each exponent  $\varkappa_i$  we may put, as we please, 0 or a natural number or also the sign  $\infty$ , and for these expressions, which we call *G-numbers* ( $G = \text{Grad}$ ), and which include the natural numbers as well, we stipulate the following, in agreement with the laws that hold for natural numbers: *Two G-numbers*

$$m = \prod q_i^{\varkappa_i}, \quad n = \prod q_i^{\lambda_i}$$

are called equal if and only if  $\varkappa_i = \lambda_i$  for every  $i$ .  $m$  is called divisible by  $n$ , a multiple of  $n$ , etc., if  $\lambda_i \leq \varkappa_i$  for every  $i$ . Here  $\infty$  counts as greater than every other exponent. If  $m$  is divisible by  $n$ , then we also form the quotient, by stipulating that

$$\frac{m}{n} = \prod q_i^{\varkappa_i - \lambda_i}$$

shall hold, where  $\varkappa_i - \lambda_i$  is to be put equal to 0 if  $\varkappa_i = \infty$ ,  $\lambda_i = \infty$ , equal to  $\infty$  if  $\varkappa_i = \infty$  but  $\lambda_i$  is finite. It follows at once that all *G-numbers* are divisible by 1, and that all go into the *G-number* all of whose exponents  $\varkappa_i$  equal  $\infty$ . If we have any system of finitely or infinitely many *G-numbers*, these always have a *greatest common divisor*  $t$ , into which all common divisors go, and a *least common multiple*  $v$ , which goes into all common multiples. The exponent of  $q_i$  in  $t$  is equal to the smallest exponent that  $q_i$  has in the given *G-numbers*, the exponent of  $q_i$  in  $v$  equal to the greatest of these exponents or, if no such exponent exists — that is, if no exponent of  $q_i$  equals  $\infty$ , but every finite number is exceeded by some of these exponents —, equal to  $\infty$ .

If  $m$  is any *G-number*, then the natural numbers that go into  $m$  form a system  $\mathfrak{S}$  of the following properties:

- 1) If  $n$  is a number from  $\mathfrak{S}$ , then every divisor of  $n$  also belongs to  $\mathfrak{S}$ .
- 2) If  $n_1, n_2$  are numbers from  $\mathfrak{S}$ , then their least common multiple is also a number from  $\mathfrak{S}$ .<sup>E 110</sup>

The number  $m$  is then in every case the least common multiple of all numbers from  $\mathfrak{S}$ , and is therefore in turn completely determined by the system  $\mathfrak{S}$ . Conversely, if we have any system  $\mathfrak{S}$  of natural numbers that has properties 1) and 2), and  $m$  is the least common multiple of all numbers from  $\mathfrak{S}$ , then  $\mathfrak{S}$  consists of all the natural numbers that go into  $m$ .

Now let  $\mathfrak{K}$  be any absolutely algebraic field of characteristic  $p$ . The degrees of the finite fields contained in  $\mathfrak{K}$  then form a system  $\mathfrak{S}$  of natural numbers that, by § 15, 3. and 8., has properties 1) and 2). Let  $m$  be the least common multiple of the numbers from  $\mathfrak{S}$ . If  $m$  is a natural number, then  $\mathfrak{K}$  is a finite field of degree  $m$ . If, conversely,  $\mathfrak{K}$  is a finite field, then  $m$  represents the degree of this field. But we now also wish, in the cases where  $\mathfrak{K}$  is not finite and accordingly  $m$  is not a natural number, to call  $m$  the (absolute) degree of  $\mathfrak{K}$ . The following therefore holds:

1. Every absolutely algebraic field of characteristic  $p$  has a definite degree, which is a *G-number*.

The following theorems also hold, as we have yet to show:

2. There is an absolutely algebraic field of characteristic  $p$  whose degree is equal to an arbitrarily prescribed *G-number*.

3. All absolutely algebraic fields of the same characteristic  $p$  and of the same degree are isomorphic. <sup>E 111</sup>

In order to arrive at a proof of 2., we undertake a numbering of the integral functions with integer coefficients reduced mod.  $p$ . By the number  $\nu$  of such a function

$$(2.) \quad f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0,$$

in which, therefore, the coefficients are numbers from the series  $0, 1, \dots, p-1$ , we understand the number  $f(p)$ , so that

$$(3.) \quad \nu = a_n p^n + a_{n-1} p^{n-1} + \cdots + a_0$$

holds. <sup>E 112</sup> Then not only does each of the functions considered here have a number  $\geq 0$ , but also every integer  $\geq 0$  represents the number of one and only one of these functions. For the equation (3.) is, after all, nothing other than the representation of the number  $\nu$  in the system with the base  $p$ . We then transfer this numbering to the integral functions of a prime field  $\mathfrak{P} = \mathfrak{P}_p$ , that is, to all the elements of  $\mathfrak{P}[x]$ , which, after all, are also uniquely represented in the form (2.). Here, as is seen at once, of two functions of different degree the one of smaller degree also has the smaller number, and among the functions of the same degree those in which the coefficient of the highest power is the unity have smaller numbers than the others.

If  $n$  is any natural number, then there are, as we know, irreducible functions of degree  $n$  in  $\mathfrak{P}$ . Among these let the one with the smallest number be denoted by  $\varphi_n(x)$ . If  $d$  is a divisor of  $n$ , then there are in a finite extension field  $\mathfrak{E}_{p,n}$   $n$  elements  $j, j_1, \dots, j_{n-1}$  that satisfy the equation  $\varphi_n(x) = 0$ , and  $d$  elements that satisfy the equation  $\varphi_d(x) = 0$ . The latter can be represented as integral functions of  $j$  whose degree is  $< n$  and whose coefficients belong to  $\mathfrak{P}$ . In the language of congruences we can express this thus: There are in  $\mathfrak{P}$   $d$  functions  $\chi_1(x), \dots, \chi_d(x)$  whose degree is  $< n$  and for which

$$\varphi_d(\chi_i(x)) \equiv 0 \pmod{\varphi_n(x)} \quad (i = 1, \dots, d)$$

holds. Among these we denote the one of smallest number by  $\psi_{d,n}(x)$ . Then we can say: If in an extension field of  $\mathfrak{P}$  the element  $j$  is a zero of  $\varphi_n(x)$ , then  $\psi_{d,n}(j)$  is a zero of  $\varphi_d(x)$ .  $\varphi_n(x)$  and  $\psi_{d,n}(x)$  are, for every natural number  $n$  and every divisor  $d$  of  $n$ , well-defined functions from  $\mathfrak{P}$  that can easily be computed for any given  $n, d$ . Let it further be pointed out that  $\varphi_1(x) = x$ ,  $\psi_{1,n}(x) = 0$  holds, while  $\psi_{d,n}(x)$ , as soon as  $d > 1$ , is at least of the first degree.  $\psi_{n,n}(x)$  becomes equal to  $x$  for  $n > 1$ .

Now let any  $G$ -number

$$m = \prod q_i^{z_i}$$

be given. If we denote for every natural number  $n$  by  $r_n$  the greatest common divisor of  $n!$  and  $m$ , then

$$(4.) \quad r_1, r_2, \dots$$

form a sequence of natural numbers each of which goes into the following ones. A natural number  $n$  that goes into  $m$  also goes into  $r_n$ , since it goes into  $n!$ . But a number that does not go into  $m$  cannot go into any of the numbers (4.) either. Consequently: The system  $\mathfrak{S}$  of the natural divisors of  $m$  is identical with the system of the numbers that go into numbers of

the sequence (4.). If we disregard the case, already settled, that  $m$  is finite, i.e. a natural number, then the numbers (4.) will grow beyond all bounds. By leaving out elements from (4.) we can bring it about that an infinite sequence of numbers remains in which already the first element is  $> 1$  and no two are equal to each other. This sequence of numbers still has the properties on which alone we rely, namely that every number goes into the following ones, and that the natural numbers going into numbers of the sequence are exactly the divisors of  $m$ .

We now introduce a system of elements

$$j_1, j_2, \dots \text{ in inf.}$$

by decreeing that  $j_n$  shall be a zero of the function  $\varphi_{r_n}(x)$  — for which we also write  $\bar{\varphi}_n(x)$ . Then  $\mathfrak{P}(j_n) = \mathfrak{K}_n$  represents a finite field of degree  $r_n$ . We thus obtain a system of fields

$$\mathfrak{K}_1, \mathfrak{K}_2, \dots,$$

which at first have nothing to do with one another. If we replace the function sign  $\psi_{r_n, r_{n+1}}$  by  $\bar{\psi}_{n, n+1}$ , then  $\bar{\psi}_{n, n+1}(j_{n+1})$  represents a zero of  $\bar{\varphi}_n(x)$ , and we therefore have a uniquely determined isomorphic correspondence between  $\mathfrak{K}_n = \mathfrak{P}(j_n)$  and the field  $\mathfrak{P}(\bar{\psi}_{n, n+1}(j_{n+1}))$  contained in  $\mathfrak{K}_{n+1} = \mathfrak{P}(j_{n+1})$ , in which the element  $j_n$  and the element  $\bar{\psi}_{n, n+1}(j_{n+1})$  correspond to each other. Therefore we may stipulate that  $j_n = \bar{\psi}_{n, n+1}(j_{n+1})$  shall hold, without the relations that have so far held between the elements thereby losing their validity. By this stipulation, which shall hold for every  $n$ , however, every field of the series

$$(5.) \quad \mathfrak{K}_0 = \mathfrak{P}, \mathfrak{K}_1, \mathfrak{K}_2, \dots$$

becomes part of the following one. The totality of all elements that occur in these fields represents a field  $\mathfrak{L}$ , and we can easily show that this field has the desired properties. First it is clear that  $\mathfrak{L}$  is an absolutely algebraic field of characteristic  $p$ , because this holds for all fields from (5.). If further  $n$  is a natural number that goes into  $m$ , then  $n$  goes into  $r_n$ , and the field  $\mathfrak{K}_n$ , whose degree is  $r_n$ , has a subfield of degree  $n$ , which is also a subfield of  $\mathfrak{L}$ . But if  $n$  does not go into  $m$ , hence also into no number  $r_\infty$ , then none of the fields  $\mathfrak{K}_\infty$  contains an element of degree  $n$ ; hence  $\mathfrak{L}$  also contains no such element, hence also no field of degree  $n$ . Therefore  $m$  is the degree of  $\mathfrak{L}$ .

We now come to the proof of 3. and assume that besides the field  $\mathfrak{L}$  just constructed, a second one,  $\mathfrak{L}'$ , is given, which, like  $\mathfrak{L}$ , is absolutely algebraic and has the characteristic  $p$  and the degree  $m$ . Then it is to be shown that  $\mathfrak{L}$  and  $\mathfrak{L}'$  are isomorphic. — In this proof we may, as is easily seen, presuppose that the prime field of  $\mathfrak{L}'$  is identical with that of  $\mathfrak{L}$ . Since each of the numbers  $r_n$  goes into the degree  $m$  of  $\mathfrak{L}'$ ,  $\mathfrak{L}'$  has, by hypothesis, a finite subfield  $\mathfrak{K}'_n$  of degree  $r_n$ , and therefore the function  $\bar{\varphi}_n(x)$  irreducible in  $\mathfrak{P}$ , whose degree is  $r_n$ , must break up into linear factors in  $\mathfrak{L}'$ . We now imagine any system of elements

$$i_1, i_2, \dots \text{ in inf.}$$

picked out from  $\mathfrak{L}'$  in such a way that  $i_n$  becomes a zero of  $\bar{\varphi}_n(x)$ .\*) <sup>E113</sup> From this system we now wish to derive a second such one

$$j'_1, j'_2, \dots \text{ in inf.}$$

\*) It is here, for the first time, that use is made of the *principle of choice*. It can in no way be avoided in the proof of the present theorem.

in a uniquely determined way. For this purpose we stipulate that  $j'_1 = i_1$  shall hold, and give a method by which  $j'_{n+1}$  is determined when the elements  $j'_1, \dots, j'_n$  are already determined. Now  $i_{n+1}$  is a zero of the function  $\bar{\varphi}_{n+1}(x)$  irreducible in  $\mathfrak{P}$ ; therefore every power  $i_{n+1}^{p^f}$  also represents a zero of  $\bar{\varphi}_{n+1}(x)$ , and we obtain every zero once if we give the exponent  $f$  the values  $0, 1, \dots, (r_{n+1} - 1)$ . Further it follows from  $\bar{\varphi}_{n+1}(i_{n+1}) = 0$  that  $\bar{\psi}_{n,n+1}(i_{n+1})$  is a zero of  $\bar{\varphi}_n(x)$ . By

$$(6.) \quad (\bar{\psi}_{n,n+1}(i_{n+1}))^{p^f}$$

every zero of  $\bar{\varphi}_n(x)$  — hence, in particular,  $j'_n$  — is represented once if the numbers  $0, 1, \dots, (r_n - 1)$  are put for  $f$ . Let  $\nu$  be that one among these numbers for which the expression (6.) becomes equal to  $j'_n$ . Then we wish to stipulate that  $j'_{n+1} = i_{n+1}^{p^\nu}$  shall hold. Since  $\bar{\psi}_{n,n+1}(x)$  is a function in the prime field, we have

$$j'_n = (\bar{\psi}_{n,n+1}(i_{n+1}))^{p^\nu} = \bar{\psi}_{n,n+1}(i_{n+1}^{p^\nu}) = \bar{\psi}_{n,n+1}(j'_{n+1}),$$

and we therefore have for every  $n$  the equations

$$(7.) \quad \bar{\varphi}_n(j'_n) = 0, \quad j'_n = \bar{\psi}_{n,n+1}(j'_{n+1}).$$

Of the fields of the series

$$(8.) \quad \mathfrak{P}, \quad \mathfrak{K}'_1 = \mathfrak{P}(j'_1), \quad \mathfrak{K}'_2 = \mathfrak{P}(j'_2), \dots$$

each is contained in the next, and all are subfields of  $\mathfrak{L}'$ . But every element from  $\mathfrak{L}'$  also occurs in fields of this series. For the degree of an element of  $\mathfrak{L}'$  is a divisor of  $m$ , hence a divisor of a number  $r_n$ , and the field  $\mathfrak{K}'_n$ , whose degree is  $r_n$ , comprises (§ 15, 5.) all elements of  $\mathfrak{L}'$  whose degree goes into  $r_n$ . Since now the element  $j_n$  of  $\mathfrak{K}_n$  and the element  $j'_n$  of  $\mathfrak{K}'_n$  are zeros of the same irreducible function  $\bar{\varphi}_n(x)$  from  $\mathfrak{P}$ , there exists a definite isomorphic correspondence  $\pi_n$  between  $\mathfrak{K}_n = \mathfrak{P}(j_n)$  and  $\mathfrak{K}'_n = \mathfrak{P}(j'_n)$ , in which the elements  $j_n$  and  $j'_n$  correspond to each other. From

$$j_n = \bar{\psi}_{n,n+1}(j_{n+1}), \quad j'_n = \bar{\psi}_{n,n+1}(j'_{n+1})$$

it follows further that the correspondence  $\pi_{n+1}$  comprises the correspondence  $\pi_n$ . But from this it results at once that by the isomorphisms

$$\pi_1, \pi_2, \dots$$

a one-to-one and indeed isomorphic correspondence between  $\mathfrak{L}$  and  $\mathfrak{L}'$  is established. This proves Theorem 3.

We now wish, even when  $m$  is an infinite  $G$ -number, to denote by  $\mathfrak{E}_{p,m}$  an absolutely algebraic field of characteristic  $p$  and of degree  $m$ . The degree  $m$  was defined as the least common multiple of the degrees of the finite fields contained in  $\mathfrak{E}_{p,m}$ , or, what amounts to the same thing, of the degrees of the elements of  $\mathfrak{E}_{p,m}$ ; and the system of these degrees is identical with the system of the natural numbers going into  $m$ . On this basis we easily show:

4. *If one adjoins to the prime field  $\mathfrak{P}_p$  a system  $\mathfrak{S}$  of algebraic elements, then there arises an absolutely algebraic field  $\mathfrak{E}_{p,m}$  whose degree  $m$  is equal to the least common multiple of the degrees of the elements of  $\mathfrak{S}$ .*

For let  $m'$  be this least common multiple. Then  $m$ , being the least common multiple of the degrees of *all* elements of  $\mathfrak{E}_{p,m}$ , is divisible by  $m'$ . Now, first, if  $\mathfrak{S}$  is a finite system, then  $\mathfrak{E}_{p,m} = \mathfrak{P}_p(\mathfrak{S})$  is a finite field and contains a field  $\mathfrak{E}_{p,m'}$ . But all elements of  $\mathfrak{E}_{p,m}$  whose degree goes into  $m'$  belong to this field. Since all elements of  $\mathfrak{S}$  belong to these, we have  $\mathfrak{E}_{p,m'} = \mathfrak{E}_{p,m}$ , hence  $m' = m$ . — If the system  $\mathfrak{S}$  is infinite,  $\alpha$  an element of  $\mathfrak{E}_{p,m}$ ,  $n$  its degree, then we can determine a finite subsystem  $\mathfrak{S}'$  of  $\mathfrak{S}$  such that  $\alpha$  is contained in the finite field  $\mathfrak{P}_p(\mathfrak{S}')$ .  $n$  then goes into the degree of  $\mathfrak{P}_p(\mathfrak{S}')$ , and this, by what precedes, is equal to the least common multiple of the degrees of the elements of  $\mathfrak{S}'$ , hence a divisor of  $m'$ . Thus  $n$  goes into  $m'$ , and  $m'$  is therefore the least common multiple not only of the degrees of the elements of  $\mathfrak{S}$ , but of all elements of  $\mathfrak{E}_{p,m}$ . Hence again  $m' = m$ .

If a field  $\mathfrak{K}$  contains a field  $\mathfrak{E}_{p,m}$  and if the natural number  $n$  goes into  $m$ , then  $\mathfrak{E}_{p,m}$  contains a finite field  $\mathfrak{E}_{p,n}$ , which in turn contains all elements of degree  $n$  occurring in  $\mathfrak{K}$  (§ 15, 5.). On the other hand the degree of every element of  $\mathfrak{E}_{p,m}$  must go into  $m$ .  $\mathfrak{E}_{p,m}$  therefore consists of all absolutely algebraic elements of  $\mathfrak{K}$  whose degree goes into  $m$ . This is the theorem § 15, 5. in its extension to all absolutely algebraic fields of prime-number characteristic. From this it follows at once that the theorems 2., 3., 4., 8. of § 15 also hold generally in the domain of the absolutely algebraic fields of prime-number characteristic.

Let  $m$  and  $m'$  be two  $G$ -numbers,  $m$  divisible by  $m'$ . Then a field  $\mathfrak{E}_{p,m}$  contains a field  $\mathfrak{E}_{p,m'}$ . Now let  $\alpha$  be an element of  $\mathfrak{E}_{p,m}$ ,  $n$  its absolute degree. The absolute degree of the field  $\mathfrak{E}_{p,m'}(\alpha)$  is then, by 4., equal to the least common multiple  $v$  of  $m'$  and  $n$ . If now  $m'$  is finite, then  $v = [\mathfrak{E}_{p,m'}(\alpha) : \mathfrak{P}] = [\alpha : \mathfrak{E}_{p,m'}] \cdot m'$ ,  $[\alpha : \mathfrak{E}_{p,m'}] = \frac{v}{m'}$ , or finally

$$(9.) \quad [\alpha : \mathfrak{E}_{p,m'}] = \frac{n}{(n, m')},$$

where again  $(n, m')$  denotes the greatest common divisor of  $n$  and  $m'$ . But the same equation holds also when  $m'$  is not a natural number. For if in this case  $\nu$  denotes any natural number going into  $m'$ , then  $\mathfrak{E}_{p,m'}$  contains a subfield  $\mathfrak{E}_{p,\nu}$ , and by (9.) we have

$$[\alpha : \mathfrak{E}_{p,m'}] \leq [\alpha : \mathfrak{E}_{p,\nu}] = \frac{n}{(n, \nu)}.$$

On the other hand  $\nu$  can be so chosen that  $[\alpha : \mathfrak{E}_{p,m'}] = \frac{n}{(n, \nu)}$  holds. For the irreducible function  $f(x)$  from  $\mathfrak{E}_{p,m'}$  which has  $\alpha$  as a zero belongs to a *finite* field, namely the one which arises from  $\mathfrak{P}$  by adjunction of the coefficients of  $f(x)$ . If  $\nu$  is the degree of this field, then  $[\alpha : \mathfrak{E}_{p,m'}] = [\alpha : \mathfrak{E}_{p,\nu}] = \frac{n}{(n, \nu)}$ . Therefore  $[\alpha : \mathfrak{E}_{p,m'}]$  is equal to the minimum of the expression  $\frac{n}{(n, \nu)}$ , and this occurs when  $(n, \nu)$  reaches its maximum. Since  $\nu$  must be a divisor of  $m'$ , this cannot be  $> (n, m')$ , but this value is also reached, namely for  $\nu = (n, m')$ . Therefore the equation (9.) holds generally.

We now consider the fields  $\mathfrak{E}_{p,k}$  between  $\mathfrak{E}_{p,m'}$  and  $\mathfrak{E}_{p,m}$ . Every  $G$ -number  $k$  which is a multiple of  $m'$  and a divisor of  $m$  represents the degree of such a field. If this is finite with respect to  $\mathfrak{E}_{p,m'}$ , then it is also simple (§ 11, 5.; § 12, 5.). If, then,  $\alpha$  is an element that is primitive with respect to  $\mathfrak{E}_{p,m'}$  and belongs to  $\mathfrak{E}_{p,k}$ ,  $n$  its absolute degree, then by what precedes

$$[\mathfrak{E}_{p,k} : \mathfrak{E}_{p,m'}] = \frac{n}{(n, m')}.$$

If all fields  $\mathfrak{E}_{p,k}$  finite with respect to  $\mathfrak{E}_{p,m'}$  are taken into consideration, then  $n$  can be every natural number going into  $m$ . But the totality of all numbers of the form  $\frac{n}{(n, m')}$  is (as follows

at once from the definition given above of the quotient of two  $G$ -numbers) identical with the totality of all natural numbers going into  $\frac{m}{m'}$ , and therefore has  $\frac{m}{m'}$  as its least common multiple. If therefore  $\mathfrak{E}_{p,m}$  is finite with respect to  $\mathfrak{E}_{p,m'}$ , then  $\frac{m}{m'}$  is a natural number, and conversely; and in this case

$$[\mathfrak{E}_{p,m} : \mathfrak{E}_{p,m'}] = \frac{m}{m'}.$$

It will therefore be advisable to adopt this equation as the definition of the relative degree for the cases in which  $\frac{m}{m'}$  is not finite. If we now put for  $k$  all multiples of  $m'$  going into  $m$ , then  $\frac{k}{m'}$  represents all divisors of  $\frac{m}{m'}$ , and indeed each one once. From this we obtain:

5. *If  $\mathfrak{E}_{p,m'}$  is a subfield of  $\mathfrak{E}_{p,m}$ , then the degrees, taken with respect to  $\mathfrak{E}_{p,m'}$ , of the fields between  $\mathfrak{E}_{p,m'}$  and  $\mathfrak{E}_{p,m}$  are divisors of  $\frac{m}{m'}$ ; every divisor of  $\frac{m}{m'}$  represents the relative degree of one and only one such field.*

Let

$$m = \Pi q_i^{\varkappa_i},$$

$\varphi(x)$  an irreducible function in a field  $\mathfrak{E}_{p,m}$ ,  $n$  its degree. By adjunction of a zero of  $\varphi(x)$ ,  $\mathfrak{E}_{p,m}$  is extended to a field  $\mathfrak{E}_{p,\mu}$ , and  $n = \frac{\mu}{m}$ . From this it follows that  $n$  cannot contain a prime factor  $q_i$  whose exponent  $\varkappa_i$  in the decomposition of  $m$  is equal to  $\infty$ . If, on the other hand,  $n$  is a natural number which contains no such prime factor, then we can determine  $\mu$  so that  $\frac{\mu}{m} = n$  holds. A field  $\mathfrak{E}_{p,\mu}$  is then simple with respect to its subfield  $\mathfrak{E}_{p,m}$ , and every primitive element is a zero of a function of degree  $n$  irreducible in  $\mathfrak{E}_{p,m}$ . Hence:

6. *In a field  $\mathfrak{E}_{p,m}$  there are irreducible functions of all and only the (finite) degrees  $n$  that contain only prime factors  $q_i$  whose exponent  $\varkappa_i$  in*

$$m = \Pi q_i^{\varkappa_i}$$

*is finite.*

One more remark may find a place here. One can also present the investigations so far (and likewise the following ones) on algebraic extensions in *Kronecker's* form of expression with the help of modular systems, but one must then extend this concept by also taking into consideration integral functions with integer coefficients of infinitely many indeterminates. As such indeterminates we then have to interpret the elements  $j_1, j_2, \dots$  introduced above, while  $\varphi_n(x)$  and  $\psi_{d,n}(x)$  are to be regarded as integral functions with integer coefficients reduced mod.  $p$  of a further indeterminate  $x$ . Now let  $m$  again be an arbitrary  $G$ -number,  $r_1, r_2, \dots$  an associated sequence of natural numbers of the kind described earlier, and let  $\bar{\varphi}_n, \bar{\psi}_{n,n+1}$  be written for  $\varphi_{r_n}, \psi_{r_n, r_{n+1}}$ . Let further  $S$  denote the system of all integral functions with integer coefficients of the indeterminates  $j$  (this is of course to be understood so that each single element of  $S$  shall always contain only a finite number of these indeterminates),  $T$  the subsystem of  $S$  which consists of the functions

$$p; \quad \bar{\varphi}_1(j_1), \bar{\varphi}_2(j_2), \dots; \quad \bar{\psi}_{1,2}(j_2) - j_1, \bar{\psi}_{2,3}(j_3) - j_2, \dots$$

By  $T$  a “modular system  $M$ ” is defined. Two elements from  $S$  are called congruent modulo  $M$  if their difference is representable in the form

$$A_1 B_1 + A_2 B_2 + \dots + A_\nu B_\nu$$

where  $A_1, A_2, \dots, A_\nu$  are elements from  $S$  and  $B_1, B_2, \dots, B_\nu$  elements from  $T$ . Now every integral function with integer coefficients reduced mod.  $p$  of  $x$  whose degree goes into  $m$  breaks up mod.  $M$  in a definite way into linear factors whose coefficients are elements from  $S$ , and the residue classes of the modular system  $M$  within  $S$  form a field of the type  $\mathfrak{E}_{p,m}$ . If we take

$$m = \Pi q_i^\infty,$$

then every integral function of  $x$  whose coefficients belong to  $S$  breaks up mod.  $M$  into linear factors (see § 17.).

### § 17.

#### Algebraically closed fields.

In § 8. we have treated the problem: *In a field  $\mathfrak{K}$  an integral function  $f(x)$  is given; sought is an extension field  $\mathfrak{L}$  in which  $f(x)$  breaks up completely.* But we can now also set ourselves the essentially further-reaching problem of *finding an extension  $\mathfrak{L}$  of the field  $\mathfrak{K}$  in which every function from  $\mathfrak{K}$  breaks up.* The preceding section contains the solution of this problem for the case of the prime field  $\mathfrak{P}_p$ . Namely, if we put

$$m = \Pi q_i^\infty, \quad \mathfrak{E}_{p,m} = \mathfrak{A}_p,$$

then  $m$  is divisible by every natural number  $n$ , and therefore in  $\mathfrak{A}_p$  every irreducible and hence also every reducible function from  $\mathfrak{P}_p$  must break up completely.\*) But it can further be seen from § 16, 6. that in  $\mathfrak{A}_p$  only irreducible functions of degree 1 exist.  $\mathfrak{A}_p$  accordingly belongs to that particular kind of field that we (§ 7.) have called closed. These are naturally of the greatest importance for the question touched on here, and we therefore put together here some simple theorems relating to them.

1. *If  $\mathfrak{L}$  is an algebraic extension of a field  $\mathfrak{K}$  and if every integral function from  $\mathfrak{K}$  breaks up into linear factors in the field  $\mathfrak{L}$ , then  $\mathfrak{L}$  is algebraically closed.*

For let  $\varphi(x)$  be an irreducible function from  $\mathfrak{L}$ ,  $j$  a zero that  $\varphi(x)$  has in  $\mathfrak{L}$  or in an extension field of  $\mathfrak{L}$ . Then  $\mathfrak{L}(j)$  is algebraic with respect to  $\mathfrak{L}$ , hence also with respect to  $\mathfrak{K}$ , and  $j$  is a zero of an integral function  $f(x)$  from  $\mathfrak{K}$ . Since this breaks up into linear factors in  $\mathfrak{L}$ , but has the linear factor  $x - j$  in  $\mathfrak{L}(j)$ ,  $j$  is an element of  $\mathfrak{L}$ , consequently  $\varphi(x)$  is of degree 1, whereby Theorem 1. is proved.

Let  $\mathfrak{L}$  be an algebraically closed field,  $\mathfrak{K}$  a subfield of  $\mathfrak{L}$ ,  $\mathfrak{A}$  the field between  $\mathfrak{K}$  and  $\mathfrak{L}$  that comprises the elements algebraic with respect to  $\mathfrak{K}$ . An arbitrary function  $\varphi(x)$  from  $\mathfrak{A}$  then breaks up into linear factors in  $\mathfrak{L}$ , its zeros are algebraic with respect to  $\mathfrak{A}$ , hence also with respect to  $\mathfrak{K}$ , consequently elements of  $\mathfrak{A}$ . Thus  $\varphi(x)$  already breaks up completely in  $\mathfrak{A}$ , the field  $\mathfrak{A}$  is therefore algebraically closed. — If  $\mathfrak{T}$  is a field between  $\mathfrak{K}$  and  $\mathfrak{L}$ ,  $\alpha$  an element from  $\mathfrak{A}$ ,  $\psi(x)$  the irreducible function from  $\mathfrak{K}$  with the zero  $\alpha$ , then  $\psi(x)$  also belongs to the field  $\mathfrak{T}$ , and if  $\mathfrak{T}$  is algebraically closed, then  $\psi(x)$  breaks up into linear factors in  $\mathfrak{T}$ ,  $\alpha$  is an element, hence  $\mathfrak{A}$  a subfield of  $\mathfrak{T}$ . Thus  $\mathfrak{A}$  proves to be the *smallest* algebraically closed field between  $\mathfrak{K}$  and  $\mathfrak{L}$ , it is contained in all other such fields. If  $\mathfrak{L}$  itself is to be a smallest possible algebraically closed extension of  $\mathfrak{K}$ , then  $\mathfrak{L} = \mathfrak{A}$  must hold. Hence:

\*) L. E. Dickson speaks of such a field (Transactions of the American Math. Soc. 8 (1907), p. 389). But he defines it incorrectly as the totality of all *Galois* fields that belong to the prime number  $p$  (*Galois* field = finite field or type of such a one); a proof of existence is not supplied.

2. *In every extension  $\mathfrak{L}$  of a field  $\mathfrak{K}$  that represents an algebraically closed field, a smallest extension of this kind is contained; it is distinguished among all the others by the fact that it is algebraic.*

If in the preceding considerations we take for  $\mathfrak{K}$  the prime field  $\mathfrak{P}$  contained in  $\mathfrak{L}$ , then  $\mathfrak{A}$  becomes an absolutely algebraic field and consists of all absolutely algebraic elements of  $\mathfrak{L}$ . If the characteristic of  $\mathfrak{L}$  is a prime number  $p$ , then  $\mathfrak{A}$  also has this characteristic, and is therefore a field  $\mathfrak{E}_{p,m}$ . Since every irreducible function from  $\mathfrak{P}_p$  breaks up in  $\mathfrak{E}_{p,m}$ ,  $m$  must be divisible by every natural number, from which

$$m = \prod q_i^\infty, \quad \mathfrak{E}_{p,m} = \mathfrak{A}_p$$

follows. Hence:

3. *In every algebraically closed field  $\mathfrak{L}$  of characteristic  $p$  a field of the type  $\mathfrak{A}_p$  is contained; it consists of all absolutely algebraic elements of  $\mathfrak{L}$ .*

Something analogous holds for fields of characteristic 0. Appealing first to known facts, we remark that the field of all algebraic numbers is algebraically closed, and that it represents an algebraic extension of the field of rational numbers. For the latter type we use, as earlier, the sign  $\mathfrak{P}_0$ ; for the former we introduce the sign  $\mathfrak{A}_0$ . One usually arrives at the field of all algebraic numbers by regarding them as special complex numbers. But also without calling in the general complex numbers to help, one can arrive from  $\mathfrak{P}_0$  — as one arrives from  $\mathfrak{P}_p$  at  $\mathfrak{A}_p$  — at an absolutely algebraic and algebraically closed field, by defining an infinite sequence of fields

$$\mathfrak{K}_0 = \mathfrak{P}_0, \quad \mathfrak{K}_1, \quad \mathfrak{K}_2, \quad \dots$$

each single one of which comprises the preceding ones and is still finite with respect to  $\mathfrak{P}_0$ , and whose elements in their totality represent an algebraically closed field. Here too, using the principle of choice, one succeeds in proving that  $\mathfrak{A}_0$  is the only type of the required kind. Therefore Theorem 3. also holds for characteristic 0.

We do not enter further into these special investigations, but will rather prove quite generally *that every field  $\mathfrak{K}$  can be extended to an algebraically closed field, and that the problem of finding such an extension has essentially only one solution, if one further demands that the extension be as small as possible, or — which by 2. comes to the same thing — that it be algebraic.*

## § 18.

### Relations between systems of integral functions and extension fields.

<sup>E114</sup> In the investigations of this section we take an arbitrarily chosen field  $\mathfrak{K}$  as basis. We consider systems of integral functions of an indeterminate  $x$  with coefficients from  $\mathfrak{K}$ . Such functions are always meant when systems of functions are spoken of without qualification; likewise expressions like “extension field”, “normal function” etc. always refer to the ground field  $\mathfrak{K}$ .

If  $\mathfrak{L}$  is an extension field,  $S$  a system of finitely or infinitely many functions that break up completely in  $\mathfrak{L}$ , then  $\mathfrak{L}$  contains a definite extension  $\mathfrak{L}'$  that is just sufficient for the complete decomposition of the functions from  $S$ . Namely,  $\mathfrak{L}' = \mathfrak{K}(\mathfrak{T})$ , where  $\mathfrak{T}$  denotes the system of zeros that the functions of the system  $S$  have within  $\mathfrak{L}$ .

If  $S$  denotes any finite system of functions, then there are always (see the end of § 8) extension fields in which the functions from  $S$  break up completely. We now set up the definition:

*Definition 1.* A function  $\varphi(x)$  is called *subordinate to the finite system of functions  $S$*  if it likewise breaks up completely in every extension field in which the functions from  $S$  break up completely.

It follows at once:

1. *The function  $\varphi(x)$  is subordinate to the finite system  $S$  as soon as it likewise breaks up in some extension field  $\mathfrak{L}_1$  that is just sufficient for the complete breaking up of the system  $S$ .*

For if  $\mathfrak{L}_2$  is any second extension within which  $S$  breaks up completely, then  $\mathfrak{L}_2$  contains an extension  $\mathfrak{L}'_2$  that is just sufficient for the complete breaking up of  $S$ . By § 8, 2.  $\mathfrak{L}_1$  and  $\mathfrak{L}'_2$  are equivalent extensions, and since  $\varphi(x)$  breaks up completely in  $\mathfrak{L}_1$ , it does so also in  $\mathfrak{L}'_2$  and consequently in  $\mathfrak{L}_2$ .

Nothing would now stand in the way of letting Definition 1. hold also for the case that the system  $S$  consists of infinitely many functions, if it were already proved that in this case too extension fields exist in which the functions of  $S$  break up completely. As it is, however, we are dependent on another definition. We arrive at one by starting from the remark that in the case of a finite system  $S$  a function  $\varphi(x)$  that is subordinate to a subsystem of  $S$  is also subordinate to  $S$  itself.

*Definition 2.* A function  $\varphi(x)$  is called *subordinate to the infinite system  $S$*  if it is subordinate to some *finite* subsystem of  $S$ . — If  $S_1, S_2$  are any two systems of functions, we say  $S_1$  is *subordinate to  $S_2$*  if every function from  $S_1$  is subordinate to the system  $S_2$ .

The theorem then holds:

2. *If the system  $S_1$  is subordinate to the system  $S_2$ , and this to the system  $S_3$ , then  $S_1$  is subordinate to the system  $S_3$ .*

For an arbitrary function  $\varphi(x)$  from  $S_1$  is subordinate to a finite subsystem  $S'_2$  of  $S_2$ , this to a finite subsystem  $S'_3$  of  $S_3$  (Def. 2.). Since  $S'_3$  is finite, there exist extensions within which all functions of  $S'_3$  break up completely. In every such extension the functions of  $S'_2$  break up, hence  $\varphi(x)$  also breaks up completely (Def. 1.). Consequently  $\varphi(x)$  is subordinate to the system  $S'_3$ , hence also to the system  $S_3$ , whereby 2. is proved.

*Definition 3.* Two systems of functions are called *equivalent* if each is subordinate to the other.

From the preceding definitions and theorems it follows at once that every system of functions is equivalent to itself; that two systems of functions that are equivalent to a third are equivalent to one another, that every system of finitely many functions is equivalent to the product of these functions.

*Definition 4.* A system of functions  $S$  shall be called *complete* if every function subordinate to  $S$  belongs to  $S$ .

If  $S$  is an arbitrary system, then a system  $S'$ , if it is to be complete and equivalent to  $S$ , must contain only such functions as are subordinate to  $S$ , but also all of these. On the other hand one sees at once that the system of all functions subordinate to  $S$  is in fact equivalent to  $S$  and complete. Thus every system  $S$  is equivalent to exactly *one* complete system. The *smallest* complete system is evidently formed by the functions that break up completely in

$\mathfrak{K}$  itself, the *greatest* by the totality of all functions from  $\mathfrak{K}$ . Further it is evident that the intersection of two complete systems, or also of an arbitrary system of finitely or infinitely many complete systems, is again a complete system.

These theorems are followed by some others that express relations between systems of functions and their associated decomposition fields. First there follows from the preceding definitions and theorems without further ado:

3. *If  $\mathfrak{L}$  is an extension of  $\mathfrak{K}$ ,  $S$  a system of functions that breaks up completely in  $\mathfrak{L}$ , then every system  $S'$  subordinate to  $S$  also breaks up completely in  $\mathfrak{L}$ , and if  $S$  and  $S'$  are equivalent and the extension  $\mathfrak{L}$  is just sufficient for the complete breaking up of  $S$ , then it is also just sufficient for the complete breaking up of  $S'$ .*

This theorem shows that, in questions about the existence and the properties of such extensions in which a given system of functions breaks up, the system may be replaced by any equivalent one.

We prove further:

4. *If the extension  $\mathfrak{N}$  is just sufficient to decompose the system of functions  $S$  completely, then it is normal, and every function that breaks up completely in  $\mathfrak{N}$  is subordinate to the system  $S$ .*

Proof: Let  $\mathfrak{T}$  be the system of those elements from  $\mathfrak{N}$  that are zeros of functions from  $S$ . Then it follows from our hypothesis that  $\mathfrak{N} = \mathfrak{K}(\mathfrak{T})$ . Now let  $\varphi(x)$  denote any irreducible function from  $\mathfrak{K}$  that has a zero  $\alpha$  in  $\mathfrak{N}$ . Then one can specify a finite subsystem  $\mathfrak{T}'$  of  $\mathfrak{T}$  such that  $\alpha$  already belongs to the field  $\mathfrak{K}(\mathfrak{T}')$ , and, because  $\mathfrak{T}'$  is finite, a finite subsystem  $S'$  of  $S$  such that the elements from  $\mathfrak{T}'$  are zeros of functions from  $S'$ . If  $\mathfrak{T}''$  denotes the system of all zeros of the functions from  $S'$ , then the extension field  $\mathfrak{N}' = \mathfrak{K}(\mathfrak{T}'')$  also contains the element  $\alpha$  and is just sufficient to decompose the functions from  $S'$  completely. Therefore  $\mathfrak{N}'$ , because  $S'$  is a finite system, is normal with respect to  $\mathfrak{K}$  by § 8, 6., and the function  $\varphi(x)$  must therefore break up completely in  $\mathfrak{N}'$  and hence in  $\mathfrak{N}$ . This shows, however, that the algebraic extension  $\mathfrak{N} = \mathfrak{K}(\mathfrak{T})$  is likewise normal. Next, from the circumstance that  $\varphi(x)$  likewise breaks up in the field  $\mathfrak{N}'$ , which is just sufficient for the complete breaking up of the finite system  $S'$ , it follows that  $\varphi(x)$  is subordinate to the system  $S'$  (Theorem 1.).  $\varphi(x)$  is accordingly also subordinate to  $S$ . If finally  $f(x)$  is any function that breaks up completely in  $\mathfrak{N}$ , then by the preceding every irreducible factor of  $f(x)$  is subordinate to the system  $S$ ; therefore the same holds of  $f(x)$  itself. This proves Theorem 4. — It follows from this that, once the existence of an extension field in which  $S$  breaks up completely is established for a system  $S$ , the two Definitions 1. and 2. come to the same thing for that system  $S$ .

5. *The totality  $S$  of all functions that break up completely in an extension field  $\mathfrak{N}$  represents a complete system, and if the extension is normal, then it is just sufficient for the complete breaking up of  $S$ .*

For a function  $\varphi(x)$  that is subordinate to  $S$  must break up completely in  $\mathfrak{N}$ , hence belongs to  $S$ , i.e. the system  $S$  is complete. If further  $\mathfrak{T}$  denotes the system of elements of  $\mathfrak{N}$  that are zeros of functions from  $S$ , then the extension  $\mathfrak{K}(\mathfrak{T})$  contained in  $\mathfrak{N}$  is just sufficient for the breaking up of  $S$ . Now if  $\mathfrak{N}$  is normal, hence also algebraic, then every element  $\alpha$  from  $\mathfrak{N}$  is a zero of a function  $\varphi(x)$  irreducible in  $\mathfrak{K}$  that breaks up completely in  $\mathfrak{N}$ , hence belongs to

$S$ . Therefore  $\alpha$  is an element of  $\mathfrak{T}$ , consequently of  $\mathfrak{K}(\mathfrak{T})$ , and  $\mathfrak{N} = \mathfrak{K}(\mathfrak{T})$  holds, whereby 5. is proved.

We conclude these investigations with the proof of the theorem:

6. *Every system of functions  $S$  is equivalent to a system of normal functions.*

Proof: (Cf. § 13, 3.). Let  $S$  first consist of a single irreducible function  $\varphi(x)$ , and let  $\mathfrak{N}$  denote an extension that is just sufficient for the complete decomposition of  $\varphi(x)$ . Then  $\mathfrak{N}$  is a normal field. If  $\mathfrak{N}$  has a primitive element  $\alpha$ , then the function  $\psi(x)$  irreducible in  $\mathfrak{K}$  that has  $\alpha$  as a zero is normal and equivalent to  $\varphi(x)$ . If  $\mathfrak{N}$  has no primitive element, then  $\mathfrak{K}$  must be an imperfect field and  $\varphi(x)$  must have an exponent  $f > 0$  (§ 13, 7.). Let

$$\varphi(x) = x^{np^f} + a_1 x^{(n-1)p^f} + \cdots + a_n.$$

Then, in the field  $\mathfrak{N}$  in which it breaks up, the function  $\varphi(x)$  is the  $p^f$ -th power of another function

$$\chi(x) = (x - \gamma_1) \cdots (x - \gamma_n) = x^n + b_1 x^{n-1} + \cdots + b_n,$$

and from  $\varphi(x) = (\chi(x))^{p^f}$  it follows that

$$a_k = b_k^{p^f}. \quad (k = 1, \dots, n)$$

$\varphi(x)$  has the zeros  $\gamma_1, \gamma_2, \dots, \gamma_n$ , while the function

$$\bar{\varphi}(x) = x^n + a_1 x^{n-1} + \cdots + a_n,$$

which is an irreducible function of the first kind, has the zeros  $\gamma_1^{p^f}, \gamma_2^{p^f}, \dots, \gamma_n^{p^f}$ . These are different from one another, and hence so are  $\gamma_1, \gamma_2, \dots, \gamma_n$ . From  $a_k = b_k^{p^f}$  it follows that  $x^{p^f} - a_k = (x - b_k)^{p^f}$ . The irreducible function from  $\mathfrak{K}$  with the zero  $b_k$  therefore has the form

$$(x - b_k)^{p^{f_k}} \quad (0 \leq f_k \leq f; k = 1, \dots, n)$$

and is a normal function. The field  $\mathfrak{N}' = \mathfrak{K}(\gamma_1^{p^f}, \gamma_2^{p^f}, \dots, \gamma_n^{p^f})$ , which is just sufficient for the complete breaking up of  $\bar{\varphi}(x)$ , is normal, contained in  $\mathfrak{N}$ , and represents a finite extension of the first kind of  $\mathfrak{K}$ . Hence  $\mathfrak{N}'$  has primitive elements. Let  $\alpha$  be one such and  $\bar{\psi}(x)$  the irreducible function from  $\mathfrak{K}$  with the zero  $\alpha$ . Then  $\bar{\psi}(x)$  is a normal function equivalent to  $\bar{\varphi}(x)$ . The system  $T$  of the normal functions

$$\bar{\psi}(x), (x - b_1)^{p^{f_1}}, (x - b_2)^{p^{f_2}}, \dots, (x - b_n)^{p^{f_n}}$$

passes into an equivalent  $T'$  if we replace  $\bar{\psi}(x)$  by  $\bar{\varphi}(x)$ . All these functions break up completely in  $\mathfrak{N}$ , and are therefore subordinate to the function  $\varphi(x)$ . A field  $\mathfrak{M}$  between  $\mathfrak{K}$  and  $\mathfrak{N}$  that suffices for the complete breaking up of the system  $T'$  must contain the elements  $b_1, b_2, \dots, b_n$ , hence the function  $\chi(x)$ , and further the zeros  $\gamma_k^{p^f}$  of  $\bar{\varphi}(x)$ , and hence also the functions  $x^{p^f} - \gamma_k^{p^f} = (x - \gamma_k)^{p^f}$ . Hence the functions

$$(\chi(x), (x - \gamma_k)^{p^f}) = x - \gamma_k$$

are also contained in  $\mathfrak{M}$ , and therefore so are the elements  $\gamma_k$ ; and since  $\mathfrak{N} = \mathfrak{K}(\gamma_1, \gamma_2, \dots, \gamma_n)$ , it follows that  $\mathfrak{M} = \mathfrak{N}$ , hence the equivalence of  $\varphi(x)$  and  $T'$ , and finally the equivalence of  $\varphi(x)$  and the system of normal functions  $T$ .

This settles Theorem 6. for the case that  $S$  consists of a single irreducible function. Now let  $S$  be an arbitrary system of functions,  $S'$  the system of all irreducible factors of the functions occurring in  $S$ , and  $S''$  the system of all normal functions subordinate to  $S'$ . Then, first,  $S$  is equivalent to  $S'$ , and  $S''$  is subordinate to the system  $S'$ . Since, further, every function from  $S'$  is, by the foregoing, equivalent to a system of normal functions, and that system is a subsystem of  $S''$ , it follows that  $S'$  and  $S''$  are equivalent, and  $S$  is equivalent to the system of normal functions  $S''$ .

### § 19.

#### Auxiliary considerations from set theory.

<sup>E 115</sup> By Theorem 5. of the preceding section there corresponds to every normal extension of a field  $\mathfrak{K}$  a class of equivalent systems of functions for whose breaking up the extension is just sufficient, and, as one sees at once, the same class of systems corresponds to every equivalent extension. The proof that, conversely, there corresponds to every class of systems one, and — apart from equivalent ones — only one, normal extension makes it necessary to draw on considerations from set theory as well, and in particular cannot be carried out completely without use of the principle of choice. <sup>E 116</sup> We therefore give here a short compilation of some concepts and theorems from the named discipline that are used in what follows.

1. *Ordered sets.* — A set or a system of elements is called *ordered*, after *G. Cantor*, if a stipulation has been made according to which, of any two different elements  $a, b$ , the one, say  $a$ , counts as the earlier (smaller), the other  $b$  as the later (greater); in symbols:

$$a < b \text{ or } b > a.$$

The stipulation must, however, be such that  $a < c$  always follows from  $a < b, b < c$ .

2. *Cut.* — If the elements of an ordered set  $M$  are divided into two subsets  $A, B$  in such a way that every element of  $M$  belongs to one and only one of these subsets, and that all elements of  $A$  are earlier than all of  $B$ , then such a division is called a *cut* (*Dedekind*), the subset  $A$  is called *segment*,  $B$  *remainder* (*Cantor*).

3. *Order types.* — By a *similar map* of two ordered sets  $M$  and  $N$  we understand a one-to-one correspondence between their elements in which the earlier of two elements from  $M$  always corresponds, in  $N$ , again to the earlier of the two assigned elements. Ordered sets that admit such a map are called *similar* or *of the same order type* (*Cantor*).

4. *Well-ordered sets.* — A set  $M$  is called *well-ordered* (*Cantor*) if a stipulation has been made according to which, of any two elements  $a, b$ , the one counts as the earlier, the other as the later, and if this stipulation is such that both  $M$  and every subset of  $M$  contain a *first* element, i.e. one that is earlier than every other element of the set or subset respectively. — *Every well-ordered set is at the same time an ordered one*; for if  $a < b, b < c$ , then  $a = c$  cannot be, because the cases  $a < b, b < a$  exclude one another; nor can  $c < a$  be, because otherwise the set consisting of the elements  $a, b, c$  would contain no first element; hence  $a < c$ . — The well-ordered sets also include the ordered finite sets; these are characterized by the fact that in them every subset also has a last element.

5. *Ordinal numbers.* — The order types of well-ordered sets are called *ordinal numbers*, the ordinal numbers of finite sets are denoted by  $1, 2, 3, \dots$  — If  $M$  and  $N$  are well-ordered sets, then one of the three mutually exclusive cases always holds:

- a)  $M$  and  $N$  are similar; there is then one and only one similar correspondence between  $M$  and  $N$ ;
- b)  $M$  is similar to a definite segment of  $N$ ;
- c)  $N$  is similar to a definite segment of  $M$ .

In the first case  $M$  and  $N$  have the same ordinal number; in the second the ordinal number of  $M$  is called *smaller*, in the third *greater* than that of  $N$ . It is expedient also to introduce an ordinal number 0, which counts as the smallest of all. <sup>E 117</sup>

Every system of ordinal numbers represents, if they are ordered according to ascending magnitude, a well-ordered set, and in particular all the ordinal numbers incl. 0 that are smaller than an ordinal number  $\sigma$  ( $\sigma > 0$ ) form a well-ordered set that itself has the ordinal number  $\sigma$ . If we therefore have a well-ordered set of the ordinal number  $\sigma$ , it is advisable to represent its elements by a sign with index:

$$a_0, a_1, a_2, \dots, a_\nu, \dots,$$

where the index  $\nu$  runs through all ordinal numbers  $0 \leq \nu < \sigma$ . To every ordinal number  $\nu$  (for  $0 < \nu < \sigma$ ) there then corresponds a definite segment of the well-ordered system that has precisely the ordinal number  $\nu$ . It is formed by all elements that precede  $a_\nu$ ; we therefore also call it the *segment determined by  $a_\nu$* . — For the purpose of simple presentation we make the following stipulations: A well-ordered system of elements  $a_\nu$  is denoted by

$$\{a_\nu\} \text{ or more precisely } \{a_\nu\} \quad (0 \leq \nu < \sigma)$$

where  $\sigma$  indicates the ordinal number of the system, or also by a mere letter, say  $A$ . In the latter case, by  $A_\nu$  ( $0 < \nu < \sigma$ ) we always understand the segment of  $A$  determined by  $a_\nu$ , while we set  $A_\sigma = A$ .

Among the ordinal numbers different from 0, those of the *first* and *second kind* are to be distinguished. An ordinal number  $\alpha$  is called of the first or second kind according as a well-ordered set of the ordinal number  $\alpha$  contains a last element or not. Since the system of all ordinal numbers below  $\alpha$  itself has the ordinal number  $\alpha$ , there is, if  $\alpha$  is of the first kind, an ordinal number  $\beta$  that immediately precedes  $\alpha$ . We put  $\beta = \alpha - 1$ ,  $\alpha = \beta + 1$ . If  $\alpha$  is of the second kind, then there is no immediately preceding ordinal number. These ordinal numbers are also called limit numbers. The reason for this designation becomes clear from the following consideration: Let  $S$  be a system of ordinal numbers of the property that there is no greatest among them, hence each is exceeded by other numbers of the same system (e.g. the system of all finite or of all even finite ordinal numbers). Let further  $T$  denote the system of all those ordinal numbers that are exceeded by some ordinal number from  $S$ . Then it is evident that  $S$  is contained in  $T$ , that  $T$  also contains no greatest number, and that, if  $\sigma$  is any ordinal number from  $T$ , every ordinal number  $< \sigma$  also belongs to  $T$ . The system  $T$  itself has an ordinal number  $\tau$ , which is a limit number. Now if  $\sigma > 0$  is any element of  $T$ , then the ordinal numbers that are  $< \sigma$  form a segment of  $T$  whose ordinal number is smaller than the ordinal number of  $T$ . I.e.,  $\sigma < \tau$ . On the other hand every ordinal number  $< \tau$  must belong to  $T$ . For if the system  $T$  were only a part of the system  $T'$  of all ordinal numbers  $< \tau$ , then the numbers from  $T'$  belonging to  $T$  would precede those not belonging to  $T$ , i.e.  $T$  would be

a segment of  $T'$ , and the ordinal number  $\tau$  of  $T$  would be smaller than that of  $T'$ , whereas  $T'$ , as the system of all ordinal numbers  $< \tau$ , must after all have the ordinal number  $\tau$ . Thus  $T$  consists of all and only the ordinal numbers  $< \tau$ , and according to the definition of  $T$ ,  $\tau$  now represents the smallest ordinal number that is exceeded by no ordinal number of the system  $S$ . Such a number therefore exists for every system of ordinal numbers that has no maximum, and by analogy with ordinary usage it would have to be called the *upper limit* of  $S$ . Every limit number  $\tau$  is, among other things, the upper limit of all ordinal numbers  $< \tau$ .

6. *Complete induction and the well-ordering theorem.* — If a certain statement relating to ordinal numbers holds for an ordinal number  $\alpha$ , does not hold for another  $\beta > \alpha$ , and  $T$  denotes the system of those ordinal numbers between  $\alpha$  and  $\beta$  (inclusive of  $\alpha$  and  $\beta$ ) for which the statement does not hold, then  $T$ , as a well-ordered set, has a first element  $\gamma$ , and  $\gamma$  is then the smallest ordinal number  $> \alpha$  for which the statement does not hold. Hence, in the area of ordinal numbers, we have the *theorem of complete induction*:<sup>E 118</sup> *If some theorem holds for the ordinal number  $\alpha$  and if we can prove that it must hold for the ordinal number  $\beta > \alpha$  as soon as it is correct for all ordinal numbers that are  $< \beta$  and  $\geq \alpha$ , then the theorem holds for all ordinal numbers  $\geq \alpha$ .* The significance of the ordinal numbers for the applications rests on the theorem of complete induction. *But their extensive applicability is opened up by the theorem of Zermelo<sup>\*)</sup>, according to which every set is capable of well-ordering.* The theorem naturally concerns only the *existence* of the well-ordering; it gives no method of actually carrying it out for every arbitrarily given set.

## § 20.

### The immediate applications.

*Definition 1. Progressive systems of functions.* — Let  $\mathfrak{K}_0$  be an arbitrary field. A well-ordered system  $S = \{f_\nu(x)\}$  of integral functions from  $\mathfrak{K}_0$  shall be called a *progressive* one (with respect to  $\mathfrak{K}_0$ ) if  $f_0(x)$  does not break up completely in  $\mathfrak{K}_0$  and none of the remaining functions  $f_\nu(x)$  is subordinate (§ 18) to the segment of  $S$  determined by it.

1. *If  $S$  is a well-ordered system of integral functions from  $\mathfrak{K}_0$  which do not all break up completely in  $\mathfrak{K}_0$ , then  $S$  contains a progressive subsystem  $S'$  which is equivalent to  $S$ .*

For if we form a subsystem  $S'$  of  $S$  in such a way that we take the first function  $f_0(x)$  into  $S'$  if it does not break up completely in  $\mathfrak{K}_0$ , and every other function if it is not subordinate to the segment of  $S$  determined by it, then it is clear, first, that the first function from  $S$  not breaking up completely in  $\mathfrak{K}_0$  belongs to  $S'$ , further that the system  $S'$  is progressive and subordinate to the system  $S$ . It therefore remains only to show that every function from  $S = \{f_\nu(x)\}$  is subordinate to the system  $S'$ . This holds, first of all, for  $f_0(x)$ , since  $f_0(x)$  either breaks up completely in  $\mathfrak{K}_0$  or belongs to  $S'$ . In order to show the same for every other function  $f_\nu(x)$ , we apply complete induction. Then it is to be regarded as proved that the segment of  $S$  determined by  $f_\nu(x)$  is subordinate to the system  $S'$ . If  $f_\nu(x)$  is subordinate to this segment, then  $f_\nu(x)$  is subordinate also to  $S'$ ; but if  $f_\nu(x)$  is not subordinate to the designated segment, then  $f_\nu(x)$  belongs to  $S'$ , and is therefore likewise subordinate to this system.

*Definition 2. Progressive systems of elements of an extension field.* — Let  $\mathfrak{K}_0$  be an arbitrary field,  $\mathfrak{L}$  any extension of  $\mathfrak{K}_0$ ,  $\mathfrak{S} = \{a_\nu\}$  a well-ordered system of elements from  $\mathfrak{L}$ .

<sup>\*)</sup> E. Zermelo, Math. Ann. vol. 59 (1904), p. 514.

The system  $\mathfrak{S}$  shall be called a *progressive* one if neither  $a_0$  belongs to the field  $\mathfrak{K}_0$ , nor any one of the remaining elements  $a_\nu$  belongs to the field that arises from  $\mathfrak{K}_0$  by adjunction of the segment determined by  $a_\nu$ . — The following theorem holds:

2. If  $\mathfrak{S} = \{a_\nu\}$  is a well-ordered system of elements of an extension field  $\mathfrak{L}$  of  $\mathfrak{K}_0$  and if not all elements from  $\mathfrak{S}$  belong to  $\mathfrak{K}_0$ , then  $\mathfrak{S}$  contains a progressive subsystem  $\mathfrak{S}'$  for which  $\mathfrak{K}_0(\mathfrak{S}') = \mathfrak{K}_0(\mathfrak{S})$  holds. We can form  $\mathfrak{S}'$  by taking the element  $a_0$  into  $\mathfrak{S}'$  if it does not belong to  $\mathfrak{K}_0$ , and every other element  $a_\nu$  if it does not belong to the field that arises from  $\mathfrak{K}_0$  by adjunction of the segment of  $\mathfrak{S}$  determined by  $a_\nu$ .

The proof is entirely analogous to that of Theorem 1., and can therefore be passed over. Since  $\mathfrak{L}$  itself can be obtained by adjunction of a system  $\mathfrak{S}$  and this is capable of well-ordering, it further follows:

3. Every extension of a field can be obtained by adjunction of a progressive system.

*Definition 3. Well-ordered fields.* — We can think of the elements of a field  $\mathfrak{K}_0$  as brought into a well-ordered sequence  $\{c_\nu\}$  ( $0 \leq \nu < \sigma$ ). With this arrangement a definite ordinal number  $\sigma$  then belongs to the field  $\mathfrak{K}_0$ . We wish, however, also to make the express stipulation that, whenever we speak of a well-ordered field  $\mathfrak{K}_0 = \{c_\nu\}$ ,  $c_0 = 0$ ,  $c_1 = \varepsilon$  shall always hold. If two well-ordered fields have the same ordinal number, then there exists between them a single well-determined similar correspondence (§ 19, 5.). If this is at the same time an isomorphic one, then we call the fields *similar-isomorphic*.

4. If  $\{\mathfrak{K}_\mu\}$  ( $0 \leq \mu < \sigma$ ) is a well-ordered sequence of well-ordered fields,  $\sigma$  a limit number, and if of any two fields of this sequence the earlier is always similar-isomorphic to a segment of the later, then there are well-ordered fields  $\mathfrak{L}$  such that every field  $\mathfrak{K}_\mu$  is similar-isomorphic to a segment of  $\mathfrak{L}$ , and such that for every element of  $\mathfrak{L}$  a segment can be given that contains this element and is similar-isomorphic to a field  $\mathfrak{K}_\mu$ . All fields  $\mathfrak{L}$  that have the designated properties are similar-isomorphic to one another.

*Proof.* Let the field  $\mathfrak{K}_\mu$  of the sequence  $\{\mathfrak{K}_\mu\}$  have the ordinal number  $\tau_\mu$ , and let its elements in their well-ordered sequence be denoted by  $c_{\mu\nu}$  ( $0 \leq \nu < \tau_\mu$ ). From our hypotheses it follows that the numbers  $\tau_\mu$  increase with  $\mu$  and that there is no greatest among them. We denote by  $\tau$  the upper limit of the numbers  $\tau_\mu$  (§ 19, 5.):

$$\tau = \lim_{\mu \rightarrow \sigma} \tau_\mu$$

and take a well-ordered system  $\mathfrak{L} = \{c_\lambda\}$  ( $0 \leq \lambda < \tau$ ) for which we stipulate addition and multiplication in the following manner: If  $c_\lambda, c_\varrho$  ( $\lambda \leq \varrho$ ) are any two elements from  $\mathfrak{L}$ , then it follows from  $\varrho < \tau$  that some of the ordinal numbers  $\tau_\mu$  of the fields  $\mathfrak{K}_\mu$  are  $> \varrho$ . Among these let  $\tau_{\mu'}$  be the smallest. The field  $\mathfrak{K}_{\mu'} = \{c_{\mu'\nu}\}$  ( $0 \leq \nu < \tau_{\mu'}$ ) then contains two elements  $c_{\mu'\lambda}, c_{\mu'\varrho}$  as well as their sum and their product. If

$$(1.) \quad c_{\mu'\lambda} + c_{\mu'\varrho} = c_{\mu'\alpha}, \quad c_{\mu'\lambda} \cdot c_{\mu'\varrho} = c_{\mu'\beta},$$

then  $\alpha < \tau_{\mu'} < \tau$ ,  $\beta < \tau_{\mu'} < \tau$ ; the system  $\mathfrak{L}$  therefore contains two elements  $c_\alpha, c_\beta$ . We stipulate that

$$(2.) \quad c_\lambda + c_\varrho = c_\varrho + c_\lambda = c_\alpha, \quad c_\lambda \cdot c_\varrho = c_\varrho \cdot c_\lambda = c_\beta$$

shall hold, whereby  $\mathfrak{L}$  becomes a system with double composition.

If now  $\mathfrak{K}_\mu$  is any field of the sequence  $\{\mathfrak{K}_\mu\}$ , then it follows from  $\tau_\mu < \tau$  that  $\mathfrak{L}$  has a segment  $\mathfrak{L}_\mu$  of the ordinal number  $\tau_\mu$ . In the similar correspondence  $\pi_\mu$  between  $\mathfrak{K}_\mu$  and  $\mathfrak{L}_\mu$  the elements  $c_{\mu\lambda}$  and  $c_\lambda$  ( $0 \leq \lambda < \tau_\mu$ ) correspond to one another. If now  $c_\lambda$  and  $c_\varrho$  ( $\lambda \leq \varrho$ ) are any two elements of  $\mathfrak{L}_\mu$  and if their sum and their product are given by the equations (2.), then  $\varrho < \tau_\mu$ , and therefore, if again  $\tau_{\mu'}$  is the smallest number from the sequence  $\{\tau_\mu\}$  that exceeds  $\varrho$ ,

$$(3.) \quad \tau_{\mu'} \leq \tau_\mu, \quad \mu' \leq \mu.$$

From the stipulations made for the compositions in  $\mathfrak{L}$  it follows that the equations (2.) entail the equations (1.). From (3.) it follows that  $\mathfrak{K}_{\mu'}$  is either identical with  $\mathfrak{K}_\mu$  or similar-isomorphic to a segment of  $\mathfrak{K}_\mu$ . In both cases it follows from (1.) that

$$(4.) \quad c_{\mu\lambda} + c_{\mu\varrho} = c_{\mu\alpha}, \quad c_{\mu\lambda} \cdot c_{\mu\varrho} = c_{\mu\beta}.$$

Since the elements  $c_{\mu\alpha}, c_{\mu\beta}$  again belong to the field  $\mathfrak{K}_\mu$ , we have  $\alpha < \tau_\mu, \beta < \tau_\mu$ ; the elements  $c_\alpha, c_\beta$  therefore again belong to the segment  $\mathfrak{L}_\mu$  of  $\mathfrak{L}$ . Further, the comparison of (2.) and (4.) shows that the similar correspondence  $\pi_\mu$  between  $\mathfrak{K}_\mu$  and  $\mathfrak{L}_\mu$  is an isomorphic one.  $\mathfrak{L}_\mu$  therefore represents a field similar-isomorphic to  $\mathfrak{K}_\mu$ . Since for every element  $c_\lambda$  of  $\mathfrak{L}$  we can find  $\tau_\mu > \lambda$ , every element of  $\mathfrak{L}$  occurs in a field  $\mathfrak{L}_\mu$ , and since of any two of these fields one contains the other,  $\mathfrak{L}$  itself is a field. As was shown, this field meets the conditions of Theorem 4.

If  $\mathfrak{L}' = \{c'_\lambda\}$  is likewise a field that meets these conditions,  $\tau'$  its ordinal number,  $\mathfrak{L}'_\mu$  the segment similar-isomorphic to  $\mathfrak{K}_\mu$ , then the ordinal number of  $\mathfrak{L}'_\mu$  is equal to  $\tau_\mu$ , hence  $\tau_\mu < \tau'$ . If on the other hand  $\lambda$  is any ordinal number  $< \tau'$ , then  $\mathfrak{L}'$  contains an element  $c'_\lambda$ ; this occurs in a segment  $\mathfrak{L}'_\mu$ , hence  $\lambda < \tau_\mu$ . Consequently  $\tau' = \lim_{\mu=\sigma} \tau_\mu = \tau$ , and there exists between  $\mathfrak{L}$  and  $\mathfrak{L}'$  a similar correspondence  $\pi$  that assigns to every element  $c_\lambda$  of  $\mathfrak{L}$  the element  $c'_\lambda$  of  $\mathfrak{L}'$ . If now for any two elements  $c_\lambda, c_\varrho$  ( $\lambda \leq \varrho$ ) of  $\mathfrak{L}$  the equations of composition (2.) hold and if we choose  $\mu$  so large that  $\tau_\mu > \varrho$ , then the field  $\mathfrak{L}_\mu$  contains the elements  $c_\lambda, c_\varrho$ , hence also  $c_\alpha$  and  $c_\beta$ . The fields  $\mathfrak{L}_\mu$  and  $\mathfrak{L}'_\mu$  are similar-isomorphic to  $\mathfrak{K}_\mu$ , hence also to one another. But the similar correspondence between  $\mathfrak{L}_\mu$  and  $\mathfrak{L}'_\mu$  assigns to the elements  $c_\lambda, c_\varrho, c_\alpha, c_\beta$  of  $\mathfrak{L}_\mu$  the elements  $c'_\lambda, c'_\varrho, c'_\alpha, c'_\beta$  of  $\mathfrak{L}'_\mu$ . Since this correspondence is at the same time isomorphic, it follows that

$$c'_\lambda + c'_\varrho = c'_\alpha, \quad c'_\lambda \cdot c'_\varrho = c'_\beta,$$

hence also the similar correspondence  $\pi$  that exists between  $\mathfrak{L}$  and  $\mathfrak{L}'$  proves to be an isomorphic one, and so Theorem 4. is completely proved.

*Definition 4. Well-ordering of the integral functions in a well-ordered field.* — If  $\mathfrak{K}_0 = \{c_\nu\}$  ( $c_0 = 0, c_1 = \varepsilon$ ) is a well-ordered field and if  $g(x)$  and  $h(x)$  are two integral functions from  $\mathfrak{K}_0$  different from one another, then we think of these as written in the form of infinite series

$$\begin{aligned} g(x) &= c_{\mu_0} + c_{\mu_1}x + c_{\mu_2}x^2 + \cdots, \\ h(x) &= c_{\nu_0} + c_{\nu_1}x + c_{\nu_2}x^2 + \cdots \end{aligned}$$

Then, as soon as the natural number  $n$  exceeds a certain value,

$$c_{\mu_n} = c_{\nu_n} = 0 = c_0, \quad \mu_n = \nu_n = 0$$

will hold. If  $k (\geq 0)$  is the greatest number for which  $\mu_k \neq \nu_k$ , then in the case  $\mu_k < \nu_k$  we say that the function  $g(x)$  precedes the function  $h(x)$  within  $\mathfrak{K}_0$ . By this stipulation the system of the integral functions from  $\mathfrak{K}_0$  is converted into a well-ordered one. For if  $S$  is an arbitrary system of integral functions from  $\mathfrak{K}_0$ , then, because  $c_0 = 0$ , the functions of smallest degree in  $S$  will precede the others. If  $n$  is this degree,  $S_n$  the subsystem of  $S$  which comprises the functions of degree  $n$ ,  $S_{n-1}$  the system of the functions from  $S_n$  in which the coefficient  $c_\nu$  of  $x^n$  has an index  $\nu$  as small as possible,  $S_{n-2}$  the system of those functions from  $S_{n-1}$  in which the coefficient of  $x^{n-1}$  has an index as small as possible, etc., finally  $f(x)$  that function from  $S_0$  in which the term free of  $x$  has an index as small as possible, then  $f(x)$  is the first function from  $S$ . But the existence of a first function within every system of functions  $S$  proves the asserted well-ordering.

*Definition 5. Primitive well-ordering.* — Let  $\mathfrak{K}_0 = \{c_\nu\}$  be a well-ordered field,  $\mathfrak{K}_1$  a simple algebraic extension of degree  $n$  ( $n > 1$ ) of  $\mathfrak{K}_0$ ,  $j$  a primitive element of  $\mathfrak{K}_1$ . Every element of  $\mathfrak{K}_1$  is then represented uniquely in the form  $g(j)$ , where  $g(x)$  denotes an arbitrary integral function from  $\mathfrak{K}_0$  of degree  $< n$ . If for any two elements  $g(j)$  and  $h(j)$  we stipulate that  $g(j)$  counts as the earlier if the function  $g(x)$  precedes the function  $h(x)$  within  $\mathfrak{K}_0$ , then it is clear by the foregoing that  $\mathfrak{K}_1$  is thereby made into a well-ordered field. From  $c_0 = 0$  it follows that the well-ordered field  $\mathfrak{K}_0$  represents a segment of the well-ordered field  $\mathfrak{K}_1$ ; from  $c_1 = \varepsilon$ , that  $j$  is the first element following the segment  $\mathfrak{K}_0$ . We say:  $\mathfrak{K}_1$  is *primitively ordered with respect to  $\mathfrak{K}_0$* , and call  $j$  the *principal element* of the primitive well-ordering. — The following theorem then holds:

5. If  $\mathfrak{K}_1$  is a simple algebraic extension of a well-ordered field  $\mathfrak{K}_0$ ,  $j$  a primitive element, then  $\mathfrak{K}_1$  can, in one and only one way, be primitively ordered with respect to  $\mathfrak{K}_0$  so that  $j$  becomes the principal element.  $\mathfrak{K}_0$  is then the segment of  $\mathfrak{K}_1$  determined by  $j$ .

*Definition 6. Regular well-ordering.* — Let  $\mathfrak{K}_0$  be a well-ordered field,  $\mathfrak{L}$  an arbitrary algebraic extension of  $\mathfrak{K}_0$ . We wish to assume that  $\mathfrak{L}$ , too, is well-ordered, and that this well-ordering has the properties described in the following: Both the field  $\mathfrak{K}_0$  and every field that arises from  $\mathfrak{K}_0$  by adjunction of a segment of  $\mathfrak{L}$  shall be a *segment* of  $\mathfrak{L}$ , provided it does not comprise all the elements of  $\mathfrak{L}$ . The segments of  $\mathfrak{L}$  thus obtained — evidently all those segments containing  $\mathfrak{K}_0$  that are at the same time fields — may be called *principal segments*; the element immediately following a principal segment we call the (*associated*) *principal element*. The principal elements form a (well-ordered) subset  $\mathfrak{J} = \{j_\nu\}$  ( $0 \leq \nu < \sigma$ ) of  $\mathfrak{L}$ .  $\mathfrak{K}_0$  is the principal segment determined by  $j_0$ ; we wish in general to denote by  $\mathfrak{K}_\nu$  ( $0 \leq \nu < \sigma$ ) the principal segment determined by  $j_\nu$ , and by  $\mathfrak{K}_\sigma$  the field  $\mathfrak{L}$  itself. — From the hypotheses so far it follows that every field  $\mathfrak{K}_\nu(j_\nu)$  ( $0 \leq \nu < \sigma$ ) likewise represents a principal segment (or is equal to  $\mathfrak{K}_\sigma = \mathfrak{L}$ ). We now make the further hypothesis that  $\mathfrak{K}_\nu(j_\nu)$  proves to be primitively ordered with respect to  $\mathfrak{K}_\nu$ . Here, therefore,  $j_\nu$  will appear as the principal element of the primitive ordering. — If the well-ordered field  $\mathfrak{L}$  has all these properties, then we call it *regularly ordered with respect to  $\mathfrak{K}_0$* . — The primitive well-ordering accordingly represents the simplest case of the regular one, characterized by  $\sigma = 1$ .

From the preceding definitions some facts result immediately, which we therefore record without proof, namely:

6. If the field  $\mathfrak{L} = \mathfrak{K}_\sigma$  is regularly ordered with respect to  $\mathfrak{K}_0$  and if  $\mathfrak{K}_\nu$  ( $0 < \nu < \sigma$ ) represents a principal segment, then  $\mathfrak{K}_\nu$  is regularly ordered with respect to  $\mathfrak{K}_0$ , and  $\mathfrak{L}$  is

regularly ordered with respect to  $\mathfrak{K}_\nu$ . If here  $\mathfrak{J} = \{j_\mu\}$  ( $0 \leq \mu < \sigma$ ) is the system of the principal elements of  $\mathfrak{L}$  with respect to  $\mathfrak{K}_0$ ,  $\mathfrak{J}'$  the segment of  $\mathfrak{J}$  determined by  $j_\nu$ ,  $\mathfrak{J}''$  the associated remainder, then  $\mathfrak{J}'$  represents the system of the principal elements of  $\mathfrak{K}_\nu$  with respect to  $\mathfrak{K}_0$ , and  $\mathfrak{J}''$  the system of the principal elements of  $\mathfrak{L}$  with respect to  $\mathfrak{K}_\nu$ .

7. If  $\mathfrak{L}$  is regularly ordered with respect to  $\mathfrak{K}_0$ , and  $\mathfrak{M}$  with respect to  $\mathfrak{L}$ , then  $\mathfrak{M}$  is regularly ordered with respect to  $\mathfrak{K}_0$  and  $\mathfrak{L}$  is a principal segment of  $\mathfrak{M}$ .

Let us retain the notations from Def. 6., and let us understand by  $\mathfrak{L}'$  any field between  $\mathfrak{K}_0$  and  $\mathfrak{L}$ . Let  $\mathfrak{L}'$  be different from  $\mathfrak{L}$ ,  $a$  the first element of  $\mathfrak{L}$  not belonging to  $\mathfrak{L}'$ ,  $\mathfrak{A}$  the segment of  $\mathfrak{L}$  determined by  $a$ . Then  $\mathfrak{L}'$  contains the field  $\mathfrak{K}_0(\mathfrak{A})$ , which by Def. 6. is a principal segment of  $\mathfrak{L}$ . But since  $\mathfrak{K}_0(\mathfrak{A})$  contains the segment  $\mathfrak{A}$ , but not the element  $a$  following it,  $a$  must be a principal element. If therefore  $\mathfrak{L}'$  is to contain all principal elements, then  $\mathfrak{L}' = \mathfrak{L}$  must hold, and thus it follows that  $\mathfrak{K}_0(\mathfrak{J}) = \mathfrak{L}$ . If we further denote by  $\mathfrak{J}_\nu$  ( $0 < \nu < \sigma$ ) the segment of  $\mathfrak{J}$  determined by the principal element  $j_\nu$  and put  $\mathfrak{L}' = \mathfrak{K}_0(\mathfrak{J}_\nu)$ , then  $\mathfrak{L}'$  is part of  $\mathfrak{K}_\nu$ , since  $\mathfrak{K}_\nu$  contains the system  $\mathfrak{J}_\nu$ . Since further  $j_\nu$  does not occur in  $\mathfrak{K}_\nu$ , hence also not in  $\mathfrak{L}'$ , and the first element  $a$  of  $\mathfrak{L}$  not contained in  $\mathfrak{L}'$  must be a principal element, it follows that  $a = j_\nu$ ,  $\mathfrak{L}' = \mathfrak{K}_\nu = \mathfrak{K}_0(\mathfrak{J}_\nu)$ . Taking Def. 2. into account, we thus obtain:

8. If the field  $\mathfrak{L}$  is regularly ordered with respect to  $\mathfrak{K}_0$ , then the principal elements form a progressive system  $\mathfrak{J}$ , we have  $\mathfrak{L} = \mathfrak{K}_0(\mathfrak{J})$ , and the principal segment of  $\mathfrak{L}$  determined by the principal element  $j_\nu$  is obtained from  $\mathfrak{K}_0$  by adjunction of the segment of  $\mathfrak{J}$  determined by  $j_\nu$ .

Retaining the notation so far, let  $a$  be any element of  $\mathfrak{L}$ ,  $\mathfrak{K}_\nu$  ( $0 \leq \nu \leq \sigma$ ) the first principal segment of  $\mathfrak{L}$  containing  $a$ , or, if there is none such, the field  $\mathfrak{L} = \mathfrak{K}_\sigma$  itself. If  $\nu > 0$ , then it follows from  $\mathfrak{K}_\nu = \mathfrak{K}_0(\mathfrak{J}_\nu)$  that there must be a finite subsystem  $\mathfrak{S}$  of  $\mathfrak{J}_\nu$  such that the element  $a$  occurs also in  $\mathfrak{K}_0(\mathfrak{S})$ . If  $j_\mu$  is the last element of  $\mathfrak{S}$ , then  $\mu < \nu$ . Further, there can be no ordinal number  $\varrho$  for which  $\mu < \varrho < \nu$ . Otherwise  $\mathfrak{S}$  would be part of  $\mathfrak{J}_\varrho$  and  $a$  an element of  $\mathfrak{K}_0(\mathfrak{J}_\varrho) = \mathfrak{K}_\varrho$ , contrary to the assumption made about  $\mathfrak{K}_\nu$ . Consequently  $\nu = \mu + 1$ , and we have the theorem:

9. If  $\{\mathfrak{K}_\nu\}$  ( $0 \leq \nu < \sigma$ ) is the system of the principal segments of the field  $\mathfrak{L} = \mathfrak{K}_\sigma$  regularly ordered with respect to  $\mathfrak{K}_0$ , and  $\mathfrak{K}_\nu$  the first field from the sequence  $\{\mathfrak{K}_\nu\}$  ( $0 \leq \nu \leq \sigma$ ) that contains an arbitrarily given element  $a$  from  $\mathfrak{L}$ , then  $\nu$  cannot be a limit number.

From this it follows easily:

10. The regular well-ordering of a field  $\mathfrak{L}$  is completely determined by the well-ordering of the ground field  $\mathfrak{K}_0$  and the well-ordered system  $\mathfrak{J} = \mathfrak{J}_\sigma = \{j_\nu\}$  ( $0 \leq \nu < \sigma$ ) of the principal elements.

For suppose we had two different regular well-orderings of  $\mathfrak{L}$ . Let us denote these by  $\mathfrak{L}' = \{c'_\lambda\}$  and  $\mathfrak{L}'' = \{c''_\lambda\}$ , by  $\mathfrak{K}'_\nu, \mathfrak{K}''_\nu$  ( $0 \leq \nu < \sigma$ ) their principal segments, which correspond to the segments  $\mathfrak{J}_\nu$  of the system  $\mathfrak{J}$ , and let us put  $\mathfrak{L}' = \mathfrak{K}'_\sigma$ ,  $\mathfrak{L}'' = \mathfrak{K}''_\sigma$ . Then, if we disregard the order of the elements, the fields  $\mathfrak{K}'_\nu, \mathfrak{K}''_\nu$  are of course identical, namely equal to  $\mathfrak{K}_0(\mathfrak{J}_\nu)$ . But if the equality sign is used to express agreement in the arrangement as well, then in any case  $\mathfrak{K}'_\sigma \neq \mathfrak{K}''_\sigma$ , while  $\mathfrak{K}'_0 = \mathfrak{K}_0 = \mathfrak{K}''_0$ . Now let  $c'_\lambda$  be the first element from  $\mathfrak{L}'$  that no longer has the same index within  $\mathfrak{L}''$ , and  $\mathfrak{K}'_\nu$  the first field of the sequence  $\{\mathfrak{K}'_\nu\}$  ( $0 < \nu \leq \sigma$ ) that contains the element  $c'_\lambda$ . Then  $\nu > 0$ , and by 9.  $\nu$  is not a limit number. We have  $\mathfrak{K}'_\nu \neq \mathfrak{K}''_\nu$ ,

on the other hand  $\mathfrak{K}'_{\nu-1} = \mathfrak{K}''_{\nu-1}$ . But since, by the prescriptions of the regular well-ordering,  $\mathfrak{K}'_{\nu} = \mathfrak{K}'_{\nu-1}(j_{\nu-1})$  must be primitively ordered with respect to  $\mathfrak{K}'_{\nu-1}$ , and  $\mathfrak{K}''_{\nu} = \mathfrak{K}''_{\nu-1}(j_{\nu-1})$  with respect to  $\mathfrak{K}''_{\nu-1} = \mathfrak{K}'_{\nu-1}$ , and in both cases  $j_{\nu-1}$  is the principal element, it follows from 5. that  $\mathfrak{K}'_{\nu} = \mathfrak{K}''_{\nu}$ , and we obtain a contradiction. Thus 10. is proved.

11. *If  $\mathfrak{L}$  is an algebraic extension of the well-ordered field  $\mathfrak{K}_0$ ,  $\mathfrak{J} = \mathfrak{J}_{\sigma} = \{j_{\nu}\}$  ( $0 \leq \nu < \sigma$ ) a progressive system of elements from  $\mathfrak{L}$ ,  $\mathfrak{K}_0(\mathfrak{J}) = \mathfrak{L}$ , then there is one and only one regular well-ordering of  $\mathfrak{L}$  with respect to  $\mathfrak{K}_0$  with  $\mathfrak{J}$  as system of principal elements.*

That there cannot be more than one well-ordering of the designated kind is already stated by Theorem 10. That there is one at all is expressed in the case  $\sigma = 1$  by Theorem 5. For  $\sigma > 1$  we carry out the proof by induction. — If  $\sigma$  is not a limit number, then we first order the field  $\mathfrak{K}_{\sigma-1} = \mathfrak{K}_0(\mathfrak{J}_{\sigma-1})$  regularly with respect to  $\mathfrak{K}_0$ , and in such a way that  $\mathfrak{J}_{\sigma-1}$  becomes the system of the principal elements; then we order  $\mathfrak{L} = \mathfrak{K}_0(\mathfrak{J}) = \mathfrak{K}_{\sigma-1}(j_{\sigma-1})$  primitively with respect to  $\mathfrak{K}_{\sigma-1}$ , with  $j_{\sigma-1}$  as the principal element. The field  $\mathfrak{L}$  thus ordered then satisfies by 6., 7. the conditions of the problem. — If  $\sigma$  is a limit number, then we first have for every  $\nu < \sigma$  a field  $\mathfrak{K}_{\nu} = \mathfrak{K}_0(\mathfrak{J}_{\nu})$  which is regularly ordered with respect to  $\mathfrak{K}_0$  and has the system of principal elements  $\mathfrak{J}_{\nu}$ . If  $\mu < \nu < \sigma$ , then the field  $\mathfrak{K}_0(\mathfrak{J}_{\mu})$  occurs as a principal segment of  $\mathfrak{K}_{\nu}$ , is by 6., 7. regularly ordered with respect to  $\mathfrak{K}_0$ , and has the system of principal elements  $\mathfrak{J}_{\mu}$ . By 10. that segment agrees with  $\mathfrak{K}_{\mu}$  also in the order of the elements. Each of the fields in the sequence  $\{\mathfrak{K}_{\nu}\}$  ( $0 \leq \nu < \sigma$ ) is therefore a segment of all the later ones. From this, and because the sequence  $\{\mathfrak{K}_{\nu}\}$  contains no last field, one sees at once that these fields in their totality constitute a well-ordered field  $\mathfrak{L}'$  of which they are all segments. Since  $\mathfrak{J}$  contains no last element, every element of  $\mathfrak{J}$  occurs in a segment  $\mathfrak{J}_{\nu}$ , hence in a field  $\mathfrak{K}_{\nu}$ , consequently in  $\mathfrak{L}'$ ;  $\mathfrak{L}'$  therefore comprises all elements of  $\mathfrak{K}_0(\mathfrak{J}) = \mathfrak{L}$ , and thus represents a well-ordering of the field  $\mathfrak{L}$ . If  $\mathfrak{A}$  is any segment of  $\mathfrak{L}'$ ,  $a$  the element of  $\mathfrak{L}'$  following this segment,  $\mathfrak{K}_{\nu}$  a field from the sequence  $\{\mathfrak{K}_{\nu}\}$  containing  $a$ , then  $\mathfrak{K}_0(\mathfrak{A})$  is a principal segment of  $\mathfrak{K}_{\nu}$ , hence a field  $\mathfrak{K}_{\mu}$  ( $\mu < \nu$ ). By adjunction of a segment of  $\mathfrak{L}'$ , a segment of  $\mathfrak{L}'$  therefore always arises again from  $\mathfrak{K}_0$ , and the segments thus obtained are the fields of the sequence  $\{\mathfrak{K}_{\nu}\}$  ( $0 \leq \nu < \sigma$ ). These therefore form the only principal segments of  $\mathfrak{L}'$ , and the elements from  $\mathfrak{J}$ , since they follow these segments, the principal elements. Since none of them is last,  $\mathfrak{K}_{\nu}(j_{\nu})$  is always again a field of the sequence  $\{\mathfrak{K}_{\nu}\}$  ( $0 \leq \nu < \sigma$ ), as such regularly ordered with respect to  $\mathfrak{K}_0$ , hence primitively ordered with respect to  $\mathfrak{K}_{\nu}$ . Thus  $\mathfrak{L}'$  represents a regular well-ordering of  $\mathfrak{L}$  with respect to  $\mathfrak{K}_0$ , with  $\mathfrak{J}$  as system of principal elements.

From 11., in combination with 3., the following results:

12. *Every algebraic extension of a well-ordered field can be regularly ordered with respect to it.*

## § 21.

### The fundamental theorem of algebraic extensions.

*Definition 1. Principal functions and principal factors of the regular well-ordering.* — Let  $\mathfrak{N} = \mathfrak{K}_{\sigma}$  be an algebraic extension of the well-ordered field  $\mathfrak{K}_0$  and regularly ordered with respect to  $\mathfrak{K}_0$ ,  $\mathfrak{J} = \mathfrak{J}_{\sigma} = \{j_{\nu}\}$  ( $0 \leq \nu < \sigma$ ) the system of principal elements,  $\mathfrak{K}_{\nu}$  respectively  $\mathfrak{J}_{\nu}$  the principal segment of  $\mathfrak{N}$  respectively segment of  $\mathfrak{J}$  determined by  $j_{\nu}$ . The element  $j_{\nu}$  is a zero of a definite irreducible function  $f_{\nu}(x)$  from  $\mathfrak{K}_0$  (with  $\varepsilon$  as coefficient of the highest power), likewise a zero of a definite irreducible function  $\varphi_{\nu}(x)$  of the field  $\mathfrak{K}_{\nu}$ , which can be

equal to  $f_\nu(x)$  and for  $\nu = 0$  is always equal to  $f_\nu(x)$ , but in every case is a factor of  $f_\nu(x)$ . We thus arrive at two systems of functions

$$F_\sigma = F = \{f_\nu(x)\}, \quad \Phi_\sigma = \Phi = \{\varphi_\nu(x)\} \quad (0 \leq \nu < \sigma).$$

We call the functions  $f_\nu(x)$  *principal functions*, the functions  $\varphi_\nu(x)$  *principal factors of the regular well-ordering*, and denote the segment of  $F$  respectively  $\Phi$  determined by  $f_\nu(x)$  respectively  $\varphi_\nu(x)$  ( $\nu \geq 1$ ) by  $F_\nu$  respectively  $\Phi_\nu$ .\*) — With reference to this notation, the following now results easily:

1. *If all principal functions are normal (with respect to  $\mathfrak{K}_0$ ), then the regularly ordered field  $\mathfrak{N} = \mathfrak{K}_\sigma$  is itself normal. It is just sufficiently large to break up the system  $F$  of principal functions completely; likewise every principal segment  $\mathfrak{K}_\nu$  is normal and just suffices for the breaking up of  $F_\nu$ . The system  $F$  is progressive.*

For since each of the normal functions  $f_\varrho(x)$  ( $0 \leq \varrho < \nu$ ) from  $F_\nu$  ( $0 < \nu \leq \sigma$ ) has a zero  $j_\varrho$  in the field  $\mathfrak{K}_\nu = \mathfrak{K}_0(j_\nu)$ , it must break up completely in  $\mathfrak{K}_\nu$ , and since the field  $\mathfrak{K}_\nu$  arises from  $\mathfrak{K}_0$  only through adjunction of zeros of the functions from  $F_\nu$ , it just suffices for the breaking up of  $F_\nu$ , and is therefore normal. Since further, in the case  $\nu < \sigma$ ,  $\mathfrak{K}_\nu$  no longer contains the element  $j_\nu$ , and the function  $f_\nu(x)$  therefore does not break up completely in  $\mathfrak{K}_\nu$ ,  $F$  is a progressive system.

*Definition 2. Normal well-ordering.* — Let  $\mathfrak{N}$  denote a normal extension of the well-ordered field  $\mathfrak{K}_0$ ; let  $\mathfrak{N}$  be regularly ordered with respect to  $\mathfrak{K}_0$ , and let the principal functions all be normal. If we use the letters in the same meaning as before, then  $j_\nu$  ( $0 \leq \nu < \sigma$ ) is a zero of the irreducible function  $\varphi_\nu(x)$  from  $\mathfrak{K}_\nu$ , and  $\varphi_\nu(x)$  is a factor of the function  $f_\nu(x)$  irreducible in  $\mathfrak{K}_0$ . Since  $\mathfrak{K}_\nu$  is a well-ordered field, the functions within  $\mathfrak{K}_\nu$ , too, have a definite arrangement, by Def. 4., § 20. This therefore also holds of the irreducible factors that  $f_\nu(x)$  has within  $\mathfrak{K}_\nu$ . Let us now assume that every function  $\varphi_\nu(x)$ , in so far as it is not the only irreducible factor of  $f_\nu(x)$  within  $\mathfrak{K}_\nu$ , precedes the remaining irreducible factors of  $f_\nu(x)$  within  $\mathfrak{K}_\nu$ . If this hypothesis is fulfilled, then we say:  $\mathfrak{N}$  is normally ordered with respect to  $\mathfrak{K}_0$ . The normal well-ordering is therefore a special case of the regular one.

*Definition 3. Distinguished zeros of the principal functions that belong to a normal well-ordering.* — Let  $\mathfrak{N}$  be a normal and normally ordered extension of the well-ordered field  $\mathfrak{K}_0$ , and let the signs used so far keep their meaning. Since the principal function  $f_\nu(x)$  is normal with respect to  $\mathfrak{K}_0$ , the field  $\mathfrak{K}_\nu(j_\nu)$  can be obtained by adjoining to  $\mathfrak{K}_\nu$  any zero of  $f_\nu(x)$ . All these zeros are primitive elements of the field  $\mathfrak{K}_\nu(j_\nu)$  with respect to  $\mathfrak{K}_\nu$ ; their degree is equal to the degree of the principal factor  $\varphi_\nu(x)$ , which is in any case greater than 1. In the case of imperfect fields the zeros of  $\varphi_\nu(x)$  need not all be different. If we therefore assume that  $\varphi_\nu(x)$  has  $r$  different zeros  $j_\nu, j'_\nu, \dots, j_\nu^{(r-1)}$  and is of degree  $n$ , then  $n \geq r \geq 1, n > 1$ . If now  $i_\nu$  is any zero of  $f_\nu(x)$  (in the field  $\mathfrak{N}$ ), then we obtain all elements of the field  $\mathfrak{K}_\nu(j_\nu)$  by replacing  $x$  by  $i_\nu$  in all integral functions  $g(x)$  from  $\mathfrak{K}_\nu$  whose degree is smaller than  $n$ . Among these functions there are therefore  $r$  that for  $x = i_\nu$  pass into zeros of  $\varphi_\nu(x)$ . By Def. 4., § 20, these  $r$  functions have a definite order within  $\mathfrak{K}_\nu$ . If  $\psi(x)$  is the first among them and if  $\psi(i_\nu) = j_\nu$ ,

\*) In order to avoid misunderstandings, we further point out that the functions  $f_\nu(x)$  within  $F$  have a definite order (designated by the index), which naturally has nothing to do with the order that was given to the functions in  $\mathfrak{K}_0$  on the basis of § 20, Def. 4.

then we call  $i_\nu$  a *distinguished zero* of  $f_\nu(x)$ . (We use this designation also when  $r = 1$ , which can occur only with imperfect fields.) The following theorem holds:

2. *The principal element  $j_\nu$  is a distinguished zero of  $f_\nu(x)$ , and among the zeros of the principal factor  $\varphi_\nu(x)$  there is no other distinguished one.*

For since the zeros  $j_\nu, j'_\nu, \dots, j_\nu^{(r-1)}$  of  $\varphi_\nu(x)$  do not occur in  $\mathfrak{K}_\nu$ , the  $r$  functions from  $\mathfrak{K}_\nu$  that for  $x = i_\nu$  pass into these zeros are all at least of degree 1. From the circumstance that the well-ordered field  $\mathfrak{K}_\nu$  begins with the elements  $0, \varepsilon$ , it follows that among all functions from  $\mathfrak{K}_\nu$  whose degree is  $\geq 1$ ,  $x$  is the first. If we therefore choose for  $i_\nu$  one of the zeros of  $\varphi_\nu(x)$ , then  $x$  is the first function from  $\mathfrak{K}_\nu$  that for  $x = i_\nu$  passes into a zero of  $\varphi_\nu(x)$ . But this is equal to  $j_\nu$  if and only if we choose  $i_\nu = j_\nu$ , which proves the assertion. — From 2. there it further follows:

3. *In the case  $\varphi_\nu(x) = f_\nu(x)$ , hence in any case for  $\nu = 0$ ,  $j_\nu$  is the only distinguished zero of  $f_\nu(x)$ .*

We now prove:

4. *If  $\mathfrak{N} = \mathfrak{K}_0(\bar{\mathfrak{J}})$  is a normal extension of the well-ordered field  $\mathfrak{K}_0$ , if every element  $i_\nu$  of the system  $\bar{\mathfrak{J}}_\sigma = \bar{\mathfrak{J}} = \{i_\nu\}$  ( $0 \leq \nu < \sigma$ ) is a zero of a normal function  $f_\nu(x)$  from  $\mathfrak{K}_0$ , and if the system of functions  $F_\sigma = F = \{f_\nu(x)\}$  is a progressive one (or, what here amounts to the same: if the system  $\bar{\mathfrak{J}}$  is a progressive one), then the field  $\mathfrak{N}$  can be normally ordered with respect to  $\mathfrak{K}_0$  in one and only one way in such a manner that  $F$  represents the system of principal functions and the elements  $i_\nu$  become distinguished zeros of the associated principal functions  $f_\nu(x)$ .*

We first show that there cannot be two different normal orderings of the designated kind. Let us assume that there were two such normal orderings  $\mathfrak{N}'$  and  $\mathfrak{N}''$  of the field  $\mathfrak{N}$ . We denote by  $\mathfrak{J}'_\sigma = \mathfrak{J}' = \{j'_\nu\}$ ,  $\{\mathfrak{K}'_\nu\}$ ,  $\Phi'_\sigma = \Phi' = \{\varphi'_\nu(x)\}$  the systems of principal elements, principal segments, principal factors of  $\mathfrak{N}'$ , by  $\mathfrak{J}''_\sigma = \mathfrak{J}'' = \{j''_\nu\}$ ,  $\{\mathfrak{K}''_\nu\}$ ,  $\Phi''_\sigma = \Phi'' = \{\varphi''_\nu(x)\}$  the corresponding systems for  $\mathfrak{N}''$ . By  $\bar{\mathfrak{J}}_\nu, F_\nu, \mathfrak{J}'_\nu, \mathfrak{J}''_\nu, \Phi'_\nu, \Phi''_\nu$  let the segments of  $\bar{\mathfrak{J}}, F$  etc. determined by  $i_\nu, f_\nu(x)$  etc. be denoted. Then  $\mathfrak{K}'_\nu, \mathfrak{K}''_\nu$  represent two normal orderings of the same field  $\mathfrak{K}_0(\bar{\mathfrak{J}}_\nu) = \mathfrak{K}_0(\mathfrak{J}'_\nu) = \mathfrak{K}_0(\mathfrak{J}''_\nu)$ , which just suffices for the breaking up of the system  $F_\nu$ . Since  $i_0$  is to be a distinguished element of  $f_0(x)$ , by 3.  $j'_0 = i_0 = j''_0$ . If the equation  $j'_\nu = j''_\nu$  does not hold for every index, then we take the smallest for which  $j'_\nu \neq j''_\nu$ . Then  $\mathfrak{J}'_\nu = \mathfrak{J}''_\nu$ , and since  $\mathfrak{J}'_\nu$  and  $\mathfrak{J}''_\nu$  represent the systems of principal elements of the fields  $\mathfrak{K}'_\nu, \mathfrak{K}''_\nu$  regularly ordered with respect to  $\mathfrak{K}_0$ , we have (even taking the arrangement into account)  $\mathfrak{K}'_\nu = \mathfrak{K}''_\nu$  (§ 20, 10.). From this it further follows that  $\varphi'_\nu(x) = \varphi''_\nu(x)$ , because  $\varphi'_\nu(x)$  respectively  $\varphi''_\nu(x)$  represents the first irreducible factor of  $f_\nu(x)$  within  $\mathfrak{K}'_\nu = \mathfrak{K}''_\nu$ . If further within  $\mathfrak{K}'_\nu = \mathfrak{K}''_\nu$   $\psi(x)$  is the first function that for  $x = i_\nu$  becomes a zero of  $\varphi'_\nu(x) = \varphi''_\nu(x)$ , then, because  $i_\nu$  is to be a distinguished zero of  $f_\nu(x)$ , we obtain  $j'_\nu = \psi(i_\nu) = j''_\nu$ , in contradiction with the assumption  $j'_\nu \neq j''_\nu$ . Consequently  $\mathfrak{J}' = \mathfrak{J}''$ , and from this it follows, by § 20, 10., that  $\mathfrak{N}' = \mathfrak{N}''$ .

We now have to show that a normal ordering of the required kind exists. — For  $\sigma = 1$  we obtain it by ordering  $\mathfrak{N}$  primitively with respect to  $\mathfrak{K}_0$  with  $i_0$  as principal element. For  $\sigma > 1$  the proof is to be carried out by induction. If  $\sigma$  is not a limit number, then let  $\mathfrak{K}_{\sigma-1}$  denote that normal ordering of the field  $\mathfrak{K}_0(\bar{\mathfrak{J}}_{\sigma-1})$  for which  $F_{\sigma-1}$  represents the system of principal functions and every element  $i_\nu$  ( $\nu < \sigma - 1$ ) becomes a distinguished zero of  $f_\nu(x)$ . If then within the well-ordered field  $\mathfrak{K}_{\sigma-1}$   $\varphi_{\sigma-1}(x)$  is the first irreducible factor of  $f_{\sigma-1}(x)$ ,  $\psi(x)$  the

first function that for  $x = i_{\sigma-1}$  becomes a zero of  $\varphi_{\sigma-1}(x)$ , then we put  $\psi(i_{\sigma-1}) = j_{\sigma-1}$  and order  $\mathfrak{N}$  primitively with respect to  $\mathfrak{K}_{\sigma-1}$  with  $j_{\sigma-1}$  as principal element. Then we have, as is at once evident, the required normal ordering. — If  $\sigma$  is a limit number, then for every  $\nu < \sigma$  let  $\mathfrak{K}_\nu$  represent that normal ordering of the field  $\mathfrak{K}_0(\bar{\mathfrak{J}}_\nu)$  for which  $F_\nu$  is the system of principal functions, while every element  $i_\mu$  ( $\mu < \nu$ ) becomes a distinguished zero of  $f_\mu(x)$ . Then a simple consideration shows that every field of the sequence  $\{\mathfrak{K}_\nu\}$  ( $0 \leq \nu < \sigma$ ) is a segment of all later ones, and that the totality of the elements occurring in these fields yields a well-ordering of  $\mathfrak{N}$  that meets all conditions of the problem.

5. If  $\mathfrak{K}_0$  and  $\bar{\mathfrak{K}}_0$  are similar-isomorphic fields, if  $\mathfrak{N} = \mathfrak{K}_\sigma$  is a normal and normally ordered extension of  $\mathfrak{K}_0$ ,  $\bar{\mathfrak{N}} = \bar{\mathfrak{K}}_\sigma$  one of the same kind, of  $\bar{\mathfrak{K}}_0$ , if  $F = \{f_\nu(x)\}$ ,  $\bar{F} = \{\bar{f}_\nu(x)\}$  ( $0 \leq \nu < \sigma$ ) are the associated systems of principal functions, and if by the similar-isomorphic correspondence  $\pi_0$  existing between  $\mathfrak{K}_0$  and  $\bar{\mathfrak{K}}_0$  the functions  $f_\nu(x)$  and  $\bar{f}_\nu(x)$  are assigned to one another, then  $\mathfrak{N}$  and  $\bar{\mathfrak{N}}$  are similar-isomorphic.

Proof by induction: If  $\sigma = 1$ ,  $n$  the degree of  $f_0(x)$  and  $\bar{f}_0(x)$ , and if  $j_0, \bar{j}_0$  are the principal elements, then we obtain all elements of  $\mathfrak{N}$  respectively  $\bar{\mathfrak{N}}$  by replacing  $x$  by  $j_0$  respectively  $\bar{j}_0$  in all functions  $g(x)$ ,  $\bar{g}(x)$  from  $\mathfrak{K}_0$  respectively  $\bar{\mathfrak{K}}_0$  whose degree is smaller than  $n$ . The functions  $g(x)$  have a definite order in  $\mathfrak{K}_0$ , and so do the functions  $\bar{g}(x)$  in  $\bar{\mathfrak{K}}_0$ , and from the circumstance that  $\pi_0$  represents a similar correspondence between  $\mathfrak{K}_0$  and  $\bar{\mathfrak{K}}_0$  it results at once that the correspondence between the functions from  $\mathfrak{K}_0$  and  $\bar{\mathfrak{K}}_0$  mediated by  $\pi_0$  is also a similar one. Further it follows from § 20, Def. 5., that we obtain a similar correspondence  $\pi_1$  comprising  $\pi_0$  between  $\mathfrak{N} = \mathfrak{K}_0(j_0)$  and  $\bar{\mathfrak{N}} = \bar{\mathfrak{K}}_0(\bar{j}_0)$  if we let the element  $\bar{g}(\bar{j}_0)$  from  $\bar{\mathfrak{N}}$  correspond to every element  $g(j_0)$  from  $\mathfrak{N}$ , where  $\bar{g}(x)$  denotes the function from  $\bar{\mathfrak{K}}_0$  corresponding in the correspondence  $\pi_0$  to the function  $g(x)$  from  $\mathfrak{K}_0$ . Since further  $\pi_0$  represents an isomorphism, it follows, as in § 8, 1., that the correspondence  $\pi_1$ , too, is isomorphic at the same time. — If  $\sigma > 1$  and if we denote by  $\mathfrak{K}_\nu, \bar{\mathfrak{K}}_\nu$  ( $\nu < \sigma$ ) the principal segments of  $\mathfrak{N}$  respectively  $\bar{\mathfrak{N}}$ , then  $\mathfrak{K}_\nu$  and  $\bar{\mathfrak{K}}_\nu$  represent normal and normally ordered extensions of  $\mathfrak{K}_0$  and  $\bar{\mathfrak{K}}_0$  whose principal functions are carried over into one another by  $\pi_0$ , and we may regard it as proved that  $\mathfrak{K}_\nu$  and  $\bar{\mathfrak{K}}_\nu$  are similar-isomorphic, i.e. that the only similar correspondence  $\pi_\nu$  existing between  $\mathfrak{K}_\nu$  and  $\bar{\mathfrak{K}}_\nu$  is at the same time isomorphic. If  $\mu < \nu < \sigma$ , then  $\mathfrak{K}_\mu$  and  $\bar{\mathfrak{K}}_\mu$  are similar segments of  $\mathfrak{K}_\nu$  respectively  $\bar{\mathfrak{K}}_\nu$ , and are therefore mapped similarly onto each other by  $\pi_\nu$  just as by  $\pi_\mu$ . The correspondence  $\pi_\mu$  therefore forms a part of  $\pi_\nu$ . If  $\sigma$  is a limit number, so that every element of  $\mathfrak{N}$  respectively  $\bar{\mathfrak{N}}$  occurs in a field  $\mathfrak{K}_\nu$  respectively  $\bar{\mathfrak{K}}_\nu$ , it follows from this that a one-to-one map  $\pi_\sigma$  of  $\mathfrak{N}$  onto  $\bar{\mathfrak{N}}$  is produced by the correspondences  $\pi_\nu$ . A simple consideration shows that the map  $\pi_\sigma$  is a similar one, because this is the case with the maps  $\pi_\nu$ ; likewise that  $\pi_\sigma$  is an isomorphism, because the correspondences  $\pi_\nu$  represent isomorphisms. — If  $\sigma$  is not a limit number, then we first have, between  $\mathfrak{K}_{\sigma-1}$  and  $\bar{\mathfrak{K}}_{\sigma-1}$ , the similar-isomorphic correspondence  $\pi_{\sigma-1}$ , which comprises  $\pi_0$ , and therefore assigns the principal functions  $f_{\sigma-1}(x)$  and  $\bar{f}_{\sigma-1}(x)$  to each other. Further, by  $\pi_{\sigma-1}$  the principal factor  $\varphi_{\sigma-1}(x)$ , as first factor of  $f_{\sigma-1}(x)$  within  $\mathfrak{K}_{\sigma-1}$ , is transformed into the first factor of  $\bar{f}_{\sigma-1}(x)$  within  $\bar{\mathfrak{K}}_{\sigma-1}$ , that is  $\bar{\varphi}_{\sigma-1}(x)$ . The fields  $\mathfrak{N}$  and  $\bar{\mathfrak{N}}$  prove to be normal and normally ordered extensions of  $\mathfrak{K}_{\sigma-1}$  and  $\bar{\mathfrak{K}}_{\sigma-1}$  with only one principal function each,  $\varphi_{\sigma-1}(x)$  respectively  $\bar{\varphi}_{\sigma-1}(x)$ . Since  $\mathfrak{K}_{\sigma-1}$  and  $\bar{\mathfrak{K}}_{\sigma-1}$  are mapped similar-isomorphically onto each other by  $\pi_{\sigma-1}$ , and  $\pi_{\sigma-1}$  at the same time carries the principal functions over into each other, the existence of the similar-isomorphic correspondence between  $\mathfrak{N}$  and  $\bar{\mathfrak{N}}$  follows as in the case  $\sigma = 1$ .

If in Theorem 5. we let  $\mathfrak{K}_0$  and  $\overline{\mathfrak{K}}_0$  coincide in one and the same well-ordered field, the following results:

6. *If  $\mathfrak{N}$  and  $\overline{\mathfrak{N}}$  are normal and normally ordered extensions of the well-ordered field  $\mathfrak{K}_0$  and the same system  $\{f_\nu(x)\}$  of principal functions belongs to both, then  $\mathfrak{N}$  and  $\overline{\mathfrak{N}}$  are similar-isomorphic.*

7. *If  $\mathfrak{K}_0$  is a well-ordered field,  $F = F_\sigma = \{f_\nu(x)\}$  ( $0 \leq \nu < \sigma$ ) a progressive system of normal functions from  $\mathfrak{K}_0$ , then there are normal and normally ordered extensions of  $\mathfrak{K}_0$  with the system of principal functions  $F$ .*

Proof by induction: In the case  $\sigma = 1$  we can, by § 8, 1., determine an extension  $\mathfrak{N}$  that just suffices for the breaking up of  $f_0(x)$ .  $\mathfrak{N}$  is normal, and since  $f_0(x)$ , too, is normal,  $\mathfrak{N} = \mathfrak{K}_0(j_0)$  if  $j_0$  is any zero of  $f_0(x)$  in  $\mathfrak{N}$ . If we order  $\mathfrak{N}$  with respect to  $\mathfrak{K}_0$  primitively and in such a way that  $j_0$  becomes principal element, then we see at once that  $\mathfrak{N}$  meets the conditions of the theorem. — If  $\sigma > 1$  and not a limit number, then let  $\mathfrak{K}_{\sigma-1}$  denote a normal and normally ordered extension of  $\mathfrak{K}_0$  with the system of principal functions  $F_{\sigma-1} = \{f_\nu(x)\}$  ( $0 \leq \nu < \sigma - 1$ ). Of the irreducible factors that the normal function  $f_{\sigma-1}(x)$  has in the well-ordered field  $\mathfrak{K}_{\sigma-1}$ , let  $\varphi_{\sigma-1}(x)$  be the first. Since  $\mathfrak{K}_{\sigma-1}$  just suffices for the breaking up of  $F_{\sigma-1}$  (Theorem 1.) and the system of normal functions  $F$  progresses, its degree must be greater than 1. If we extend  $\mathfrak{K}_{\sigma-1}$  by adjunction of a zero  $j_{\sigma-1}$  of  $\varphi_{\sigma-1}(x)$  to a field  $\mathfrak{N}$ , and order this primitively with respect to  $\mathfrak{K}_{\sigma-1}$  with  $j_{\sigma-1}$  as principal element, then  $\mathfrak{N}$  evidently meets the conditions of Theorem 7. — If  $\sigma$  is a limit number, then let  $\mathfrak{K}'_\nu$  ( $0 < \nu < \sigma$ ) denote a normal and normally ordered extension of  $\mathfrak{K}_0$  with the system of principal functions  $F_\nu = \{f_\lambda(x)\}$  ( $0 \leq \lambda < \nu$ ). If  $\mu < \nu$ , then  $\mathfrak{K}'_\nu$  has a principal segment that is normal and normally ordered with respect to  $\mathfrak{K}_0$  and has the system of principal functions  $F_\mu$ . By 6. this segment must be similar-isomorphic to  $\mathfrak{K}'_\mu$ . Thus the following results: *Of the fields of the sequence  $\mathfrak{K}_0, \{\mathfrak{K}'_\nu\}$  ( $0 < \nu < \sigma$ ) each is similar-isomorphic to a segment of every later one.* Consequently there is (§ 20, 4.) a well-ordered field  $\overline{\mathfrak{N}}$  of such a nature that  $\mathfrak{K}_0$  is similar-isomorphic to a segment  $\overline{\mathfrak{K}}_0$  and every field  $\mathfrak{K}'_\nu$  ( $0 < \nu < \sigma$ ) to a segment  $\overline{\mathfrak{K}}_\nu$  of  $\overline{\mathfrak{N}}$ , and that every element from  $\overline{\mathfrak{N}}$  occurs in segments  $\overline{\mathfrak{K}}_\nu$ . From the circumstance that a similar-isomorphic correspondence exists between  $\mathfrak{K}_0$  and  $\overline{\mathfrak{K}}_0$  it follows that we obtain a field  $\mathfrak{N}$ , similar-isomorphic to  $\overline{\mathfrak{N}}$ , which is at the same time an extension field of  $\mathfrak{K}_0$ , if we replace the segment  $\overline{\mathfrak{K}}_0$  of  $\overline{\mathfrak{N}}$  by the well-ordered system  $\mathfrak{K}_0$  and decree that every equation of composition ( $a + b = c$ ,  $a \cdot b = d$ ) from  $\overline{\mathfrak{N}}$  shall become an equation of composition from  $\mathfrak{N}$ , if the corresponding elements of  $\mathfrak{K}_0$  are substituted for any elements of  $\overline{\mathfrak{K}}_0$  occurring in it. By this substitution every segment  $\overline{\mathfrak{K}}_\nu$  of  $\overline{\mathfrak{N}}$  passes over into a segment  $\mathfrak{K}_\nu$  of  $\mathfrak{N}$  similar-isomorphic to it, hence also to  $\mathfrak{K}'_\nu$ , and every element of  $\mathfrak{N}$  occurs in such segments  $\mathfrak{K}_\nu$ . By the similar-isomorphic correspondence  $\pi_\nu$  between  $\mathfrak{K}'_\nu$  and  $\mathfrak{K}_\nu$  all order relations and equations of the one field are carried over into correct order relations and equations of the other. Since further the elements of  $\mathfrak{K}_0$ , hence also the functions of the system  $F$ , are not altered by  $\pi_\nu$ ,  $\mathfrak{K}_\nu$ , like  $\mathfrak{K}'_\nu$ , represents a normal and normally ordered extension of  $\mathfrak{K}_0$  with  $F_\nu$  as system of principal functions. But from the circumstance that the field  $\mathfrak{N}$  is composed of the elements of the sequence of fields  $\{\mathfrak{K}_\nu\}$ , and that every field of this sequence is a segment of all later ones and a segment of  $\mathfrak{N}$ , it is at once evident that  $\mathfrak{N}$  itself, too, is normally ordered with respect to  $\mathfrak{K}_0$ , and that  $F$  represents the associated system of principal functions.

From what precedes, the fundamental theorem now follows easily:

8. If  $\mathfrak{K}_0$  is an arbitrary field,  $S$  an arbitrary system of integral functions in  $\mathfrak{K}_0$ , then there is one and essentially only one extension of  $\mathfrak{K}_0$  that is just sufficiently large to break up all functions of the system  $S$  into linear factors.

Proof: In the question treated here the system  $S$  can be replaced by any equivalent system (§ 18, 3.), and it may therefore be assumed that  $S$  contains only normal functions (§ 18, 6.). Further we can think of the system  $S$  as well-ordered and, if it is not progressive, replace it by an equivalent progressive subsystem (§ 20, 1.). Accordingly we may assume from the outset that a progressive system of normal functions  $F = \{f_\nu(x)\}$  is present. Further, we may presuppose that the field  $\mathfrak{K}_0$  is well-ordered. But then by 7. there is a normal and normally ordered extension  $\mathfrak{N}$  of  $\mathfrak{K}_0$  with  $F$  as system of principal functions, and by 1. this is just sufficient for the complete breaking up of  $F$ . — Let us now assume that there is also a second extension  $\overline{\mathfrak{N}}$  of  $\mathfrak{K}_0$  that just suffices for the complete breaking up of  $F$ . Then we have to prove the equivalence of the extensions  $\mathfrak{N}$  and  $\overline{\mathfrak{N}}$ . For this purpose we make use of the principle of choice. For we think of one zero in each case as picked out from the zeros that the functions  $f_\nu(x)$  have in  $\mathfrak{N}$ , so that we have a system  $\overline{\mathfrak{J}} = \{i_\nu\}$ , where  $i_\nu$  is a zero of  $f_\nu(x)$ . Since normal functions are concerned,  $\overline{\mathfrak{N}} = \mathfrak{K}_0(\overline{\mathfrak{J}})$ . By 4.  $\overline{\mathfrak{N}}$  can be normally ordered with respect to  $\mathfrak{K}_0$  in such a way that  $F$  becomes the system of principal functions (and that the elements  $i_\nu$  become distinguished zeros of the principal functions. The latter is now no longer of any significance, but without this part Theorem 4. could not be proved). Thus  $\mathfrak{N}$  and  $\overline{\mathfrak{N}}$  are normal and normally ordered extensions of  $\mathfrak{K}_0$  with the same system of principal functions, and there exists between them a similar-isomorphic correspondence  $\pi$  (Theorem 6.). Since by this every element of the common segment  $\mathfrak{K}_0$  is assigned to itself, the extensions  $\mathfrak{N}$  and  $\overline{\mathfrak{N}}$  are equivalent.

From 8. it further follows by specialization:

9. Every field can be extended algebraically, and indeed essentially only in one way, to an algebraically closed field. — To every arbitrary field type there corresponds in this way a definite closed one.

For if we understand by  $S$  the system of *all* integral functions from  $\mathfrak{K}_0$ , then an extension field of  $\mathfrak{K}_0$  is algebraically closed and algebraic with respect to  $\mathfrak{K}_0$  if and only if it just suffices for the breaking up of  $S$ . From this there follows by 8. the first part of 9. — Now let any field type be given, let  $\mathfrak{K}_0$  and  $\mathfrak{K}'_0$  be two fields of this type and  $\mathfrak{L}$  and  $\mathfrak{L}'$  algebraic and algebraically closed extensions of  $\mathfrak{K}_0$  and  $\mathfrak{K}'_0$ . Then it is to be shown that  $\mathfrak{L}$  and  $\mathfrak{L}'$  are of the same type. For this purpose we introduce a system  $\mathfrak{S}$  of new elements, which we assign uniquely to the elements of  $\mathfrak{L}'$  not belonging to  $\mathfrak{K}'_0$ . This assignment gives, together with an isomorphism  $\pi_0$  between  $\mathfrak{K}_0$  and  $\mathfrak{K}'_0$ , a map  $\pi_1$  between  $\mathfrak{L}'$  and  $\overline{\mathfrak{L}} = \mathfrak{K}_0 + \mathfrak{S}$ . If we decree that by  $\pi_1$  every equation of composition  $a' + b' = c'$ ,  $a' \cdot b' = d'$  from  $\mathfrak{L}'$ , even if the elements  $a', b'$  do not both belong to  $\mathfrak{K}'_0$ , shall pass over into an equation of composition from  $\overline{\mathfrak{L}}$ , then  $\overline{\mathfrak{L}}$  becomes a field isomorphic to  $\mathfrak{L}'$ , consequently algebraically closed, and represents an algebraic extension of  $\mathfrak{K}_0$ .  $\mathfrak{L}$  and  $\overline{\mathfrak{L}}$  are therefore, by the already proved first part of 9., equivalent extensions of  $\mathfrak{K}_0$ , and we have an isomorphic correspondence  $\overline{\pi}_1$  between  $\mathfrak{L}$  and  $\overline{\mathfrak{L}}$ , which leaves the elements of  $\mathfrak{K}_0$  unchanged. From  $\overline{\pi}_1$  and  $\pi_1$  there results the isomorphic correspondence between  $\mathfrak{L}$  and  $\mathfrak{L}'$  that was to be proved. It presents itself as an extension of the isomorphism  $\pi_0$  existing between  $\mathfrak{K}_0$  and  $\mathfrak{K}'_0$ .

## § 22.

**Transcendental extensions. Algebraic dependence between elements of an extension field.**

We call every non-algebraic extension of a field *transcendental*. — We base the following investigations, which are to lead us to a perspicuous division of all fields, on a field  $\mathfrak{K}$ , and refer expressions such as “extension field”, “transcendental” etc. to it, unless otherwise noted. If  $\mathfrak{S}$  is a system of elements of an extension field  $\mathfrak{L}$  and  $a$  an element of  $\mathfrak{L}$ , then we call  $a$  *algebraically dependent on  $\mathfrak{S}$  (with respect to  $\mathfrak{K}$ )* if  $a$  is algebraic with respect to the field  $\mathfrak{K}(\mathfrak{S})$ ; and we call a system of elements  $\mathfrak{S}'$  *algebraically dependent on  $\mathfrak{S}$*  if every element of  $\mathfrak{S}'$  depends algebraically on  $\mathfrak{S}$ .

1. *If the element  $a$  depends algebraically on the system  $\mathfrak{S}$ , then there is a finite subsystem  $\mathfrak{S}'$  of  $\mathfrak{S}$  on which  $a$  depends algebraically.*

For it follows from our hypothesis that  $a$  is a zero of an integral function  $\varphi(x)$  of the field  $\mathfrak{K}(\mathfrak{S})$ . Since  $\varphi(x)$  has only finitely many coefficients, there is a finite subsystem  $\mathfrak{S}'$  of  $\mathfrak{S}$  such that these coefficients already occur in  $\mathfrak{K}(\mathfrak{S}')$ .<sup>E 119</sup> But then  $a$  depends algebraically on  $\mathfrak{S}'$ .

2. *If  $\mathfrak{S}_3$  depends algebraically on  $\mathfrak{S}_2$ ,  $\mathfrak{S}_2$  on  $\mathfrak{S}_1$ , then  $\mathfrak{S}_3$  is algebraically dependent on  $\mathfrak{S}_1$ .*<sup>E 120</sup>

For if we put  $\mathfrak{K}(\mathfrak{S}_1) = \mathfrak{K}_1$ ,  $\mathfrak{K}(\mathfrak{S}_2) = \mathfrak{K}_2$ , then it follows from our hypothesis that  $\mathfrak{K}_1(\mathfrak{S}_2)$  is algebraic with respect to  $\mathfrak{K}_1$ ,  $\mathfrak{K}_2(\mathfrak{S}_3)$  with respect to  $\mathfrak{K}_2$  (§ 7, 7.). Since  $\mathfrak{K}_2$  is a subfield of  $\mathfrak{K}_1(\mathfrak{S}_2)$ , the elements of  $\mathfrak{K}_2(\mathfrak{S}_3)$  are algebraic with respect to  $\mathfrak{K}_1(\mathfrak{S}_2)$ , hence also with respect to  $\mathfrak{K}_1 = \mathfrak{K}(\mathfrak{S}_1)$  (§ 7, 9.). Consequently the elements of  $\mathfrak{S}_3$  are algebraic with respect to  $\mathfrak{K}(\mathfrak{S}_1)$ , q.e.d.

If we therefore call two systems  $\mathfrak{S}_1, \mathfrak{S}_2$  *algebraically equivalent (with respect to  $\mathfrak{K}$ )* or briefly *equivalent* if each depends algebraically on the other, then two systems that are equivalent to a third are also equivalent to each other, etc.

We call a system  $\mathfrak{S}$  of elements of an extension field *algebraically reducible (with respect to  $\mathfrak{K}$ )*, or briefly *reducible*, if it is equivalent to a proper part of itself or consists of a single element algebraic with respect to  $\mathfrak{K}$ ; otherwise we call  $\mathfrak{S}$  *(algebraically) irreducible*<sup>15</sup>. From this definition it is immediately clear that in a reducible system that contains more than one element, at least *one* element occurs that depends algebraically on the system of the remaining elements. Together with 1., this immediately gives:

3. *Every subsystem of an irreducible system is irreducible.*<sup>E 121</sup>

4. *Every reducible system contains a finite reducible subsystem.*<sup>E 122</sup>

*Purely transcendental extensions.* — We call an extension of a field *purely transcendental* if it can be obtained by adjunction of an irreducible system  $\mathfrak{S}$ . If  $\mathfrak{S}$  consists of only finitely many elements  $x_1, x_2, \dots, x_n$ , then we are dealing with the same kind of extension we considered at the end of § 5: The field  $\mathfrak{K}(\mathfrak{S})$  consists of the rational functions of the transcendentals or indeterminates  $x_1, x_2, \dots, x_n$  with coefficients from  $\mathfrak{K}$ . If the system  $\mathfrak{S}$  is infinite, then  $\mathfrak{K}(\mathfrak{S})$  consists of the elements of all fields  $\mathfrak{K}(\mathfrak{S}')$ , where  $\mathfrak{S}'$  denotes every finite subsystem of  $\mathfrak{S}$ . The most general purely transcendental extension is therefore obtained by introducing an

<sup>15</sup> In modern terms: *algebraically independent*. — Trans.

arbitrary system  $\mathfrak{S}$  of infinitely many “indeterminates”. Every finite subsystem  $\mathfrak{S}'$  of  $\mathfrak{S}$  then yields an extension  $\mathfrak{K}(\mathfrak{S}')$  of the kind considered earlier, and the totality of all fields  $\mathfrak{K}(\mathfrak{S}')$  constitutes a field (§ 2, 2.), which arises from  $\mathfrak{K}$  by adjunction of the irreducible system  $\mathfrak{S}$ . — If we have two extensions  $\mathfrak{K}(\mathfrak{S}_1)$ ,  $\mathfrak{K}(\mathfrak{S}_2)$ , if  $\mathfrak{S}_1$  and  $\mathfrak{S}_2$  are irreducible systems, and if the finite or infinitely large number of their elements (cardinal number, power) is equal, i.e. if we can establish a one-to-one correspondence  $\varphi$  between their elements, then there is a definite isomorphism  $\pi$  between  $\mathfrak{K}(\mathfrak{S}_1)$  and  $\mathfrak{K}(\mathfrak{S}_2)$  by which every element of  $\mathfrak{K}$  is assigned to itself and the elements of  $\mathfrak{S}_1$  and  $\mathfrak{S}_2$  are related to each other in the same manner as by  $\varphi$ . This was shown for the case of finite systems in § 5, but follows from it immediately for infinite systems on the basis of a simple consideration. Thus:

5. *Two purely transcendental extensions  $\mathfrak{K}(\mathfrak{S}_1)$ ,  $\mathfrak{K}(\mathfrak{S}_2)$  of a field  $\mathfrak{K}$ , in which the irreducible systems  $\mathfrak{S}_1, \mathfrak{S}_2$  contain equally many elements, are equivalent.* <sup>E 123</sup>

6. *If an irreducible system  $\mathfrak{S}$  becomes reducible by the addition of an element  $a$ , then  $a$  is algebraically dependent on  $\mathfrak{S}$ .*

For the reducible system  $\mathfrak{S} + a$  contains a finite reducible system  $\mathfrak{T}$ .  $a$  must occur in  $\mathfrak{T}$ , because otherwise  $\mathfrak{T}$  would be a part of  $\mathfrak{S}$ , hence irreducible. Let  $\mathfrak{T} = \mathfrak{T}' + a$ , and let  $\mathfrak{T}'$  consist of the elements  $x_1, x_2, \dots, x_n$ . Since  $\mathfrak{T}'$  is irreducible, every field of the sequence

$$\mathfrak{K}, \mathfrak{K}_1 = \mathfrak{K}(x_1), \mathfrak{K}_2 = \mathfrak{K}_1(x_2), \dots, \mathfrak{K}_n = \mathfrak{K}_{n-1}(x_n) = \mathfrak{K}(\mathfrak{T}')$$

is transcendental with respect to the preceding one. If  $\mathfrak{K}_n(a)$  were also transcendental with respect to  $\mathfrak{K}_n$ , then (§ 5, 9.) every element of  $\mathfrak{T}$  would be algebraically independent of the system of the remaining elements, so  $\mathfrak{T}$  would be irreducible. Since this is not the case,  $a$  is algebraic with respect to  $\mathfrak{K}_n = \mathfrak{K}(\mathfrak{T}')$ , hence algebraically dependent on  $\mathfrak{T}'$  and thus also on  $\mathfrak{S}$ .

7. *If  $\mathfrak{S}$  is an irreducible system (with respect to  $\mathfrak{K}$ ) and the element  $a$  is transcendental with respect to  $\mathfrak{K}$  but algebraically dependent on  $\mathfrak{S}$ , then  $\mathfrak{S}$  contains a definite finite subsystem  $\mathfrak{T}$  with the following properties:  $a$  is algebraically dependent on  $\mathfrak{T}$ ; every subsystem of  $\mathfrak{S}$  on which  $a$  depends algebraically contains the system  $\mathfrak{T}$ ; if any element of  $\mathfrak{T}$  is replaced by  $a$ , then  $\mathfrak{S}$  passes over into an equivalent irreducible system; none of the remaining elements of  $\mathfrak{S}$  has this property.*

Proof: <sup>E 124</sup> Let  $\mathfrak{S}'$  denote any subsystem of  $\mathfrak{S}$  on which  $a$  depends algebraically (the system  $\mathfrak{S}$  itself not excluded). Then  $\mathfrak{S}'$  has finite subsystems on which  $a$  depends algebraically. <sup>E 125</sup> Let  $\mathfrak{T}$  be one such with as few elements as possible. Let the elements of  $\mathfrak{T}$  be  $\alpha_1, \alpha_2, \dots, \alpha_m$ , and let  $\mathfrak{T}_i$  ( $i = 1, \dots, m$ ) denote the system that remains after omission of  $\alpha_i$  from  $\mathfrak{T}$  (in the case  $m = 1$  the empty system). Since  $a$  is algebraically dependent on the system  $\mathfrak{T}$  but algebraically independent of each of the systems  $\mathfrak{T}_i$ , the system  $\mathfrak{T} + a$  is reducible, while the systems  $\mathfrak{T}_i + a$  are irreducible (Theorem 6.). This holds also in the case  $m = 1$ , because  $a$  is transcendental with respect to  $\mathfrak{K}$ . Since the irreducible system  $\mathfrak{T}_i + a$  passes over into the reducible  $\mathfrak{T} + a$  by addition of  $\alpha_i$ ,  $\alpha_i$  depends algebraically on  $\mathfrak{T}_i + a$ , and the systems  $\mathfrak{T}_i + a$  and  $\mathfrak{T} + a$  are equivalent. Likewise  $\mathfrak{T}$  and  $\mathfrak{T} + a$  are equivalent. Thus we see: *The  $m + 1$  systems  $\mathfrak{T}_i + a$ ,  $\mathfrak{T}$  are equivalent to  $\mathfrak{T} + a$ , hence also to one another.*

We now want to show that every subsystem  $\mathfrak{S}''$  of  $\mathfrak{S}$  on which  $a$  depends algebraically must contain the system  $\mathfrak{T}$ . For this purpose we denote by  $\mathfrak{U}$  a finite subsystem of  $\mathfrak{S}''$ , consisting of as few elements as possible, on which  $a$  depends algebraically, and demonstrate the identity of

$\mathfrak{U}$  and  $\mathfrak{T}$ . Let  $\mathfrak{U}$  consist of the elements  $\beta_1, \dots, \beta_n$ , and let  $\mathfrak{U}_i$  ( $i = 1, \dots, n$ ) denote the system remaining after omission of  $\beta_i$  from  $\mathfrak{U}$ . Then the systems  $\mathfrak{U}_i + a$  and  $\mathfrak{U}$  are irreducible and equivalent to one another as well as to the reducible system  $\mathfrak{U} + a$ . — Because of their property as smallest systems on which  $a$  depends algebraically, neither of the systems  $\mathfrak{T}, \mathfrak{U}$  can be a proper part of the other. If they were therefore different, we might assume that  $\alpha_1$  does not occur in  $\mathfrak{U}$  and  $\beta_1$  not in  $\mathfrak{T}$ . Now let  $\mathfrak{V}$  be the subsystem of  $\mathfrak{S}$  that contains all elements of  $\mathfrak{T}$  and all of  $\mathfrak{U}$ , and no other element. Since  $\mathfrak{T}_1 + a$  is equivalent to the system  $\mathfrak{T}$  contained in  $\mathfrak{V}$ , we obtain from  $\mathfrak{V}$  a system  $\mathfrak{V}'$  equivalent to  $\mathfrak{V}$  if we replace  $\alpha_1$  by  $a$ .  $\mathfrak{V}'$  contains the system  $\mathfrak{U} + a$ , and since this is equivalent to  $\mathfrak{U}$ , we obtain a system  $\mathfrak{V}''$  equivalent to  $\mathfrak{V}'$  if we omit the element  $a$  from  $\mathfrak{V}'$ . According to this,  $\mathfrak{V}$  would be equivalent to a proper part  $\mathfrak{V}''$  of itself, hence reducible. But that is not possible, because  $\mathfrak{V}$  is a part of the irreducible system  $\mathfrak{S}$ .

*Thus  $\mathfrak{T}$  must in fact be contained in every subsystem of  $\mathfrak{S}$  on which  $a$  depends algebraically.* If therefore  $\mathfrak{S}_i$  ( $i = 1, \dots, m$ ) denotes the system that remains after omission of  $\alpha_i$  from  $\mathfrak{S}$ , then  $a$  is algebraically independent of the irreducible system  $\mathfrak{S}_i$ , so the system  $\mathfrak{S}_i + a$  is likewise irreducible. But  $\mathfrak{S}_i + a$  arises from  $\mathfrak{S}$  when we replace  $\alpha_i$  by  $a$ , or, what comes to the same thing,  $\mathfrak{T} = \mathfrak{T}_i + \alpha_i$  by the equivalent system  $\mathfrak{T}_i + a$ . Therefore  $\mathfrak{S}$  and  $\mathfrak{S}_i + a$  are equivalent systems. Thus: *We obtain a system that is irreducible and equivalent to  $\mathfrak{S}$  if we replace one of the elements of  $\mathfrak{T}$  by  $a$ .* — If on the other hand  $\gamma$  is an element of  $\mathfrak{S}$  not occurring in  $\mathfrak{T}$ , after whose omission  $\mathfrak{S}'$  remains, then  $\mathfrak{S}'$  contains the system  $\mathfrak{T}$ , so  $a$  depends algebraically on  $\mathfrak{S}'$ , and the system  $\mathfrak{S}' + a$ , which arises from  $\mathfrak{S}$  when  $\gamma$  is replaced by  $a$ , is therefore reducible. It is equivalent to the system  $\mathfrak{S}'$ , and since this, as a proper part of the irreducible system  $\mathfrak{S}$ , cannot be equivalent to  $\mathfrak{S}$ ,  $\mathfrak{S}' + a$ , too, is not equivalent to  $\mathfrak{S}$ . This completes the proof of 7. in all its parts.

8. *Let  $\mathfrak{U}$  and  $\mathfrak{V}$  be finite irreducible systems of  $m$  and  $n$  elements respectively; let  $n \leq m$ , and let  $\mathfrak{V}$  be algebraically dependent on  $\mathfrak{U}$ . Then in the case  $m = n$  the systems  $\mathfrak{U}$  and  $\mathfrak{V}$  are equivalent, but in the case  $n < m$ ,  $\mathfrak{U}$  is equivalent to an irreducible system that consists of  $\mathfrak{V}$  and  $m - n$  elements of  $\mathfrak{U}$ .*

For let  $u_1, \dots, u_m$  be the elements of  $\mathfrak{U}$ ,  $v_1, \dots, v_n$  those of  $\mathfrak{V}$ . Since  $v_1$  is transcendental with respect to  $\mathfrak{K}$  and depends algebraically on  $\mathfrak{U}$ , then by 7.  $\mathfrak{U}$  contains at least one element whose replacement by  $v_1$  turns  $\mathfrak{U}$  into an irreducible system equivalent to  $\mathfrak{U}$ . This establishes the assertion for the case  $n = 1$ . For  $n > 1$  the proof is to be conducted by complete induction. Since the system  $\mathfrak{V}'$ , which consists of the elements  $v_1, \dots, v_{n-1}$ , is irreducible and depends algebraically on  $\mathfrak{U}$ , we may take it as proved that  $\mathfrak{U}$  is equivalent to an irreducible system  $\mathfrak{U}'$  that consists of  $\mathfrak{V}'$  and  $m - n + 1$  elements of  $\mathfrak{U}$ .  $v_n$  depends algebraically on  $\mathfrak{U}'$ , but not on  $\mathfrak{V}'$ . If therefore  $\mathfrak{T}$  is the smallest subsystem of  $\mathfrak{U}'$  on which  $v_n$  depends algebraically, then  $\mathfrak{T}$  contains at least one of the  $m - n + 1$  elements of  $\mathfrak{U}$ . If we replace one such by  $v_n$ , then  $\mathfrak{U}'$  becomes an irreducible system equivalent to  $\mathfrak{U}$ , which consists of  $\mathfrak{V}$  and  $m - n$  elements of  $\mathfrak{U}$ . In the case  $m = n$ , therefore,  $\mathfrak{U}$  and  $\mathfrak{V}$  are equivalent.

We also see from this that an irreducible system  $\mathfrak{V}$  algebraically dependent on  $\mathfrak{U}$  cannot contain more than  $m$  elements. Otherwise a proper part  $\mathfrak{V}'$  of  $\mathfrak{V}$  consisting of  $m$  elements would, by what has just been proved, be equivalent to  $\mathfrak{U}$ .  $\mathfrak{V}$  would then be algebraically dependent on  $\mathfrak{V}'$ , hence reducible. Thus:

9. *An irreducible system  $\mathfrak{V}$  that depends algebraically on a finite system  $\mathfrak{U}$  cannot contain more elements than the latter; in the case of an equal number of elements both systems are equivalent.*

## § 23.

**The degree of transcendence and the division of fields into classes.**

In the following considerations, in which, as before, we refer to a ground field  $\mathfrak{K}$ , we again make use of the well-ordering theorem.

1. *Every system  $\mathfrak{S}$  whose elements are not all algebraic with respect to  $\mathfrak{K}$  is equivalent to an irreducible subsystem.*

Proof: If  $\mathfrak{S}$  contains algebraic elements, then after omission of these there remains a system equivalent to  $\mathfrak{S}$ , with which we can operate further. We may therefore assume from the outset that every element of  $\mathfrak{S}$  is transcendental with respect to  $\mathfrak{K}$ . If now, first,  $\mathfrak{S}$  is finite,  $\mathfrak{T}$  a subsystem equivalent to  $\mathfrak{S}$  of as few elements as possible, then  $\mathfrak{T}$  is evidently also irreducible. — If the system  $\mathfrak{S}$  is infinite, then we think of it as well-ordered —  $\mathfrak{S} = \{a_\nu\}$  — and denote by  $\mathfrak{S}_\nu$  the segment determined by  $a_\nu$ . If we omit from  $\mathfrak{S}$  every element  $a_\nu$  ( $\nu > 0$ ) that depends algebraically on the associated segment  $\mathfrak{S}_\nu$ , then there remains a system  $\mathfrak{S}'$  that is irreducible and equivalent to  $\mathfrak{S}$ . For, first,  $a_0$ , because it belongs to  $\mathfrak{S}'$ , is algebraically dependent on  $\mathfrak{S}'$ . If, further, it is assumed as already proved that the elements of the segment  $\mathfrak{S}_\nu$  depend algebraically on  $\mathfrak{S}'$ , then the same holds for  $a_\nu$ , because  $a_\nu$  either depends algebraically on  $\mathfrak{S}_\nu$  or belongs to  $\mathfrak{S}'$ . From this there results the equivalence of  $\mathfrak{S}$  and  $\mathfrak{S}'$ . If  $\mathfrak{S}'$  were reducible and  $\mathfrak{T}$  a finite reducible subsystem of  $\mathfrak{S}'$  with as few elements as possible,  $a_\nu$  the last element of  $\mathfrak{T}$ , then  $a_\nu$ , because transcendental with respect to  $\mathfrak{K}$ , would not be the only element of  $\mathfrak{T}$ , and the system  $\mathfrak{T}'$ , which remains after omission of  $a_\nu$  from  $\mathfrak{T}$  and is a part of  $\mathfrak{S}_\nu$ , would be irreducible. Consequently (§ 22, 6.)  $a_\nu$  would be algebraically dependent on  $\mathfrak{T}'$ , hence also on  $\mathfrak{S}_\nu$ . But then  $a_\nu$  would not belong to  $\mathfrak{S}'$ , and we would obtain a contradiction. Thus  $\mathfrak{S}'$  is irreducible, and with this Theorem 1. is proved.

Now let  $\mathfrak{L} = \mathfrak{K}(\mathfrak{S})$  denote an arbitrary transcendental extension of  $\mathfrak{K}$ . Then  $\mathfrak{S}$  is equivalent to an irreducible system  $\mathfrak{S}'$ , and the elements of  $\mathfrak{S}$  are therefore algebraic with respect to  $\mathfrak{K}(\mathfrak{S}')$ . Hence  $\mathfrak{K}(\mathfrak{S})$  represents an algebraic extension of  $\mathfrak{K}(\mathfrak{S}')$ ,  $\mathfrak{K}(\mathfrak{S}')$  a purely transcendental one of  $\mathfrak{K}$ , and we obtain the theorem:

2. *Every transcendental extension of a field can be decomposed into a purely transcendental one and an algebraic one following upon it.*

Naturally such a decomposition can take place in infinitely many ways. Let us assume that  $\mathfrak{S}_1$  and  $\mathfrak{S}_2$  are two irreducible systems from  $\mathfrak{L}$  on which all elements of  $\mathfrak{L}$  depend algebraically; then  $\mathfrak{S}_1$  and  $\mathfrak{S}_2$  are equivalent. For the case that one of these systems is finite, it was shown above that the other, too, is finite and contains equally many elements (§ 22, 9.). We shall show that also in the case of infinite systems the cardinal numbers agree, hence (§ 22, 5.)  $\mathfrak{K}(\mathfrak{S}_1)$  and  $\mathfrak{K}(\mathfrak{S}_2)$  are equivalent extensions of  $\mathfrak{K}$ .<sup>E 126</sup> For this purpose we first introduce some designations.

If  $\{c_\mu\}$  ( $0 \leq \mu < \tau$ ) is a well-ordered sequence of elements of an extension field,  $\tau$  a limit number, and if from a definite  $\mu$  on all elements  $c_\mu$  are equal to one another, say equal to  $a$ , then we say: *the sequence has a limit value, this is equal to  $a$* ; in symbols

$$\lim_{\mu=\tau} c_\mu = a.$$

— Let there be given a well-ordered double sequence:  $\{c_{\mu\nu}\}$  ( $0 \leq \mu < \tau$ ,  $0 \leq \nu < \sigma$ ), which we think of as ordered in rows and columns, and let the rows be denoted by  $\mathfrak{W}_\mu$ , so that

$\mathfrak{W}_\mu = \{c_{\mu\nu}\} (0 \leq \nu < \sigma)$ . If  $\tau$  is a limit number and every column has a limit value

$$\lim_{\mu=\tau} c_{\mu\nu} = c'_\nu \quad (0 \leq \nu < \sigma),$$

then we say: *the sequence  $\{\mathfrak{W}_\mu\}$  has the limit value  $\mathfrak{W}' = \{c'_\nu\}$ .*

Let  $\mathfrak{U}$  and  $\mathfrak{V} = \{v_\mu\} (0 \leq \mu < \tau)$  be two irreducible systems, well-ordered in an arbitrary manner, let  $\mathfrak{W}$  depend algebraically on  $\mathfrak{U}$ , and let  $v_\mu$  denote an arbitrary element of  $\mathfrak{V}$ ,  $\mathfrak{W}_\mu$  the segment of  $\mathfrak{W}$  determined by  $v_\mu$ .  $\mathfrak{U}$  contains (§ 22, 7.) a definite smallest subsystem  $\mathfrak{T}$  on which  $v_\mu$  depends algebraically.  $\mathfrak{T}$  may well contain elements that occur in  $\mathfrak{W}_\mu$ , but certainly contains also elements that do not occur in  $\mathfrak{W}_\mu$ . If we replace the last of these by  $v_\mu$ , then  $\mathfrak{U}$  passes over into an irreducible system equivalent to  $\mathfrak{U}$  of the same ordinal number. *For this system, completely determined by  $\mathfrak{U}$ ,  $\mathfrak{V}$  and  $\mu$ , we introduce the sign  $\vartheta_\mu(\mathfrak{U}, \mathfrak{V})$ .*

Now let  $\mathfrak{U} = \{u_\nu\} (0 \leq \nu < \sigma)$  and  $\mathfrak{V} = \{v_\mu\} (0 \leq \mu < \tau)$  be irreducible well-ordered systems, let  $\mathfrak{W}$  depend algebraically on  $\mathfrak{U}$ , and let there be given a double sequence  $\{c_{\mu\nu}\} (0 \leq \mu \leq \tau, 0 \leq \nu < \sigma)^*$ , whose rows we denote by  $\mathfrak{W}_\mu$ . We shall assume that the following relations hold:

- 1) Let every row  $\mathfrak{W}_\mu = \{c_{\mu\nu}\} (0 \leq \nu < \sigma)$  represent an irreducible system and be equivalent to  $\mathfrak{U}$ , so that  $\mathfrak{W}$  depends algebraically on every system  $\mathfrak{W}_\mu$ .
- 2) Let  $\mathfrak{W}_0 = \mathfrak{U}$ , hence  $c_{0\nu} = u_\nu (0 \leq \nu < \sigma)$ .
- 3) If  $0 < \mu \leq \tau$ ,  $\mu$  not a limit number, let  $\mathfrak{W}_\mu = \vartheta_{\mu-1}(\mathfrak{W}_{\mu-1}, \mathfrak{V})$ .
- 4) If  $0 < \mu \leq \tau$ ,  $\mu$  a limit number, let the sequence  $\{\mathfrak{W}_\lambda\} (0 \leq \lambda < \mu)$  have a limit, and let this be equal to  $\mathfrak{W}_\mu$ .

If these conditions are satisfied, then we say: *the sequence of systems  $\{\mathfrak{W}_\mu\} (0 \leq \mu \leq \tau)$  — or also: the double sequence  $\{c_{\mu\nu}\}$  — belongs to the pair of systems  $\mathfrak{U}, \mathfrak{V}$ .* The hypothesis for this mode of expression is therefore always that  $\mathfrak{U}$  and  $\mathfrak{V}$  are well-ordered irreducible systems and that  $\mathfrak{W}$  depends algebraically on  $\mathfrak{U}$ .

By conditions 1) to 4), each row is determined by the ones preceding it, and since  $\mathfrak{W}_0 = \mathfrak{U}$  is required, we obtain first:

a) *No more than one sequence of systems can belong to a pair of systems  $\mathfrak{U}, \mathfrak{V}$ .* It also follows immediately from our conditions:

b) If the sequence of systems  $\{\mathfrak{W}_\mu\} (0 \leq \mu \leq \tau)$  belongs to the pair of systems  $\mathfrak{U}, \mathfrak{V}$ , and if  $0 < \varrho < \tau$ ,  $\mathfrak{V}_\varrho$  the segment of  $\mathfrak{V}$  determined by  $v_\varrho$ , then the sequence of systems  $\{\mathfrak{W}_\mu\} (0 \leq \mu \leq \varrho)$  belongs to the pair of systems  $\mathfrak{U}, \mathfrak{V}_\varrho$ .

We now pick out, under the hypothesis that the sequence of systems  $\{\mathfrak{W}_\mu\}$  belongs to  $\mathfrak{U}, \mathfrak{V}$ , a column  $\{c_{\mu\nu}\} (0 \leq \mu \leq \tau)$  from the double sequence  $\{c_{\mu\nu}\}$ . If not all elements of the column are equal to the initial element  $c_{0\nu} = u_\nu$ , then let  $c_{\varrho\nu}$  be the first one different from  $u_\nu$ . Then  $\varrho$  cannot be a limit number, because otherwise by 4)  $c_{\varrho\nu}$  represents the limit of  $\{c_{\mu\nu}\} (0 \leq \mu < \varrho)$ , hence is equal to preceding elements of the column. Since  $\varrho$  is not a limit number, by 3)  $\mathfrak{W}_\varrho = \vartheta_{\varrho-1}(\mathfrak{W}_{\varrho-1}, \mathfrak{V})$ , and  $\mathfrak{W}_\varrho$  arises from  $\mathfrak{W}_{\varrho-1}$  when a certain element of  $\mathfrak{W}_{\varrho-1}$  is replaced by  $v_{\varrho-1}$ . Now since  $c_{\varrho\nu}$  is different from  $c_{\varrho-1,\nu}$ ,  $c_{\varrho\nu} = v_{\varrho-1}$  must hold. But then for every  $\mu > \varrho$   $c_{\mu\nu} = v_{\varrho-1}$ . For if instead  $\mu$  denotes the smallest ordinal number  $> \varrho$  for which  $c_{\mu\nu} \neq v_{\varrho-1}$ , then, as before, it follows that  $\mu$  is not a limit number and that  $\mathfrak{W}_\mu$  arises from  $\mathfrak{W}_{\mu-1}$  when  $c_{\mu-1,\nu} = v_{\varrho-1}$  is replaced by  $c_{\mu\nu} = v_{\mu-1}$ . But according to the definition of the sign  $\vartheta$ ,  $\vartheta_{\mu-1}(\mathfrak{W}_{\mu-1}, \mathfrak{V})$  arises from  $\mathfrak{W}_{\mu-1}$  when a certain element of  $\mathfrak{W}_{\mu-1}$  that does

\*) Note at this place the equality sign before  $\tau$ .

not belong to the segment of  $\mathfrak{V}$  determined by  $v_{\mu-1}$  is replaced by  $v_{\mu-1}$ . The element  $v_{\varrho-1}$ , however, belongs to this segment. From this follows

c) If the sequence of systems  $\{\mathfrak{W}_\mu\}$  ( $0 \leq \mu \leq \tau$ ), where  $\mathfrak{W}_\mu = \{c_{\mu\nu}\}$ , belongs to the pair of systems  $\mathfrak{U}, \mathfrak{V}$ , then in a column  $\{c_{\mu\nu}\}$  ( $0 \leq \mu \leq \tau$ ) either all elements are equal to  $u_\nu$ , or there exists an ordinal number  $\varrho$ ,  $0 < \varrho \leq \tau$ , that is not a limit number, such that  $c_{\mu\nu} = u_\nu$  for  $\mu < \varrho$ ,  $c_{\mu\nu} = v_{\varrho-1}$  for  $\mu \geq \varrho$ .

If, under the same hypotheses, we pick out an arbitrary element  $v_{\varrho-1}$  from  $\mathfrak{V}$ , then by 3) it occurs in  $\mathfrak{W}_\varrho$ , say as  $c_{\varrho\nu}$ ; and since, as  $\mu$  runs through the ordinal numbers  $> \varrho$ , it cannot, as we saw, be replaced by any  $v_{\mu-1}$ ,  $v_{\varrho-1}$  occurs in every system  $\mathfrak{W}_\mu$  whose index is  $\mu \geq \varrho$ . Thus:

d) If the sequence of systems  $\{\mathfrak{W}_\mu\}$  ( $0 \leq \mu \leq \tau$ ) belongs to the pair of systems  $\mathfrak{U}, \mathfrak{V} = \{v_\mu\}$  ( $0 \leq \mu < \tau$ ), and if  $\mathfrak{V}_\mu$  ( $0 < \mu < \tau$ ) denotes the segment determined by  $v_\mu$ , while we put  $\mathfrak{V} = \mathfrak{V}_\tau$ , then  $\mathfrak{W}_\mu$  ( $0 < \mu \leq \tau$ ) contains all elements of  $\mathfrak{V}_\mu$  (naturally not necessarily in the same order as  $\mathfrak{V}_\mu$ ).

We now assert:

e) *To every pair  $\mathfrak{U}, \mathfrak{V}$  of irreducible well-ordered systems, the second of which depends algebraically on the first, there belongs a sequence of systems.*

We put as before  $\mathfrak{U} = \{u_\nu\}$  ( $0 \leq \nu < \sigma$ ),  $\mathfrak{V} = \mathfrak{V}_\tau = \{v_\mu\}$  ( $0 \leq \mu < \tau$ ) and denote by  $\mathfrak{V}_\mu$  the segment of  $\mathfrak{V}$  determined by  $v_\mu$ . In the case  $\tau = 1$  we evidently obtain the required sequence of systems by putting  $\mathfrak{W}_0 = \mathfrak{U}$ ,  $\mathfrak{W}_1 = \vartheta_0(\mathfrak{U}, \mathfrak{V})$ . For  $\tau > 1$ , e) is to be proved by induction. — If  $\tau$  is not a limit number, then, first, a sequence of systems  $\{\mathfrak{W}_\mu\}$  ( $0 \leq \mu \leq \tau-1$ ) belongs to the pair of systems  $\mathfrak{U}, \mathfrak{V}_{\tau-1}$ , and if we put  $\vartheta_{\tau-1}(\mathfrak{W}_{\tau-1}, \mathfrak{V}) = \mathfrak{W}_\tau$ , then it follows immediately that the sequence of systems  $\{\mathfrak{W}_\mu\}$  ( $0 \leq \mu \leq \tau$ ) meets all conditions 1) to 4), hence belongs to  $\mathfrak{U}, \mathfrak{V}$ . — Let  $\tau$  be a limit number. If, then,  $0 < \lambda \leq \varrho < \tau$ , there belongs to the pair  $\mathfrak{U}, \mathfrak{V}_\varrho$  one, and by a) only one, sequence of systems  $\{\mathfrak{W}_\mu\}$  ( $0 \leq \mu \leq \varrho$ ), and it follows from b) that the subsequence  $\{\mathfrak{W}_\mu\}$  ( $0 \leq \mu \leq \lambda$ ) belongs to  $\mathfrak{U}, \mathfrak{V}_\lambda$ . Consequently for every  $\mu < \tau$  there exists a uniquely determined system  $\mathfrak{W}_\mu$  such that the segment of the sequence  $\{\mathfrak{W}_\mu\}$  ( $0 \leq \mu < \tau$ ) reaching up to a  $\mathfrak{W}_\varrho$  (inclusive) represents the sequence of systems belonging to  $\mathfrak{U}, \mathfrak{V}_\varrho$ . We put  $\mathfrak{W}_\mu = \{c_{\mu\nu}\}$  ( $0 \leq \nu < \sigma$ ) and consider a column  $\{c_{\mu\nu}\}$  ( $0 \leq \mu < \tau$ ). If not all elements are equal to  $u_\nu$  and if  $c_{\varrho\nu}$  is the first one different from  $u_\nu$ , then all elements of the column following upon  $c_{\varrho\nu}$  are equal to  $c_{\varrho\nu}$ , because the assumption  $c_{0\nu} \neq c_{\varrho\nu}$ ,  $c_{\varrho\nu} \neq c_{\varkappa\nu}$ ,  $\varrho < \varkappa$  is, by c), incompatible with the fact that the sequence  $\{\mathfrak{W}_\mu\}$  ( $0 \leq \mu \leq \varkappa$ ) belongs to  $\mathfrak{U}, \mathfrak{V}_\varkappa$ . Therefore every column, and consequently also the sequence  $\{\mathfrak{W}_\mu\}$  ( $0 \leq \mu < \tau$ ), has a limit. We put

$$\lim_{\mu=\tau} \mathfrak{W}_\mu = \mathfrak{W}_\tau, \quad \mathfrak{W}_\tau = \{c_{\tau\nu}\} \quad (0 \leq \nu < \sigma)$$

and assert that the sequence of systems  $\{\mathfrak{W}_\mu\}$  ( $0 \leq \mu \leq \tau$ ) belongs to  $\mathfrak{U}, \mathfrak{V}$ . — In order to prove this, we have to show two things, namely:

f)  $\mathfrak{W}_\tau$  is irreducible,

g)  $\mathfrak{W}_\tau$  is equivalent to  $\mathfrak{W}_0 = \mathfrak{U}$ .

If the system  $\mathfrak{W}_\tau$  were reducible, it would contain a finite reducible subsystem  $\mathfrak{T}$ . Every element of  $\mathfrak{T}$ , as limit value of its column, is equal to preceding elements of this column, and since  $\mathfrak{T}$  contains only finitely many elements, we can determine  $\varrho < \tau$  so that all elements of  $\mathfrak{T}$  already occur in  $\mathfrak{W}_\varrho$ . According to this  $\mathfrak{W}_\varrho$  would be reducible, which contradicts the circumstance that the sequence of systems  $\{\mathfrak{W}_\mu\}$  ( $0 \leq \mu \leq \varrho$ ) belongs to  $\mathfrak{U}, \mathfrak{V}_\varrho$ . This

proves f). — An arbitrary element of  $\mathfrak{V}$  can be denoted by  $v_{\varrho-1}$ , where  $\varrho < \tau$ .  $v_{\varrho-1}$  occurs in  $\mathfrak{W}_{\varrho}$ , say as  $c_{\varrho\nu}$ , and then in  $\{c_{\mu\nu}\}$  ( $0 \leq \mu < \tau$ ) for every  $\mu \geq \varrho$   $c_{\mu\nu} = v_{\varrho-1}$ , hence also  $c_{\tau\nu} = \lim_{\mu=\tau} c_{\mu\nu} = v_{\varrho-1}$ .  $\mathfrak{W}_{\tau}$  therefore contains all elements of  $\mathfrak{V}$ . Since further every element of  $\mathfrak{W}_{\tau}$  already occurs in a system  $\mathfrak{W}_{\varrho}$  ( $\varrho < \tau$ ) and  $\mathfrak{W}_{\varrho}$  is equivalent to  $\mathfrak{W}_0$ ,  $\mathfrak{W}_{\tau}$  depends algebraically on  $\mathfrak{W}_0$ , and in order to prove g) we still have to show that  $\mathfrak{W}_0$ , too, depends algebraically on  $\mathfrak{W}_{\tau}$ . For this purpose we carry out a more general demonstration. We denote by  $\mathfrak{W}_{\mu\nu}$  ( $0 \leq \mu \leq \tau$ ,  $0 < \nu < \sigma$ ) the segment of  $\mathfrak{W}_{\mu}$  determined by  $c_{\mu\nu}$  and put  $\mathfrak{W}_{\mu} = \mathfrak{W}_{\mu\sigma}$ . We denote further by  $\mathfrak{W}'_{\mu\nu}$  ( $0 < \mu \leq \tau$ ,  $0 < \nu \leq \sigma$ ) that subsystem of  $\mathfrak{W}_{\mu}$  that contains all elements of  $\mathfrak{W}_{\mu\nu}$ , all elements of  $\mathfrak{V}_{\mu}$ , but otherwise no element, and put  $\mathfrak{W}'_{0\nu} = \mathfrak{W}_{0\nu}$  ( $0 < \nu \leq \sigma$ ). We now assert:

h) Every system  $\mathfrak{W}'_{\mu\nu}$  ( $0 \leq \mu \leq \tau$ ,  $0 < \nu \leq \sigma$ ) is algebraically dependent on every system  $\mathfrak{W}'_{\varrho\nu}$  ( $\mu \leq \varrho \leq \tau$ ).

This assertion, namely if we choose  $\mu = 0$ ,  $\nu = \sigma$ ,  $\varrho = \tau$ , also contains the assertion that  $\mathfrak{W}_0$  depends algebraically on  $\mathfrak{W}_{\tau}$ . Thus h) proves g), and therefore e). Now should the assertion h) not hold for every system  $\mathfrak{W}'_{\mu\nu}$ , then we choose from among the systems for which it does not hold one whose second index  $\nu$  is as small as possible. We then seek for this  $\mathfrak{W}'_{\mu\nu}$  that  $\mathfrak{W}'_{\varrho\nu}$  with smallest index  $\varrho > \mu$  on which  $\mathfrak{W}'_{\mu\nu}$  does not depend algebraically. Now let  $a$  be an element of  $\mathfrak{W}'_{\mu\nu}$  that does not depend algebraically on  $\mathfrak{W}'_{\varrho\nu}$ . Then  $a$  does not belong to  $\mathfrak{W}'_{\varrho\nu}$ , hence not to  $\mathfrak{V}_{\varrho}$  either, hence not to  $\mathfrak{V}_{\mu}$  either, and consequently belongs to  $\mathfrak{W}_{\mu\nu}$ . Further,  $a$  must be the last element of  $\mathfrak{W}_{\mu\nu}$ . Otherwise  $a$  would belong to a segment  $\mathfrak{W}_{\mu\lambda}$  of  $\mathfrak{W}_{\mu\nu}$ , hence also to the system  $\mathfrak{W}'_{\mu\lambda}$ ; since this, because of the minimum property of  $\nu$ , depends algebraically on  $\mathfrak{W}'_{\varrho\lambda}$  and  $\mathfrak{W}'_{\varrho\lambda}$  is a part of  $\mathfrak{W}'_{\varrho\nu}$ ,  $a$  would depend algebraically on  $\mathfrak{W}'_{\varrho\nu}$ . Consequently  $a$  is the last element of  $\mathfrak{W}_{\mu\nu}$ , hence  $\nu$  is not a limit number, and we have

$$a = c_{\mu,\nu-1}, \quad \mathfrak{W}_{\mu\nu} = \mathfrak{W}_{\mu,\nu-1} + c_{\mu,\nu-1},$$

and since  $a$  does not belong to  $\mathfrak{V}_{\mu}$ ,

$$\mathfrak{W}'_{\mu\nu} = \mathfrak{W}'_{\mu,\nu-1} + c_{\mu,\nu-1},$$

(where in the case  $\nu = 1$  both  $\mathfrak{W}_{\mu,\nu-1}$  and  $\mathfrak{W}'_{\mu,\nu-1}$  denote the empty system). If we let  $\lambda$  run through all numbers that are  $\geq \mu$  and  $< \varrho$ , then, because of the minimum property of  $\varrho$ ,  $\mathfrak{W}'_{\mu\nu}$  is algebraically dependent on every system  $\mathfrak{W}'_{\lambda\nu}$ , and therefore none of these systems can depend algebraically on  $\mathfrak{W}'_{\varrho\nu}$ . Now, however, all elements of  $\mathfrak{W}'_{\lambda\nu}$  except  $c_{\lambda,\nu-1}$  belong to  $\mathfrak{W}'_{\lambda,\nu-1}$ , hence depend algebraically on  $\mathfrak{W}'_{\varrho,\nu-1}$  and thus on  $\mathfrak{W}'_{\varrho\nu}$ . Thus  $c_{\lambda,\nu-1}$  cannot depend algebraically on  $\mathfrak{W}'_{\varrho\nu}$ . The elements  $c_{\lambda,\nu-1}$  must therefore be different from the element  $c_{\varrho,\nu-1}$  contained in  $\mathfrak{W}'_{\varrho\nu}$ . From this it follows that  $\varrho$  is not a limit number and

$$(1.) \quad c_{\varrho-1,\nu-1} = u_{\nu-1}, \quad c_{\varrho,\nu-1} = v_{\varrho-1}, \quad \mathfrak{W}_{\varrho} = \vartheta_{\varrho-1}(\mathfrak{W}_{\varrho-1}, \mathfrak{V})$$

holds. Let  $\mathfrak{T}$  denote the smallest subsystem of  $\mathfrak{W}_{\varrho-1}$  on which  $v_{\varrho-1}$  depends algebraically. According to the definition of the sign  $\vartheta_{\varrho-1}$ ,  $\mathfrak{W}_{\varrho}$  arises from  $\mathfrak{W}_{\varrho-1}$  when the last of the elements of  $\mathfrak{T}$  not belonging to  $\mathfrak{V}_{\varrho-1}$  is replaced by  $v_{\varrho-1}$ . In consequence of (1.),  $c_{\varrho-1,\nu-1} = u_{\nu-1}$  must be this last element; but that means that every element of  $\mathfrak{T}$  belongs either to  $\mathfrak{W}_{\varrho-1,\nu}$  or to  $\mathfrak{V}_{\varrho-1}$ . If therefore  $\mathfrak{T}'$  denotes the system into which  $\mathfrak{T}$  passes when  $v_{\varrho-1}$  is substituted for  $u_{\nu-1}$ , then every element of  $\mathfrak{T}'$  belongs either to  $\mathfrak{W}_{\varrho,\nu}$  or to  $\mathfrak{V}_{\varrho-1}$ ;  $\mathfrak{T}'$  is therefore a part of  $\mathfrak{W}'_{\varrho\nu}$ . On the other hand  $\mathfrak{T}'$  is equivalent to  $\mathfrak{T}$ , and the element contained in  $\mathfrak{T}$ ,  $a = u_{\nu-1} = c_{\varrho-1,\nu-1}$ ,

therefore depends algebraically on  $\mathfrak{W}'_{\mu\nu}$ . Since this contradicts what precedes, the assertion h) holds for all systems  $\mathfrak{W}'_{\mu\nu}$ , and thus e) is proved.

What is of interest for our purpose is solely the fact that the system  $\mathfrak{V}$ , as a part of  $\mathfrak{W}_\tau$ , is mapped one-to-one onto a part of  $\mathfrak{U}$  in the similar correspondence existing between  $\mathfrak{U} = \mathfrak{W}_0$  and  $\mathfrak{W}_\tau$ . If the systems  $\mathfrak{U}$  and  $\mathfrak{V}$  are equivalent, then it follows in the same way that a one-to-one map of  $\mathfrak{U}$  onto a part of  $\mathfrak{V}$  is possible. But from this it follows, by a known theorem of *Bernstein*, that a one-to-one correspondence between  $\mathfrak{U}$  and  $\mathfrak{V}$  is also possible, and thus:

3. *Equivalent irreducible systems have the same cardinal number.*

If a transcendental extension  $\mathfrak{L}$  of a field  $\mathfrak{K}$  is decomposed, by insertion of a field  $\mathfrak{K}(\mathfrak{S})$ , into a purely transcendental and an algebraic one, then we obtain from this one decomposition all possible ones by replacing the irreducible system  $\mathfrak{S}$  by all possible equivalent irreducible systems. The cardinal number of  $\mathfrak{S}$  is therefore completely determined by  $\mathfrak{K}$  and  $\mathfrak{L}$ ; we call it the *degree of transcendence of the extension* or *degree of transcendence of  $\mathfrak{L}$  with respect to  $\mathfrak{K}$* . To algebraic extensions we ascribe the degree of transcendence 0.

Let  $\mathfrak{L}$  be a field between  $\mathfrak{K}$  and  $\mathfrak{M}$ ,  $\mathfrak{S}$  a system of elements of  $\mathfrak{L}$  irreducible with respect to  $\mathfrak{K}$ ,  $\mathfrak{T}$  a system of elements of  $\mathfrak{M}$  irreducible with respect to  $\mathfrak{L}$ . Let  $\mathfrak{L}$  be algebraic with respect to  $\mathfrak{K}(\mathfrak{S})$ ,  $\mathfrak{M}$  with respect to  $\mathfrak{L}(\mathfrak{T})$ , so that the cardinal numbers  $s$  and  $t$  of  $\mathfrak{S}$  and  $\mathfrak{T}$  represent the degrees of transcendence of  $\mathfrak{L}$  with respect to  $\mathfrak{K}$  and of  $\mathfrak{M}$  with respect to  $\mathfrak{L}$ .<sup>E 127</sup> — With respect to  $\mathfrak{K}(\mathfrak{S} + \mathfrak{T})$  all elements of  $\mathfrak{L}$  and all of  $\mathfrak{T}$  are then algebraic. But by adjoining all these elements to  $\mathfrak{K}(\mathfrak{S} + \mathfrak{T})$  we obtain the field  $\mathfrak{L}(\mathfrak{T})$ , which is therefore algebraic with respect to  $\mathfrak{K}(\mathfrak{S} + \mathfrak{T})$ . Since likewise  $\mathfrak{M}$  is algebraic with respect to  $\mathfrak{L}(\mathfrak{T})$ ,  $\mathfrak{M}$  represents an algebraic extension of  $\mathfrak{K}(\mathfrak{S} + \mathfrak{T})$ . — We consider an arbitrary finite subsystem of  $\mathfrak{S} + \mathfrak{T}$  and represent it in the form  $\mathfrak{S}' + \mathfrak{T}'$ , where  $\mathfrak{S}'$  is a part of  $\mathfrak{S}$ ,  $\mathfrak{T}'$  a part of  $\mathfrak{T}$ .  $\mathfrak{S}'$  is irreducible with respect to  $\mathfrak{K}$ ,  $\mathfrak{T}'$  with respect to  $\mathfrak{L}$ , hence also with respect to  $\mathfrak{K}(\mathfrak{S}')$ . If therefore  $\mathfrak{S}'$  consists of the elements  $x_1, \dots, x_m$ ,  $\mathfrak{T}'$  of the elements  $y_1, \dots, y_n$ , then each of the elements  $x_1, \dots, x_m, y_1, \dots, y_n$  is transcendental with respect to the field that arises by adjoining the preceding ones to  $\mathfrak{K}$ , and therefore, with respect to  $\mathfrak{K}$ , none of these elements depends algebraically on the system of the remaining ones. With respect to  $\mathfrak{K}$  the system  $\mathfrak{S}' + \mathfrak{T}'$  is therefore irreducible, and since it represents an arbitrary finite subsystem of  $\mathfrak{S} + \mathfrak{T}$ ,  $\mathfrak{S} + \mathfrak{T}$ , too, is irreducible with respect to  $\mathfrak{K}$  (§ 22, 4.). The cardinal number of  $\mathfrak{S} + \mathfrak{T}$  is denoted by  $s + t$ , and the theorem therefore holds:

4. *An extension that is composed of two successive extensions of the degrees of transcendence  $s$  and  $t$  has the degree of transcendence  $s + t$ .*

One sees immediately that this also holds if  $s$  or  $t$  is equal to 0.

By the *absolute degree of transcendence* of a field  $\mathfrak{K}$  we understand its degree of transcendence with respect to the prime field, and we combine into a class  $K_{c,t}$  all those fields (or field types) that have the same characteristic  $c$  and the same absolute degree of transcendence  $t$ .  $c$  can be 0 or an arbitrary prime number,  $t$  0 or a natural number or an arbitrary transfinite cardinal number. In every class  $K_{c,t}$  we have two remarkable types. For if we carry out, on a prime field  $\mathfrak{P}_c$ , a purely transcendental extension of degree of transcendence  $t$ , we arrive at a well-determined type (§ 22, 5.), which belongs to the class  $K_{c,t}$  and may be denoted by  $\mathfrak{R}_{c,t}$ . Further, by § 21, 9., a definite algebraically closed type belongs to this — let it be called  $\mathfrak{A}_{c,t}$  — which arises from  $\mathfrak{R}_{c,t}$  by algebraic extension, and therefore likewise belongs to the class  $K_{c,t}$ .

5. If a field  $\mathfrak{R}'_{c,t}$  of the type  $\mathfrak{R}_{c,t}$  is extended algebraically to an algebraically closed field  $\mathfrak{A}'_{c,t}$ , then all fields between  $\mathfrak{R}'_{c,t}$  and  $\mathfrak{A}'_{c,t}$  belong to the class  $K_{c,t}$ . But also every type of the class  $K_{c,t}$  is represented by at least one field between  $\mathfrak{R}'_{c,t}$  and  $\mathfrak{A}'_{c,t}$ .

That all fields between  $\mathfrak{R}'_{c,t}$  and  $\mathfrak{A}'_{c,t}$  belong to the class  $K_{c,t}$  follows from the fact that they are algebraic with respect to  $\mathfrak{R}'_{c,t}$  and  $\mathfrak{R}'_{c,t}$  belongs to this class. Next, it follows from our hypotheses that  $\mathfrak{A}'_{c,t}$  is of the type  $\mathfrak{A}_{c,t}$ . Now let  $\mathfrak{K}$  be an arbitrary field of the class  $K_{c,t}$ ,  $\overline{\mathfrak{P}}_c$  the prime field contained in  $\mathfrak{K}$ . From  $\mathfrak{K}$  we can pick out a system  $\mathfrak{S}$  irreducible with respect to  $\overline{\mathfrak{P}}_c$  in such a way that  $\mathfrak{K}$  is algebraic with respect to  $\overline{\mathfrak{R}}_{c,t} = \overline{\mathfrak{P}}_c(\mathfrak{S})$ . If we extend  $\mathfrak{K}$  algebraically to an algebraically closed field  $\overline{\mathfrak{A}}_{c,t}$ , then this is also algebraic with respect to  $\overline{\mathfrak{R}}_{c,t}$ . From the membership of  $\mathfrak{K}$  in  $K_{c,t}$  it follows that  $\mathfrak{S}$  has the cardinal number  $t$ ,  $\overline{\mathfrak{R}}_{c,t}$  is of the type  $\mathfrak{R}_{c,t}$ ,  $\overline{\mathfrak{A}}_{c,t}$  of the type  $\mathfrak{A}_{c,t}$ . Further, it follows (cf. the proof of § 21, 9.) that  $\overline{\mathfrak{A}}_{c,t}$  can be mapped isomorphically onto  $\mathfrak{A}'_{c,t}$  in such a way that  $\overline{\mathfrak{R}}_{c,t}$  passes over into  $\mathfrak{R}'_{c,t}$ . In doing so,  $\mathfrak{K}$  is related isomorphically to a field between  $\mathfrak{R}'_{c,t}$  and  $\mathfrak{A}'_{c,t}$ ; the type of  $\mathfrak{K}$  is therefore represented among these fields. — If  $\mathfrak{K}$  is itself algebraically closed, then  $\mathfrak{K} = \overline{\mathfrak{A}}_{c,t}$  is of the type  $\mathfrak{A}_{c,t}$ . Consequently:

6. The type  $\mathfrak{A}_{c,t}$  is the only algebraically closed one of the class  $K_{c,t}$ . <sup>E 128</sup>

## § 24.

### Supplementary remarks of various content.

*The cardinal number* (power, number of the elements) *of a field*. — From the well-ordering theorem it follows easily that the cardinal numbers, too, form a well-ordered sequence, that the sum and the product of two cardinal numbers, of which at least one is transfinite, is equal to the greater, that the system of all finite subsets of an infinite set  $M$  has the same power as  $M$ . From this one concludes further that the number of the integral functions of an indeterminate  $x$  in an infinite field is not greater than the number of the elements of the field, and that the same holds for the zeros of these functions. Algebraic extension of an infinite field therefore does not raise its power. A further simple consequence of the theorems cited is that in the case  $t \geq \aleph_0$  (where  $\aleph_0$  denotes the smallest transfinite cardinal number, the power of the countable sets) the field  $\mathfrak{R}_{c,t}$ , and therefore every field of the class  $K_{c,t}$ , has the cardinal number  $t$ , while in the case of a finite  $t$  a field of the class  $K_{c,t}$ , if it is not finite (which can be the case only for  $c = p$ ,  $t = 0$ ), has  $\aleph_0$  elements. — For a field whose elements are not countable, the cardinal number therefore coincides with the absolute degree of transcendence. Since the continuum is not countable, one concludes (§ 23, 6.) that all algebraically closed fields of the power of the continuum and of characteristic 0 are isomorphic to one another. These fields include the field of complex numbers and the field of all algebraic functions of one or several variables, among others.

*The theorem of Lüroth*. — Theorem II of § 14 has the following counterpart:

If  $\mathfrak{K}(x)$  is a simple transcendental extension of  $\mathfrak{K}$ , then every field between  $\mathfrak{K}$  and  $\mathfrak{K}(x)$  is also simple with respect to  $\mathfrak{K}$ .

We can also formulate this theorem thus: If  $\mathfrak{L}$  is a purely transcendental extension of  $\mathfrak{K}$  with degree of transcendence 1, then every field between  $\mathfrak{K}$  and  $\mathfrak{L}$  also represents a purely transcendental extension of  $\mathfrak{K}$ . — The obvious question whether the same theorem holds for every purely transcendental extension has not yet been settled. <sup>E 129</sup>

In order to arrive at a proof of the theorem of *Lüroth*, we introduce beside  $x$  a new indeterminate  $t$  and consider the integral functions of  $t$  with coefficients from  $\mathfrak{K}(x)$ . To every such function  $g(t)$  there belongs a function, arising from it by multiplication by a factor from  $\mathfrak{K}(x)$ , *primitive with respect to*  $x$

$$\bar{g}(t) = \varphi_0(x)t^n + \varphi_1(x)t^{n-1} + \cdots + \varphi_n(x),$$

which is distinguished by the fact that its coefficients are integral functions of  $x$  that do not all have a common divisor. This function is determined up to a factor from  $\mathfrak{K}$ ; if one wants it to be completely determined, one may further decree that in  $\varphi_0(x)$  the coefficient of the highest power shall be  $\varepsilon$ . — One shows in a known manner that the product of two primitive functions is again primitive, and from this it follows at once that from an equation of the form  $f(t) = g(t) \cdot h(t)$ , where  $f(t)$ ,  $g(t)$ ,  $h(t)$  are integral functions of  $t$  with coefficients from  $\mathfrak{K}(x)$ , one again obtains a correct equation if one replaces these functions by the associated primitive ones.

Let  $\frac{\varphi(t)}{\psi(t)}$  be a rational function of  $t$  with coefficients from  $\mathfrak{K}$  in reduced form,  $m$  its degree ( $> 0$ ),  $y$  an element transcendental with respect to  $\mathfrak{K}(t)$ . Then the function

$$\varphi(t) - y \cdot \psi(t)$$

is of degree  $m$  in  $t$ , it is primitive in  $y$  and, as we shall show at once, irreducible in the field  $\mathfrak{K}(y)$ . For if one had a decomposition

$$\varphi(t) - y \cdot \psi(t) = g(t) \cdot h(t),$$

then on the transition to the functions primitive in  $y$  the left side would not change; we may therefore assume from the outset that  $g(t)$  and  $h(t)$  are primitive. Then one of these functions, say  $g(t)$ , would have to be free of  $y$ , the other of the first degree in  $y$ . But then one recognizes, by ordering according to powers of  $y$ , that  $g(t)$  would have to go into  $\varphi(t)$  and  $\psi(t)$ , whereas  $\varphi(t)$  and  $\psi(t)$  were presupposed to be relatively prime. — If we put  $y = \frac{\varphi(x)}{\psi(x)}$ , then  $\mathfrak{K}(y)$  becomes a field between  $\mathfrak{K}$  and  $\mathfrak{K}(x)$ , and  $x$  a zero of the function  $\varphi(t) - y \cdot \psi(t)$ , which is of degree  $m$  and irreducible in  $\mathfrak{K}(y)$ ; consequently  $[\mathfrak{K}(x) : \mathfrak{K}(y)] = m$ , i.e. the degree of  $\mathfrak{K}(x)$  with respect to  $\mathfrak{K}(y)$  is equal to the degree of  $y$  as a rational function of  $x$ . — We now show that the function

$$\psi(x) \cdot (\varphi(t) - y \cdot \psi(t)) = \varphi(t)\psi(x) - \psi(t)\varphi(x)$$

is primitive in  $x$  as an integral function of  $t$ . For this purpose we put

$$\varphi(x) = a_0 + a_1x + \cdots, \quad \psi(x) = b_0 + b_1x + \cdots,$$

so that

$$\varphi(t)\psi(x) - \psi(t)\varphi(x) = (a_0\psi(x) - b_0\varphi(x)) + (a_1\psi(x) - b_1\varphi(x))t + \cdots$$

holds. Now if all the coefficients  $\gamma_i = a_i\psi(x) - b_i\varphi(x)$  had a common factor  $\chi(x)$ , then this would also go into all the expressions

$$\gamma_i b_k - \gamma_k b_i = (a_i b_k - a_k b_i)\psi(x), \quad \gamma_i a_k - \gamma_k a_i = (a_i b_k - a_k b_i)\varphi(x),$$

and hence, because we can (since  $m > 0$ ) choose  $i$  and  $k$  so that  $a_i b_k - a_k b_i \neq 0$  holds, also into  $\varphi(x)$  and  $\psi(x)$ , which contradicts the assumption that  $\varphi(x)$  and  $\psi(x)$  are relatively prime. If therefore  $\varphi(t)\psi(x) - \psi(t)\varphi(x)$  breaks up into two factors in the domain of integrity  $\mathfrak{K}[t, x]$ , then none of them can be a function of  $x$  alone. In exactly the same way one shows that neither of the two factors can be a function of  $t$  alone.

Now let  $\mathfrak{M}$  be an arbitrary field, different from  $\mathfrak{K}$ , between  $\mathfrak{K}$  and  $\mathfrak{K}(x)$ . Then  $\mathfrak{K}(x)$  is finite with respect to  $\mathfrak{M}$ ; for if  $y$  is an element of  $\mathfrak{M}$  not contained in  $\mathfrak{K}$ , then, as we saw,  $\mathfrak{K}(x)$  is finite with respect to  $\mathfrak{K}(y)$ , and  $\mathfrak{M}$  lies between  $\mathfrak{K}(y)$  and  $\mathfrak{K}(x)$ . Let

$$(1.) \quad [\mathfrak{K}(x) : \mathfrak{M}] = n.$$

Then  $x$  is a zero of an irreducible function of degree  $n$  from  $\mathfrak{M}$

$$g(t) = t^n + u_1 t^{n-1} + \cdots + u_n,$$

whose coefficients, since  $x$  is transcendental with respect to  $\mathfrak{K}$ , cannot all occur in  $\mathfrak{K}$ . Let  $y = \frac{\varphi(x)}{\psi(x)}$  in reduced form be one of the coefficients of  $g(t)$  that do not occur in  $\mathfrak{K}$ ,  $m$  its degree in  $x$ . Then  $\mathfrak{M}$  lies between  $\mathfrak{K}(y)$  and  $\mathfrak{K}(x)$ , and we obtain  $[\mathfrak{K}(x) : \mathfrak{K}(y)] = m$ , hence because of (1.)

$$(2.) \quad [\mathfrak{M} : \mathfrak{K}(y)] = \frac{m}{n}, \quad m \geq n.$$

To  $g(t)$  there belongs a function primitive in  $x$

$$\bar{g}(t) = \varphi_0(x)t^n + \varphi_1(x)t^{n-1} + \cdots + \varphi_n(x),$$

where  $\frac{\varphi_k(x)}{\varphi_0(x)} = u_k$  ( $k = 1, \dots, n$ ). Since  $y$  also occurs among the functions  $u_k$ ,  $\bar{g}(t)$  is at least of degree  $m$  in  $x$ . — Now  $x$  is a zero of the function  $\varphi(t) - y\psi(t)$  belonging to the field  $\mathfrak{M}$ ; this must therefore be divisible by the function  $g(t)$  irreducible in  $\mathfrak{M}$ . We therefore obtain

$$\varphi(t) - \frac{\varphi(x)}{\psi(x)} \cdot \psi(t) = g(t) \cdot h(t),$$

and, if we pass over to the associated functions primitive in  $x$ ,

$$(3.) \quad \varphi(t)\psi(x) - \psi(t)\varphi(x) = \bar{g}(t)\bar{h}(t).$$

The left side of (3.) is of degree  $m$  in  $x$ ,  $\bar{g}(t)$  is, as we saw, *at least* of degree  $m$  in  $x$ ; from (3.) it therefore now follows that  $\bar{g}(t)$  must be *exactly* of degree  $m$  in  $x$  and  $\bar{h}(t)$  free of  $x$ . Since it was further shown that  $\varphi(t)\psi(x) - \psi(t)\varphi(x)$  can have no factor that is a function of  $t$  alone,  $\bar{h}(t)$  cannot contain  $t$  either, and we obtain, by comparing the degrees in  $t$  on both sides of (3.),

$$m = n$$

and from this by (2.)

$$\mathfrak{M} = \mathfrak{K}(y).$$

This proves the theorem of *Lüroth*.

This “rational” proof of the theorem has the advantage that it holds without any restriction for all fields  $\mathfrak{K}$ , whereas the usual form of proof presupposes that the field  $\mathfrak{K}$  is perfect and

has infinitely many elements. This form of proof requires cumbersome modifications in the case of an imperfect field; for finite fields it fails entirely.

*The algebraically closed extensions.* — The demonstration of the existence of an algebraically closed extension belonging to a given field  $\mathfrak{K}$  does not yet give us a method for actually producing such an extension. Even for the arrangement of the elements of a field  $\mathfrak{K}$  into a well-ordered system, to which that proof refers, there is in the nature of things no general method. However, the production of an algebraically closed extension is by no means bound to an already executed well-ordering of  $\mathfrak{K}$ . Two examples of this. In both, the ground field is of the power of the continuum — a power of which, as is known, it has not yet even been possible to establish whether it equals  $\aleph_1$ , the second transfinite cardinal number. Fields of this power include, among others, the field of the real or of the complex numbers, the field of the rational functions of a variable  $z$  with complex coefficients, and then also the field  $K(p)$  of the so-called  $p$ -adic numbers introduced by *K. Hensel*<sup>\*)</sup>.

In the case  $\mathfrak{K} = K(p)$  we reach the goal on the basis of various investigations that *Hensel* has carried out in the work cited and in a treatise that appeared recently in this Journal<sup>16\*\*)</sup>. Essential here is the demonstration that every integral function  $f(x)$  from  $K(p)$  breaks up completely in a field that arises from  $K(p)$  by adjunction of a zero of a function  $g(x)$  that is irreducible in  $K(p)$  and whose coefficients are ordinary integers. This demonstrates that the system of all integral functions from  $K(p)$  is equivalent to the system  $S$  of integral functions with integer coefficients. Now while the first-named system is of the power of the continuum, the system  $S$  is countable and can therefore be ordered into a simple sequence. If we have decided on some arrangement and denote the functions thus ordered by  $f_n(x)$ , where  $n$  runs through the natural numbers, then by the methods of *Hensel* we can compute the first function from  $S$  that is equivalent to the system

$$f_1(x), f_2(x), \dots, f_n(x)$$

and that is irreducible in  $K(p)$  and moreover normal, by a finite procedure. If this is denoted by  $\varphi_n(x)$ , then we have a system of normal functions

$$\varphi_1(x), \varphi_2(x), \dots, \varphi_n(x), \dots,$$

in which every segment is subordinate to the following function. If we introduce a system of symbols  $j_n$ , with the decree that  $j_n$  shall be a zero of  $\varphi_n(x)$ , then we obtain a system of extensions of the field  $\mathfrak{K} = K(p)$ :

$$(4.) \quad \mathfrak{K}_1 = \mathfrak{K}(j_1), \dots, \mathfrak{K}_n = \mathfrak{K}(j_n), \dots$$

If  $r_n$  denotes the degree of  $\varphi_n(x)$ , then every element of  $\mathfrak{K}_n$  is representable in the form  $g(j_n)$ , where  $g(x)$  is an integral function from  $K(p)$  and its degree is smaller than  $r_n$ .  $r_{n-1}$  of the elements of  $\mathfrak{K}_n$  are zeros of  $\varphi_{n-1}(x)$ . Now if we want every field of the sequence (4.) to be part of the following one, so that, as in the case treated in § 16, these fields in their totality constitute the algebraically closed field sought, then we must still decree which of the zeros of

<sup>\*)</sup> Theorie der algebraischen Zahlen I (Leipzig and Berlin 1908).

<sup>\*\*) Vol. 136 (1909), p. 183.</sup>

<sup>16</sup> The Journal für die reine und angewandte Mathematik. — Trans.

$\varphi_{n-1}(x)$  contained in  $\mathfrak{K}_n$  shall be equal to  $j_{n-1}$ . Now it is true that it has so far not been possible to represent  $K(p)$  or any system of the power of the continuum as a well-ordered system; on the other hand  $K(p)$  can very easily be represented as an ordered system<sup>\*)</sup>. On the basis of such an ordering of  $K(p)$  we obtain an arrangement of the integral functions from  $K(p)$  by prescribing that the function  $g(x) = a_0 + a_1x + \cdots$  shall precede the function  $h(x) = b_0 + b_1x + \cdots$  if, in the case  $a_k = b_k$  ( $k < n$ ),  $a_n \neq b_n$ , the element  $a_n$  is earlier than  $b_n$ . Then we can stipulate that, if  $g(x)$  is the first function from  $K(p)$  that, for  $x = j_n$ , goes over into a zero of  $\varphi_{n-1}(x)$ ,  $g(j_n) = j_{n-1}$  shall hold. — This solves the problem.

In the second place we consider the field  $\mathfrak{K} = \mathfrak{C}(z)$ , which arises from the field  $\mathfrak{C}$  of the complex numbers by adjunction of a transcendental element  $z$  (field of the rational functions of one variable). Here the system of all integral functions of an indeterminate  $x$  in  $\mathfrak{K}$  is no longer equivalent to a countable system, but here the production of an algebraically closed extension of  $\mathfrak{K}$  (without the principle of choice) succeeds easily with the resources of analysis. Namely, let  $\mathfrak{A}$  be the system of all series, convergent for sufficiently small values of  $r$ , of the form

$$\sum_{k=q}^{+\infty} a_k r^{\frac{k}{n}} \left( \cos \frac{k}{n} \varphi + i \sin \frac{k}{n} \varphi \right),$$

where  $r$  denotes a positive,  $\varphi$  a real variable,  $n$  any natural number,  $q$  any integer,  $r^{\frac{k}{n}}$  is always to be taken positive, and the coefficients  $a_k$ , whose index  $k$  runs through all integers from  $q$  upwards, are arbitrary complex numbers. Every such series represents, in its domain of convergence, a single-valued function of  $r$  and  $\varphi$ . Two series count as the same element of  $\mathfrak{A}$  if they converge to the same value for all pairs of values  $r, \varphi$  of their domain of convergence. To two elements  $\alpha, \beta$  from  $\mathfrak{A}$  there belong, as one shows in a known manner, two further ones  $\gamma, \delta$  such that, within the common area of convergence, the relations

$$(5.) \quad \alpha + \beta = \gamma, \quad \alpha \cdot \beta = \delta$$

hold between  $\alpha, \beta, \gamma, \delta$  as functions of  $r$  and  $\varphi$ . If we let the equations (5.) count as equations of composition for  $\mathfrak{A}$ , then  $\mathfrak{A}$  becomes a system with double composition, which easily proves to be an algebraically closed field. To every element  $R(z)$  of  $\mathfrak{K} = \mathfrak{C}(z)$  there corresponds in  $\mathfrak{A}$  an element  $\alpha$  such that, for sufficiently small values of  $r$ ,  $R(r(\cos \varphi + i \sin \varphi))$  becomes equal to  $\alpha$ . The field  $\mathfrak{K}$  is thus mapped isomorphically onto a subfield  $\mathfrak{K}'$  of  $\mathfrak{A}$ , and since  $\mathfrak{A}$  is algebraically closed, the elements of  $\mathfrak{A}$  algebraic with respect to  $\mathfrak{K}'$  form a field  $\mathfrak{A}'$  that is algebraically closed and algebraic with respect to  $\mathfrak{K}'$ .

*Isomorphic map of a field onto a subfield.* — If  $\mathfrak{L}$  is an algebraic extension of the field  $\mathfrak{K}$ ,  $\mathfrak{L}'$  a field between  $\mathfrak{K}$  and  $\mathfrak{L}$  and different from  $\mathfrak{L}$ ,  $\alpha$  an element of  $\mathfrak{L}$  not contained in  $\mathfrak{L}'$ ,  $\varphi(x)$  the irreducible function from  $\mathfrak{K}$  with the zero  $\alpha$ , then the number of the irreducible factors of  $\varphi(x)$  is greater in the field  $\mathfrak{L}$  than in the field  $\mathfrak{L}'$ ,  $\mathfrak{L}$  and  $\mathfrak{L}'$  are therefore not equivalent extensions. If  $\mathfrak{K}$  is a prime field, then  $\mathfrak{L}$  and  $\mathfrak{L}'$  cannot be isomorphic, because under an isomorphic correspondence between  $\mathfrak{L}$  and  $\mathfrak{L}'$  every element of the prime field would remain unchanged, and  $\mathfrak{L}$  and  $\mathfrak{L}'$  would therefore represent equivalent extensions of  $\mathfrak{K}$ . This proves:

1. *An absolutely algebraic field is isomorphic to no proper part of itself.*

<sup>\*)</sup> Hensel, Neue Grundlagen der Arithmetik. This Journal vol. 127, p. 52, 53.

Since every subfield of an absolutely algebraic field is again absolutely algebraic, there holds

2. *Two subfields of an absolutely algebraic field, of which the one is a proper part of the other, cannot be isomorphic.*

The property denoted by 2. is characteristic of the absolutely algebraic fields; for if the field  $\mathfrak{L}$  is not absolutely algebraic and  $x$  is an element transcendental with respect to its prime field  $\mathfrak{P}$ , then  $\mathfrak{P}(x^2)$  is a proper part of  $\mathfrak{P}(x)$ , but both fields are isomorphic. On the other hand 1. expresses no characteristic property of absolutely algebraic fields; for one sees very easily that e.g. a field of the type  $\mathfrak{A}_{c,t}$ , where  $t$  is finite, cannot be isomorphic to any proper part of itself.

Among the fields that are isomorphic to a proper part of themselves, we have to distinguish two kinds. A representative of the first kind is the field  $\mathfrak{R}_{c,1}$ . It has infinitely many subfields, which, however, except for the prime field, are all of the type  $\mathfrak{R}_{c,1}$  by the theorem of *Lüroth*. A field lying between a field  $\mathfrak{R}_{c,1}$  and an isomorphic subfield is therefore always again isomorphic to  $\mathfrak{R}_{c,1}$ . The field  $\mathfrak{A}_{c,t}$  for infinite  $t$  is of another kind. By adjunction of a transcendental element  $x$  there arises from  $\mathfrak{A}_{c,t}$  a field  $\mathfrak{A}_{c,t}(x)$  that again has the degree of transcendence  $t$ , but is evidently not algebraically closed, hence not of the type  $\mathfrak{A}_{c,t}$ . But if we extend  $\mathfrak{A}_{c,t}(x)$  algebraically to an algebraically closed field, then this is again of the type  $\mathfrak{A}_{c,t}$ . Here, therefore, between two isomorphic fields there lies a non-isomorphic one. Every time such a case occurs, we have two fields  $\mathfrak{R}_1, \mathfrak{R}_2$  of different types, each of which is isomorphic to a part of the other. The subfields of  $\mathfrak{R}_1$  therefore represent the same types as the subfields of  $\mathfrak{R}_2$ .

## Appendix A

Outline of *Galois Theory*<sup>\*)</sup>

By Reinhold Baer and Helmut Hasse

*This appendix is not by Steinitz. Its references to Steinitz's text, to the Explanatory Notes (Appendix B) and to itself are to the pages of this edition.*

We consider a *ground field*  $\mathfrak{K}$  and a field  $\mathfrak{N}$  containing  $\mathfrak{K}$ , algebraic over  $\mathfrak{K}$  and normal<sup>\*\*)</sup> , both of which we wish to *hold fixed* in what follows. Our task is to gain an overview of the *intermediate fields*  $\mathfrak{Z}$  between  $\mathfrak{K}$  and  $\mathfrak{N}$  by studying the so-called *Galois group*<sup>\*\*\*)</sup>  of  $\mathfrak{N}$ ; we shall further show for which classes of extensions of  $\mathfrak{K}$  the procedure of studying the subgroups of the *Galois group* gives information about the intermediate fields.

*The totality  $N$  of the automorphisms of  $\mathfrak{N}$  [= isomorphic maps of  $\mathfrak{N}$  onto itself] for which  $\mathfrak{K}$  remains elementwise invariant is called the group of  $\mathfrak{N}$ .*

One verifies at once that  $N$  is a group.

We now make an assignment of intermediate fields and subgroups:

*If  $U$  is a subgroup of  $N$ , let there be assigned to  $U$  the totality  $\mathfrak{N}(U)$  of all and only those elements of  $\mathfrak{N}$  that go into themselves under every map in  $U$ .*

*If  $\mathfrak{Z}$  is an intermediate field between  $\mathfrak{K}$  and  $\mathfrak{N}$ , let there be assigned to  $\mathfrak{Z}$  the totality  $N(\mathfrak{Z})$  of all and only those elements of  $N$  that leave every element of  $\mathfrak{Z}$  invariant.*

Then we have:

*$\mathfrak{N}(U)$  is always an intermediate field between  $\mathfrak{K}$  and  $\mathfrak{N}$ .*

*$N(\mathfrak{Z})$  is always a subgroup of  $N$ .*

For:

Since  $U$  is a subset of  $N$ ,  $U$  leaves all elements of  $\mathfrak{K}$  invariant;  $\mathfrak{N}(U)$  contains  $\mathfrak{K}$ . Since further the elements of  $U$  are isomorphisms, they leave invariant, along with  $\mathfrak{a}$  and  $\mathfrak{b}$ , also  $\mathfrak{a} \pm \mathfrak{b}$ ,  $\mathfrak{a} \cdot \mathfrak{b}$  and  $\mathfrak{a} : \mathfrak{b}$  for  $\mathfrak{b} \neq 0$ , i.e.  $\mathfrak{N}(U)$  is a subfield of  $\mathfrak{N}$ .

If the element  $a$  of  $N(\mathfrak{Z})$  leaves the field  $\mathfrak{Z}$  elementwise invariant, so do  $a^{-1}$  and, along with  $a$  and  $b$ , also  $a \cdot b$ .

<sup>\*)</sup> The account of *Galois* theory given here rests on ideas of *Steinitz* and *Dedekind*.

Cf. 1. *H. Hasse*: Höhere Algebra II (1927).

2. *O. Haupt*: Einführung in die Algebra II (1929), Fünfter Abschnitt.

3. *A. Loewy*: Neue elementare Begründung und Erweiterung der *Galoisschen* Theorie, Sitz.-Ber. d. Heidelberger Ak. d. Wiss. Math.-nat. Kl. 1925 (7) and 1927 (1).

4. *F. K. Schmidt*: Bemerkungen zum *Brandtschen* Gruppoid, Sitz.-Ber. d. Heidelberger Ak. d. Wiss. Math.-nat. Kl. 1927 (8), p. 97 ff.

5. *W. Krull*: *Galoissche* Theorie der unendlichen algebraischen Erweiterungen, Math. Ann. vol. 100 (1928), p. 687.

6. *R. Baer*: Beiträge zur *Galoisschen* Theorie, Sitz.-Ber. d. Heidelberger Ak. d. Wiss. Math.-nat. Kl. 1928 (14).

7. *E. Steinitz*: Algebraische Theorie der Körper, which we cite in what follows merely by giving the pages or sections and theorems, while our Explanatory Notes on it are cited simply by their numbers.

<sup>\*\*)</sup>  Cf. p. 28.

<sup>\*\*\*)</sup>  Cf. p. 48.

Further, as follows at once from the definition:

$$N[\mathfrak{N}(U)] \geq U^* \quad \Bigg| \quad \mathfrak{N}[N(\mathfrak{Z})] \geq \mathfrak{Z}^*.$$

We investigate when the equations:

$$N[\mathfrak{N}(U)] = U \quad \Bigg| \quad \mathfrak{N}[N(\mathfrak{Z})] = \mathfrak{Z}$$

*always* hold. If both equations hold, we have obtained the desired one-to-one assignment between subgroups of  $N$  on the one hand and intermediate fields between  $\mathfrak{K}$  and  $\mathfrak{N}$  on the other.

As a result of this investigation it will turn out:

*The two equations always hold if and only if*

1.  $\mathfrak{N}$  is of the first kind over  $\mathfrak{K}$  and
2.  $\mathfrak{N}$  is finite over  $\mathfrak{K}^{**}$ .

**Definition 1:** Two fields  $\mathfrak{Z}$  and  $\overline{\mathfrak{Z}}$  between  $\mathfrak{K}$  and  $\mathfrak{N}$  are called *conjugate [over  $\mathfrak{K}$ ]* if they can be carried into each other by automorphisms in  $N$ .

**Lemma 1:** Two intermediate fields  $\mathfrak{Z}$  and  $\overline{\mathfrak{Z}}$  between  $\mathfrak{K}$  and  $\mathfrak{N}$  are conjugate if and only if they are equivalent extensions of  $\mathfrak{K}$ .

The necessity of the condition is trivial. To prove its sufficiency, we prove somewhat more, namely:

**Lemma 1a:** If  $\mathfrak{Z}$  and  $\overline{\mathfrak{Z}}$  are two fields between  $\mathfrak{K}$  and  $\mathfrak{N}$  and there is an isomorphism  $\pi$  between  $\mathfrak{Z}$  and  $\overline{\mathfrak{Z}}$  that assigns each element of  $\mathfrak{K}$  to itself, then there is an automorphism  $p$  in  $N$  that extends  $\pi$ .

For the proof we first think of a well-ordering of  $\mathfrak{N}$  as given, and then construct two chains of fields and a chain of isomorphisms between the fields of the two chains.

1.  $\mathfrak{K}_0 = \mathfrak{Z}$ ,  $\mathfrak{L}_0 = \overline{\mathfrak{Z}}$ ,  $\pi_0 = \pi$ .
2. Suppose already constructed for all  $\mu < \nu$ : the field  $\mathfrak{K}_\mu$  between  $\mathfrak{K}$  and  $\mathfrak{N}$ , the field  $\mathfrak{L}_\mu$  between  $\mathfrak{K}$  and  $\mathfrak{N}$  and the isomorphism  $\pi_\mu$  between  $\mathfrak{K}_\mu$  and  $\mathfrak{L}_\mu$ ; for  $\varrho < \mu$  let  $\mathfrak{K}_\varrho$  be a subfield of  $\mathfrak{K}_\mu$ ,  $\mathfrak{L}_\varrho$  a subfield of  $\mathfrak{L}_\mu$ , and let  $\pi_\varrho$  be extended by  $\pi_\mu$ .

*Case 1:* Let  $\nu$  not be a limit number. Then let  $\mathfrak{a}_\nu$  be the first element of  $\mathfrak{N}$  that does not yet occur in  $\mathfrak{K}_{\nu-1}$  [if there is none, we have already reached the end of our construction], and  $\mathfrak{K}_\nu = \mathfrak{K}_{\nu-1}(\mathfrak{a}_\nu)$ .

Since  $\mathfrak{N}$  is algebraic over  $\mathfrak{K}$ ,  $\mathfrak{a}_\nu$  satisfies an irreducible equation  $\varphi_\nu(x) = 0$  with coefficients in  $\mathfrak{K}_{\nu-1}$ . To this equation  $\pi_{\nu-1}$  assigns a certain equation  $\psi_\nu(x) = 0$  with coefficients in  $\mathfrak{L}_{\nu-1}$ , necessarily also irreducible. We then assert:

$\varphi_\nu(x)$  and  $\psi_\nu(x)$  are divisors of the same irreducible polynomial  $\chi_\nu(x)$  with coefficients in  $\mathfrak{K}$ .

For let  $\chi_\nu(x) = \varphi_\nu(x) \cdot f_\nu(x)$ ; then  $f_\nu(x)$  is also a polynomial with coefficients in  $\mathfrak{K}_{\nu-1}$ . To this  $\pi_{\nu-1}$  assigns a polynomial  $g_\nu(x)$  with coefficients in  $\mathfrak{L}_{\nu-1}$ . Since finally  $\pi_{\nu-1}$  extends

<sup>\*)</sup> If  $A$  and  $B$  are two sets,  $A \geq B$  means that  $B$  is a subset of  $A$ .

<sup>\*\*) Here 1. goes back to *E. Steinitz*, 2. to *W. Krull*.</sup>

the isomorphism  $\pi_0 = \pi$ , and therefore assigns every element of  $\mathfrak{K}$  to itself,  $\pi_{\nu-1}$  assigns the polynomial  $\chi_\nu(x)$  to itself, and so we have:  $\chi_\nu(x) = \psi_\nu(x) \cdot g_\nu(x)$ , which proves our assertion.

Since  $\chi_\nu(x)$  has the zero  $\mathfrak{a}_\nu$  in  $\mathfrak{N}$  and  $\mathfrak{N}$  is normal over  $\mathfrak{K}$ ,  $\chi_\nu(x)$ , and hence also  $\varphi_\nu(x)$  and  $\psi_\nu(x)$ , break up into linear factors in  $\mathfrak{N}$ . So there is a zero in  $\mathfrak{N}$ , and hence also a first zero  $\mathfrak{b}_\nu$  of  $\psi_\nu(x)$  in the well-ordering of  $\mathfrak{N}$ . We put  $\mathfrak{L}_\nu = \mathfrak{L}_{\nu-1}(\mathfrak{b}_\nu)$ .

By the theorem stated in Erl. 53 there is therefore an isomorphism  $\pi_\nu$  between  $\mathfrak{K}_\nu$  and  $\mathfrak{L}_\nu$  that extends  $\pi_{\nu-1}$  and in particular assigns  $\mathfrak{b}_\nu$  to  $\mathfrak{a}_\nu^{*})$ .

*Case 2:* Let  $\nu$  be a limit number. Then let  $\mathfrak{K}_\nu$  be the union of all  $\mathfrak{K}_\mu$  with  $\mu < \nu$ , and  $\mathfrak{L}_\nu$  the union of all  $\mathfrak{L}_\mu$  with  $\mu < \nu$ . By § 2, Theorem 2 these  $\mathfrak{L}_\nu$  and  $\mathfrak{K}_\nu$  are fields between  $\mathfrak{K}$  and  $\mathfrak{N}$ . Further let  $\pi_\nu$  be the union isomorphism (cf. Erl. 111) of all  $\pi_\mu$  with  $\mu < \nu$ .

This process is continued until at some point  $\mathfrak{K}_\sigma = \mathfrak{N}$  [ $\sigma$  is then certainly at most equal to the order type of  $\mathfrak{N}$ ]. We assert:

$$\mathfrak{L}_\sigma = \mathfrak{N}.$$

For if  $\lambda_\sigma(x)$  is an irreducible, non-linear polynomial in  $\mathfrak{L}_\sigma$ , then  $\pi_\sigma$  assigns to it an irreducible, non-linear polynomial  $\varkappa_\sigma(x)$  with coefficients in  $\mathfrak{K}_\sigma$ . As shown above,  $\lambda_\sigma(x)$  and  $\varkappa_\sigma(x)$  are then divisors of the same irreducible polynomial  $\varkappa(x)$  in  $\mathfrak{K}$ . Since  $\mathfrak{N}$  is normal over  $\mathfrak{K}$  and  $\varkappa_\sigma(x)$  has no zero in  $\mathfrak{N}$  [ $\mathfrak{K}_\sigma = \mathfrak{N}$ ],  $\varkappa(x)$ , and hence also its divisor  $\lambda_\sigma(x)$ , has no zeros in  $\mathfrak{N}$ , i.e. an irreducible equation in  $\mathfrak{L}_\sigma$  that has zeros in  $\mathfrak{N}$  is linear, so its solutions belong to  $\mathfrak{L}_\sigma$ , which proves our assertion.

If we now put  $p = \pi_\sigma$ , then  $p$  is the desired automorphism; for  $\pi_\sigma$  extends  $\pi_0 = \pi$  and is an isomorphism between  $\mathfrak{K}_\sigma = \mathfrak{N}$  and  $\mathfrak{L}_\sigma = \mathfrak{N}$ , i.e. an automorphism in  $N$  extending  $\pi$ .

**Definition 2:** Two elements  $\mathfrak{a}_1$  and  $\mathfrak{a}_2$  of  $\mathfrak{N}$  are called conjugate [over  $\mathfrak{K}$ ], if there is an automorphism  $a$  in  $N$  that carries  $\mathfrak{a}_1$  into  $\mathfrak{a}_2$ .

**Lemma 2:** The elements  $\mathfrak{a}_1$  and  $\mathfrak{a}_2$  are conjugate over  $\mathfrak{K}$  if and only if they satisfy the same irreducible equation in  $\mathfrak{K}$ .

A. Let  $\mathfrak{a}_1$  and  $\mathfrak{a}_2$  be conjugate and say  $\mathfrak{a}_2 = a(\mathfrak{a}_1)$ . Further let

$$f(x) = \sum_{i=0}^n \mathfrak{c}_i x^i = 0$$

be the irreducible equation in  $\mathfrak{K}$  that  $\mathfrak{a}_1$  satisfies, i.e.

$$\sum_{i=0}^n \mathfrak{c}_i \mathfrak{a}_1^i = 0.$$

Since under  $a$  the elements of  $\mathfrak{K}$  each go into themselves, the application of  $a$  to the above equation yields:

$$\sum_{i=0}^n \mathfrak{c}_i \mathfrak{a}_2^i = 0,$$

i.e.  $\mathfrak{a}_2$  too is a zero of  $f(x)$ .

B. Conversely, suppose  $\mathfrak{a}_1$  and  $\mathfrak{a}_2$  satisfy the same irreducible equation in  $\mathfrak{K}$ . Then by the theorem stated in Erl. 53 there is an isomorphism  $\pi$  between  $\mathfrak{K}(\mathfrak{a}_1)$  and  $\mathfrak{K}(\mathfrak{a}_2)$  that assigns

---

<sup>\*)</sup> This determines  $\pi_\nu$  uniquely.

every element of  $\mathfrak{K}$  to itself and  $\mathfrak{a}_2$  to  $\mathfrak{a}_1$ . By Lemma 1a,  $\pi$  can be extended to a desired automorphism  $a$  in  $N^*$ ).

**Theorem 1:** *A field  $\mathfrak{Z}$  between  $\mathfrak{K}$  and  $\mathfrak{N}$  is normal if and only if it is identical with its conjugates, i.e. if it goes into itself under all automorphisms in  $N$ .*

A. Suppose  $\mathfrak{Z}$  goes into itself under all automorphisms in  $N$ ; let  $\mathfrak{a}$  be an arbitrary element of  $\mathfrak{Z}$ ,  $\alpha(x) = 0$  the irreducible equation in  $\mathfrak{K}$  that  $\mathfrak{a}$  satisfies, and  $\mathfrak{b}$  an arbitrary other root of  $\alpha(x) = 0$ . By Lemma 2 there is an automorphism in  $N$  that carries  $\mathfrak{a}$  into  $\mathfrak{b}$ ; so  $\mathfrak{b}$  belongs to  $\mathfrak{Z}$ , so  $\alpha(x)$  breaks up completely in  $\mathfrak{Z}$  and, since this holds for every irreducible  $\alpha(x)$  in  $\mathfrak{K}$  that has a zero in  $\mathfrak{Z}$ ,  $\mathfrak{Z}$  is normal over  $\mathfrak{K}$ .

B. Conversely, if  $\mathfrak{Z}$  is normal over  $\mathfrak{K}$  and  $\mathfrak{a}$  an arbitrary element of  $\mathfrak{Z}$ , then under automorphisms in  $N$ , by Lemma 2,  $\mathfrak{a}$  goes only into elements  $\mathfrak{b}$  that satisfy the same irreducible equation in  $\mathfrak{K}$  as  $\mathfrak{a}$  and that therefore, because  $\mathfrak{Z}$  is normal, themselves belong to  $\mathfrak{Z}$ . So  $\mathfrak{Z}$  goes under all automorphisms of  $N$  into a part of itself. But since with  $a$  also  $a^{-1}$  belongs to  $N$ ,  $\mathfrak{Z}$  goes under automorphisms in  $N$  exactly into itself.

From Theorem 1 there follows immediately the

**Addendum 1:** *If  $\mathfrak{N}_1$  is a field containing  $\mathfrak{N}$ , normal and algebraic over  $\mathfrak{K}$  [e.g. an algebraically closed one], then a field  $\mathfrak{Z}$  between  $\mathfrak{K}$  and  $\mathfrak{N}$  is normal if and only if it goes into itself under all automorphisms of  $\mathfrak{N}_1$  that leave  $\mathfrak{K}$  elementwise invariant.*

**Addendum 2:** *If the field  $\mathfrak{Z}$  between  $\mathfrak{K}$  and  $\mathfrak{N}$  just suffices to break up a set  $\Sigma$  of polynomials in  $\mathfrak{K}$  completely, then  $\mathfrak{Z}$  is normal over  $\mathfrak{K}$ .*

*Proof*<sup>\*\*)</sup>: Since  $\mathfrak{Z}$  just suffices for the breaking up of the polynomials in  $\Sigma$ ,  $\mathfrak{Z}$  can be obtained from  $\mathfrak{K}$  by adjunction of all the zeros [contained in  $\mathfrak{N}$ ] of the polynomials in  $\Sigma$ . By Lemma 2, under automorphisms in  $N$  this system  $\mathfrak{S}$  of all zeros of polynomials in  $\Sigma$  goes into itself; hence  $\mathfrak{Z} = \mathfrak{K}(\mathfrak{S})$  goes into itself under all automorphisms in  $N$ , and is therefore normal over  $\mathfrak{K}$  by Theorem 1.

**Definition 3:** *If  $\mathfrak{Z}$  is a field between  $\mathfrak{K}$  and  $\mathfrak{N}$ , let the mapping degree  $A[\mathfrak{Z} : \mathfrak{K}]$  of  $\mathfrak{Z}$  over  $\mathfrak{K}$  be the cardinality of the set of the distinct isomorphisms of  $\mathfrak{Z}$  effected by automorphisms in  $N$  [which need not all map  $\mathfrak{Z}$  onto itself], i.e. the cardinality of the set of cosets of  $N$  with respect to  $N(\mathfrak{Z})$ , the index of  $N(\mathfrak{Z})$  in  $N$ .*

**Theorem 2:** *We have*

$$A[\mathfrak{Z} : \mathfrak{K}] = 1,$$

*if and only if either  $\mathfrak{Z} = \mathfrak{K}$  or  $\mathfrak{Z}$  is a root field<sup>\*\*\*)</sup> over  $\mathfrak{K}$ .*

*Proof:* For by Lemma 2 the element  $\mathfrak{a}$  of  $\mathfrak{Z}$  goes into itself under all automorphisms in  $N$  if no element different from  $\mathfrak{a}$  satisfies the irreducible equation  $\alpha(x) = 0$  in  $\mathfrak{K}$  that  $\mathfrak{a}$  satisfies. But by p. 33, equation (4), this is the case if and only if either  $\alpha(x)$  is linear or  $\alpha(x) = x^{p^n} - \mathfrak{c} = 0$ , where in the second case  $p \neq 0$  is the characteristic of  $\mathfrak{K}$ .

<sup>\*)</sup> That the use of Lemma 1a in the proof of Lemma 2 is grounded in the nature of the matter is shown by the theorem that extensions which share with the normal extensions the property stated in Lemma 2 also share with them that of Lemma 1a; cf. *R. Baer: Abbildungseigenschaften algebraischer Erweiterungen*, § 3 (to appear shortly in the *Math. Zeitschr.*).

<sup>\*\*\*)</sup> The theorem is also proved by *Steinitz*, cf. § 8, Theorem 6; there, however, use is made of the theorem on symmetric functions, whose use is avoided here in the whole construction of *Galois* theory and in particular in the proof of this theorem.

<sup>\*\*\*)</sup> Cf. p. 43.

**Addendum:** If  $\mathfrak{Z}$  is an intermediate field between  $\mathfrak{K}$  and  $\mathfrak{N}$  and  $\mathfrak{Z}_0$  is the field between  $\mathfrak{K}$  and  $\mathfrak{Z}$  uniquely determined by § 14, Theorem 1 such that  $\mathfrak{Z}_0$  is of the first kind<sup>\*)</sup> over  $\mathfrak{K}$  and  $\mathfrak{Z}$  is a root field over  $\mathfrak{Z}_0$  [possibly  $\mathfrak{Z} = \mathfrak{Z}_0$ ], then:

$$A[\mathfrak{Z} : \mathfrak{K}] = A[\mathfrak{Z}_0 : \mathfrak{K}].$$

For if  $a_1$  and  $a_2$  are two automorphisms in  $N$  that effect the same isomorphism in  $\mathfrak{Z}_0$ , then  $a_1 \cdot a_2^{-1}$  effects the identical isomorphism in  $\mathfrak{Z}_0$ ; so by Theorem 2, if we let  $\mathfrak{Z}_0$  take the place of the ground field  $\mathfrak{K}$  only there,  $a_1 \cdot a_2^{-1}$  must effect the identical isomorphism in  $\mathfrak{Z}$ ; hence  $a_1$  and  $a_2$  effect the same isomorphism in  $\mathfrak{Z}$  if and only if they effect the same isomorphism in  $\mathfrak{Z}_0$ , from which our addendum follows.

To determine the mapping degree we therefore now need only investigate extensions of the first kind.

**Definition 4:** If  $\mathfrak{Z}$  is finite over  $\mathfrak{K}$ , let the basis degree  $B[\mathfrak{Z} : \mathfrak{K}] = [\mathfrak{Z} : \mathfrak{K}]^{**})$ ; but if  $\mathfrak{Z}$  is infinite over  $\mathfrak{K}$ , let  $\mathfrak{K}_\nu$  for  $0 \leq \nu \leq \sigma$  be a tower of fields generating  $\mathfrak{Z}$  such that

1.  $\mathfrak{K}_0 = \mathfrak{K}$ ,
2.  $\mathfrak{K}_{\nu+1}$  is simple over  $\mathfrak{K}_\nu$ ,
3. if  $\nu$  is a limit number,  $\mathfrak{K}_\nu$  is the union of all  $\mathfrak{K}_\mu$  with  $\mu < \nu$ , that is, by § 2, Theorem 2, a field,
4.  $\mathfrak{K}_\sigma = \mathfrak{Z}$

holds; then let the basis degree  $B[\mathfrak{Z} : \mathfrak{K}]$  be the smallest cardinality that the set of fields of such a generating tower of fields can have. <sup>\*\*\*\*\*)</sup>

**Theorem 3:** Let  $\mathfrak{Z}$  be a field between  $\mathfrak{K}$  and  $\mathfrak{N}$ , and specifically one of the first kind over  $\mathfrak{K}$ .

a) If  $\mathfrak{Z}$  is finite over  $\mathfrak{K}$ , then:

$$A[\mathfrak{Z} : \mathfrak{K}] = B[\mathfrak{Z} : \mathfrak{K}].$$

b) If  $\mathfrak{Z}$  is infinite over  $\mathfrak{K}$ , then:

$$A[\mathfrak{Z} : \mathfrak{K}] = 2^{B[\mathfrak{Z} : \mathfrak{K}]} > B[\mathfrak{Z} : \mathfrak{K}]^{*****}).$$

*Proof:* ad a) By § 13, Theorem 7,  $\mathfrak{Z}$  is a simple extension of  $\mathfrak{K}$ , i.e.  $\mathfrak{Z} = \mathfrak{K}(\mathfrak{a})^{*****})$ . Let  $\mathfrak{a} = \mathfrak{a}_1, \dots, \mathfrak{a}_n$  be all the roots of the irreducible equation  $\alpha(x) = 0$  in  $\mathfrak{K}$  that  $\mathfrak{a}$  satisfies. Since

<sup>\*)</sup> Cf. p. 44.

<sup>\*\*)</sup> Cf. p. 23.

<sup>\*\*\*)</sup> Such a smallest cardinality always exists, at least if one presupposes the axiom of choice and the well-ordering theorem, since the cardinalities then form a well-ordered series.

<sup>\*\*\*\*\*)</sup> We shall be able to show later, under the assumption of the generalized continuum hypothesis of Cantor, that any two towers of fields generating  $\mathfrak{Z}$  have the same cardinality if  $\mathfrak{Z}$  is infinite over  $\mathfrak{K}$  and of the first kind; cf. Addendum to Theorem 3.

<sup>\*\*\*\*\*)</sup> Since, after all, the power set always has greater cardinality than the set itself. Cf. e.g. *F. Hausdorff: Grundzüge der Mengenlehre* (1914), p. 56, Theorem II.

<sup>\*\*\*\*\*)</sup> The following proof can also be carried out without use of this theorem; one then has only to use, beyond the proof carried out here, the multiplication theorem for the basis degree (§ 7, Theorem 2) and the corresponding multiplication theorem for the mapping degree in finite extensions. Cf. especially (2) in the proof ad b) of this theorem, where the multiplication theorem for the finite mapping degree is essentially proved along with it without use of the theorem of Abel or of Theorem 3 a).

$\mathfrak{Z}$  is of the first kind over  $\mathfrak{K}$ , the  $\mathfrak{a}_i$  are all distinct. From Lemma 2 it follows that we obtain all isomorphisms of  $\mathfrak{Z}$  that can be induced by automorphisms in  $N$  if we carry  $\mathfrak{a}$  in turn into  $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ , i.e. we have  $A[\mathfrak{Z} : \mathfrak{K}] = n$ . But since  $\mathfrak{Z}$  is of the first kind over  $\mathfrak{K}$ ,  $n$  is the degree of  $\alpha(x)$ , i.e.

$$n = [\mathfrak{a} : \mathfrak{K}] = [\mathfrak{Z} : \mathfrak{K}] = B[\mathfrak{Z} : \mathfrak{K}],$$

hence  $A[\mathfrak{Z} : \mathfrak{K}] = B[\mathfrak{Z} : \mathfrak{K}]$ .

ad b) Let  $\mathfrak{K}_\nu$  for  $0 \leq \nu \leq \sigma$  be a chain of fields generating  $\mathfrak{Z}$ , constructed as above, and let  $\mathfrak{m}$  be its [infinite] cardinality. Then we want to prove:

$$(b) \quad A[\mathfrak{Z} : \mathfrak{K}] = 2^{\mathfrak{m}}.$$

Since  $\mathfrak{Z}$  is an extension of the first kind of  $\mathfrak{K}$  and  $\mathfrak{K}_{\nu+1}$  is a simple algebraic extension of  $\mathfrak{K}_\nu$ , we have:

$$(1) \quad 2 \leq [\mathfrak{K}_{\nu+1} : \mathfrak{K}_\nu] = B[\mathfrak{K}_{\nu+1} : \mathfrak{K}_\nu] < \aleph_0.$$

(2) If then  $\pi_\nu$  is any isomorphism of  $\mathfrak{K}_\nu$  that can be induced by automorphisms in  $N$ , it can be extended in exactly  $[\mathfrak{K}_{\nu+1} : \mathfrak{K}_\nu]$  distinct ways to isomorphisms of  $\mathfrak{K}_{\nu+1}$  that can be induced by automorphisms in  $N$ .

For if  $\mathfrak{K}_{\nu+1} = \mathfrak{K}_\nu(\mathfrak{a}_\nu)$  and  $\mathfrak{a}_\nu$  satisfies the irreducible equation  $\alpha_\nu(x) = 0$  in  $\mathfrak{K}_\nu$ , then under  $\pi_\nu$  the polynomial  $\alpha_\nu(x)$  goes into an irreducible polynomial  $\beta_\nu(x)$  of the field  $\mathfrak{L}_\nu$  into which  $\mathfrak{K}_\nu$  goes under  $\pi_\nu$ . Necessarily  $\beta_\nu(x) = 0$  is likewise an equation of the first kind, which therefore has only simple zeros. As in the proof of Lemma 1. one sees that all zeros of  $\beta_\nu(x)$  lie in  $\mathfrak{N}$ . Since the degree of  $\beta_\nu(x)$  is equal to that of  $\alpha_\nu(x)$ , i.e. equal to  $[\mathfrak{K}_{\nu+1} : \mathfrak{K}_\nu]$ , it follows from the theorem stated in Erl. 53 and from Lemma 2 that  $\mathfrak{a}_\nu$  can be carried by automorphisms in  $N$  into all zeros of  $\beta_\nu(x)$ . Since, finally, the automorphisms in  $N$  are to extend the isomorphism  $\pi_\nu$ , only the zeros of  $\beta_\nu(x)$  can come into question as images of  $\mathfrak{a}_\nu$ , which proves our assertion (2).

From (1) and (2) it now follows at once:

$$(3) \quad 2^{\mathfrak{m}} \leq A[\mathfrak{Z} : \mathfrak{K}] \leq \aleph_0^{\mathfrak{m}}.$$

Now, however, the following general aleph equation holds:

$$(4) \quad \text{If } \aleph_\alpha \leq \aleph_\beta, \text{ then } 2^{\aleph_\beta} = \aleph_\alpha^{\aleph_\beta}.$$

For we have

$$2 \leq \aleph_\alpha \leq \aleph_\beta \leq 2^{\aleph_\beta},$$

hence, if we raise this inequality to the  $\aleph_\beta$ -th power:

$$2^{\aleph_\beta} \leq \aleph_\alpha^{\aleph_\beta} \leq (2^{\aleph_\beta})^{\aleph_\beta} = 2^{(2^{\aleph_\beta})} = 2^{\aleph_\beta *}).$$

Since in (3)  $\mathfrak{m}$  is an infinite cardinality, hence  $\mathfrak{m} \geq \aleph_0$ , i.e. an  $\aleph$ , our assertion (b) follows from (3) and (4).

If in (b) one chooses in particular  $\mathfrak{m} = B[\mathfrak{Z} : \mathfrak{K}]$ , which by the definition of the basis degree is always possible, the assertion of the theorem results.

\*) The proof after *W. Sierpinski*: Leçons sur les nombres transfinis, Paris 1928.

**Addendum:** Under the assumption of the generalized continuum hypothesis of Cantor:

$$(c) \quad 2^{\aleph_\nu} = \aleph_{\nu+1}$$

if  $\mathfrak{Z}$  is infinite over  $\mathfrak{K}$ , all towers of fields generating  $\mathfrak{Z}$  have the same cardinality, i.e. the basis degree  $B[\mathfrak{Z} : \mathfrak{K}]$  is the cardinality of every tower of fields generating  $\mathfrak{Z}^*$ .

*Proof:* Let  $\aleph_{\nu_1}$  and  $\aleph_{\nu_2}$  be the cardinalities of two towers of fields generating  $\mathfrak{Z}$ ; then by (b)

$$\begin{aligned} A[\mathfrak{Z} : \mathfrak{K}] &= 2^{\aleph_{\nu_1}} \\ &= 2^{\aleph_{\nu_2}}. \end{aligned}$$

By (c),  $2^{\aleph_{\nu_i}} = \aleph_{\nu_i+1}$ ; hence

$$\aleph_{\nu_1+1} = \aleph_{\nu_2+1}^{**},$$

hence  $\aleph_{\nu_1} = \aleph_{\nu_2}$ .

**Main Theorem 1:** The equation

$$\mathfrak{N}[N(\mathfrak{Z})] = \mathfrak{Z}$$

holds for the field  $\mathfrak{Z}$  between  $\mathfrak{K}$  and  $\mathfrak{N}$  if and only if every element of  $\mathfrak{N}$  that is a root element with respect to  $\mathfrak{Z}$  is already contained in  $\mathfrak{Z}$ .

*Proof:* A. Suppose  $\mathfrak{N}, \mathfrak{Z}$  satisfy the condition of the theorem and let  $\mathfrak{a}$  be an element of  $\mathfrak{N}$  but not of  $\mathfrak{Z}$ ; then the irreducible equation in  $\mathfrak{Z}$  that  $\mathfrak{a}$  satisfies has in  $\mathfrak{N}$  at least one solution  $\mathfrak{b}$  different from  $\mathfrak{a}$ . If we now apply Lemma 2 to  $\mathfrak{Z}$  as ground field, there is therefore an automorphism of  $\mathfrak{N}$  that leaves  $\mathfrak{Z}$  elementwise invariant, hence belongs to  $N(\mathfrak{Z})$ , and carries  $\mathfrak{a}$  into  $\mathfrak{b} \neq \mathfrak{a}$ ;  $\mathfrak{a}$  therefore does not belong to  $\mathfrak{N}[N(\mathfrak{Z})]$  if it does not belong to  $\mathfrak{Z}$ . Hence:

$$\mathfrak{N}[N(\mathfrak{Z})] \leq \mathfrak{Z}, \text{ i.e. } = \mathfrak{Z} \text{ (cf. above p. 95).}$$

B. Let  $\mathfrak{a}$  be an element of  $\mathfrak{N}$  but not of  $\mathfrak{Z}$  that is a root element with respect to  $\mathfrak{Z}$ . Then  $\mathfrak{a}$  satisfies an equation  $x^{p^f} - \mathfrak{c} = 0$  in  $\mathfrak{Z}$ , which therefore has only the solution  $\mathfrak{a}$ . If we now apply Lemma 2 with  $\mathfrak{Z}$  as ground field, it follows that  $\mathfrak{a}$  goes into itself under all automorphisms of  $\mathfrak{N}$  that leave  $\mathfrak{Z}$  elementwise invariant, which therefore belong to  $N(\mathfrak{Z})$ ; hence  $\mathfrak{a}$  belongs to  $\mathfrak{N}[N(\mathfrak{Z})]$  without belonging to  $\mathfrak{Z}$ , i.e.  $\mathfrak{N}[N(\mathfrak{Z})] > \mathfrak{Z}$ .

**Addendum:** We have

$$\mathfrak{N}[N(\mathfrak{Z})] = \mathfrak{Z},$$

for all fields  $\mathfrak{Z}$  between  $\mathfrak{K}$  and  $\mathfrak{N}$  if and only if  $\mathfrak{N}$  is of the first kind over  $\mathfrak{K}$ .

*Proof:* A. If  $\mathfrak{N}$  is of the first kind over  $\mathfrak{K}$ , then, by § 13, Theorems 8, 9, it is also of the first kind over every  $\mathfrak{Z}$ . Hence every root element of  $\mathfrak{N}$  with respect to  $\mathfrak{Z}$  belongs to  $\mathfrak{Z}$ , i.e. by Main Theorem 1:

$$\mathfrak{N}[N(\mathfrak{Z})] = \mathfrak{Z}.$$

B. If  $\mathfrak{N}$  is not of the first kind over  $\mathfrak{K}$ , then by § 14, Theorem 1 there is a field  $\mathfrak{N}_0$  between  $\mathfrak{K}$  and  $\mathfrak{N}$  that is a proper subfield of  $\mathfrak{N}$ , such that  $\mathfrak{N}$  is a root field over  $\mathfrak{N}_0$  and  $\mathfrak{N}_0$  is of the

\*) This statement stands in analogy to § 23, Theorem 3. — Cf. also *R. Baer*: Eine Anwendung der Kontinuumshypothese in der Algebra, Journal für d. r. u. angew. Math. vol. 162 (1930), p. 132.

\*\*) So far it has not been possible to infer  $\aleph_\nu = \aleph_\mu$  from  $2^{\aleph_\nu} = 2^{\aleph_\mu}$  without use of the continuum hypothesis. Cf. *W. Sierpinski*: Sur l'hypothèse du continu, Fund. Math. vol. 5 (1924), p. 183.

first kind over  $\mathfrak{K}$ . By Theorem 2 we then have  $A[\mathfrak{N} : \mathfrak{N}_0] = 1$ , i.e.  $N(\mathfrak{N}_0)$  consists only of the identity map. But then  $\mathfrak{N}[N(\mathfrak{N}_0)] = \mathfrak{N}$ , hence not equal to  $\mathfrak{N}_0$ .

**Main Theorem 2<sup>\*</sup>**: Let  $\mathfrak{N}_0$  be the field between  $\mathfrak{K}$  and  $\mathfrak{N}$  uniquely determined by § 14, Theorem 1, such that  $\mathfrak{N}$  is a root field over  $\mathfrak{N}_0$  and  $\mathfrak{N}_0$  is of the first kind over  $\mathfrak{K}$ ; if  $\mathfrak{K}$  is perfect, let  $\mathfrak{N}_0 = \mathfrak{N}$ . We have

$$N[\mathfrak{N}(U)] = U,$$

for all subgroups  $U$  of  $N$  if and only if  $\mathfrak{N}_0$  is finite over  $\mathfrak{K}$ .

*Proof*: A. Let  $\mathfrak{N}_0$  be finite over  $\mathfrak{K}$ . Then  $\mathfrak{N}(U)$  is a field between  $\mathfrak{K}$  and  $\mathfrak{N}$ . Let  $\mathfrak{N}(U)_0$  be the field between  $\mathfrak{K}$  and  $\mathfrak{N}(U)$  uniquely determined by § 14, Theorem 1, over which  $\mathfrak{N}(U)$  is a root field and which is of the first kind over  $\mathfrak{K}$ ; for perfect  $\mathfrak{K}$  let  $\mathfrak{N}(U)_0 = \mathfrak{N}(U)$ . By § 13, Theorem 8,  $\mathfrak{N}(U)_0$  is a subfield of  $\mathfrak{N}_0$ , namely the set-theoretic intersection of  $\mathfrak{N}(U)$  and  $\mathfrak{N}_0$ . From Theorem 2 it follows that

$$N[\mathfrak{N}(U)] = N[\mathfrak{N}(U)_0] \text{ holds.}$$

By Theorem 3 a),  $N$  is finite and the order of  $N$  is

$$A[\mathfrak{N}_0 : \mathfrak{K}] = B[\mathfrak{N}_0 : \mathfrak{K}] = [\mathfrak{N}_0 : \mathfrak{K}] \equiv n.$$

Since  $\mathfrak{N}_0$  is of the first kind and finite over  $\mathfrak{K}$ ,  $\mathfrak{N}_0$  is, by § 13, Theorem 7, simple over  $\mathfrak{K}$ , i.e.  $\mathfrak{N}_0 = \mathfrak{K}(\mathfrak{a})^{**}$ .

Under the maps in  $U$  let  $\mathfrak{a}$  go into  $\mathfrak{a}_1 = \mathfrak{a}, \mathfrak{a}_2, \dots, \mathfrak{a}_u$ ; then  $u$  is the order of  $U$ . We consider  $\varphi(x) \equiv \prod_{i=1}^u (x - \mathfrak{a}_i)$ ; this polynomial goes into itself under all maps in  $U$ ; so its coefficients belong, by the definition of  $\mathfrak{N}(U)$ , to  $\mathfrak{N}(U)$ , hence also to  $\mathfrak{N}(U)_0$ ; since  $\mathfrak{N}(U)_0(\mathfrak{a}) = \mathfrak{K}(\mathfrak{a}) = \mathfrak{N}_0$ , we have  $[\mathfrak{N}_0 : \mathfrak{N}(U)_0] = [\mathfrak{a} : \mathfrak{N}(U)_0] \leq u$ ; for  $\mathfrak{a}$  is a zero of  $\varphi(x)$ .

On the other hand,  $[\mathfrak{N}_0 : \mathfrak{N}(U)_0]$  is, by Theorem 3 a), applied to  $\mathfrak{N}(U)_0$  as ground field, equal to the order  $u'$  of  $N[\mathfrak{N}(U)_0]$ , for which by the inequality on p. 95  $u' \geq u$  holds; thus we have  $u' = u$ , i.e. the order of  $N[\mathfrak{N}(U)_0]$  is equal to that of its subgroup  $U$ , which, for finite groups (and these, after all, are what concern us here), has the identity

$$N[\mathfrak{N}(U)] = N[\mathfrak{N}(U)_0] = U$$

as a consequence.

B. Let  $\mathfrak{N}_0$  be infinite over  $\mathfrak{K}$ ; then by Theorem 3 b) the group  $N$  has at least the cardinality of the continuum, and so does every infinite group  $N(\mathfrak{Z})$ ; this follows from Theorem 3 b) if one takes  $\mathfrak{Z}$  as ground field in place of  $\mathfrak{K}$ .

Let  $U$  now be a countable subgroup of  $N$ ; such always exist, for  $N$  has the cardinality of the continuum, and so certainly contains a countable subset  $S$ ; the smallest subgroup of  $N$  containing  $S$  is then also countable, since, after all, it consists only of products of finite length, each of finitely many elements of  $S$ . Then  $N[\mathfrak{N}(U)]$  is an  $N(\mathfrak{Z})$  [ $\mathfrak{Z} = \mathfrak{N}(U)$ ], and so has at least the cardinality  $2^{\aleph_0} > \aleph_0$ , and must therefore contain elements that do not occur in  $U$ .

<sup>\*</sup>) This runs parallel to the Addendum to Main Theorem 1, whereas the theorem corresponding to Main Theorem 1 would have to draw upon topology, an auxiliary means foreign to our considerations. Cf. *W. Krull: Galoissche Theorie der unendlichen algebraischen Erweiterungen*, Math. Ann. vol. 100 (1928), p. 687.

<sup>\*\*</sup>) The use of this theorem can again be circumvented by using the multiplication theorem for the basis degree and constructing several equations in place of the one fundamental equation  $\varphi(x) = 0$ , but otherwise proceeding as indicated in the proof.

**Main Theorem 3:** *We have*

$$(F) \quad N[\mathfrak{N}(U)] = U, \quad \mathfrak{N}[N(\mathfrak{Z})] = \mathfrak{Z},$$

for all subgroups  $U$  of  $N$  and for all fields  $\mathfrak{Z}$  between  $\mathfrak{K}$  and  $\mathfrak{N}$  if and only if  $\mathfrak{N}$  is of the first kind and finite over  $\mathfrak{K}$ .

This follows from the Addendum to Main Theorem 1 and from Main Theorem 2.

**Definition 5:** *If  $H_1$  and  $H_2$  are two subgroups of  $N$  or two subfields of  $\mathfrak{N}$ , let  $H_1 \cap H_2$  be the intersection group or the intersection field, respectively, and  $H_1 \cup H_2$  the union group or the union field, respectively, of  $H_1$  and  $H_2$ .*

**Theorem 4:** *If  $\mathfrak{Z}_1$  and  $\mathfrak{Z}_2$  are two fields between  $\mathfrak{K}$  and  $\mathfrak{N}$ , then*

$$(1) \quad N(\mathfrak{Z}_1 \cup \mathfrak{Z}_2) = N(\mathfrak{Z}_1) \cap N(\mathfrak{Z}_2),$$

$$(2) \quad N(\mathfrak{Z}_1 \cap \mathfrak{Z}_2) = N(\mathfrak{Z}_1) \cup N(\mathfrak{Z}_2).$$

*If further  $U_1$  and  $U_2$  are two subgroups of  $N$ , then:*

$$(3) \quad \mathfrak{N}(U_1 \cup U_2) = \mathfrak{N}(U_1) \cap \mathfrak{N}(U_2),$$

$$(4) \quad \mathfrak{N}(U_1 \cap U_2) = \mathfrak{N}(U_1) \cup \mathfrak{N}(U_2)^*).$$

*Proof:* ad (1): for  $i = 1, 2$  we have  $N(\mathfrak{Z}_1) \cap N(\mathfrak{Z}_2) \leq N(\mathfrak{Z}_i)$ ; so under  $N(\mathfrak{Z}_1) \cap N(\mathfrak{Z}_2)$  all elements of  $\mathfrak{Z}_1$  and all of  $\mathfrak{Z}_2$  remain invariant, so also all of  $\mathfrak{Z}_1 \cup \mathfrak{Z}_2$ ; and this means

$$N(\mathfrak{Z}_1) \cap N(\mathfrak{Z}_2) \leq N(\mathfrak{Z}_1 \cup \mathfrak{Z}_2).$$

Conversely, if an automorphism in  $N$  leaves all elements of  $\mathfrak{Z}_1 \cup \mathfrak{Z}_2$  invariant, it also leaves invariant all those of  $\mathfrak{Z}_1$  and of  $\mathfrak{Z}_2$ , and is therefore contained in  $N(\mathfrak{Z}_1) \cap N(\mathfrak{Z}_2)$  as the totality of the automorphisms leaving both  $\mathfrak{Z}_1$  and  $\mathfrak{Z}_2$  elementwise invariant, i.e.

$$N(\mathfrak{Z}_1) \cap N(\mathfrak{Z}_2) \geq N(\mathfrak{Z}_1 \cup \mathfrak{Z}_2).$$

From this (1) follows. In the same way one sees (2)–(4).

From Theorem 4 there follows by specialization the

**Addendum:** *If  $U_1 \leq U_2$ , then*

$$\mathfrak{N}(U_1) \geq \mathfrak{N}(U_2),$$

*and if  $\mathfrak{Z}_1 \leq \mathfrak{Z}_2$ , then*

$$N(\mathfrak{Z}_1) \geq N(\mathfrak{Z}_2).$$

**Theorem 5:** *Let  $\mathfrak{Z}$  be a field between  $\mathfrak{K}$  and  $\mathfrak{N}$ ; two automorphisms in  $N$  effect the same isomorphism of  $\mathfrak{Z}$  if and only if they belong to the same coset of  $N$  with respect to  $N(\mathfrak{Z})^{**}$ .*

*Proof:* Let  $a_1$  and  $a_2$  be two automorphisms in  $N$ . These effect the same isomorphism of  $\mathfrak{Z}$  if and only if  $a_1 a_2^{-1}$  effects the identical isomorphism of  $\mathfrak{Z}$ , i.e. belongs to  $N(\mathfrak{Z})$ .

<sup>\*)</sup> We must consider fields  $\mathfrak{N}(U)$  and groups  $N(\mathfrak{Z})$ , since only for these can the fulfilment of (F) be counted on.

<sup>\*\*) Cf. Definition 3, where this theorem, which could equally well have been proved there, was stated without proof</sup>

**Theorem 6:** Let no element of  $\mathfrak{N}$  that does not belong to  $\mathfrak{Z}$  be a root element with respect to  $\mathfrak{Z}$ . Then an automorphism  $a$  in  $N$  effects an automorphism of  $\mathfrak{Z}$  if and only if  $a$  belongs to the normalizer<sup>\*)</sup> of  $N(\mathfrak{Z})$  in  $N$ , i.e. if  $a$  is permutable with  $N(\mathfrak{Z})$ <sup>\*\*)</sup> .

*Proof:* A. Let  $a$  effect an automorphism of  $\mathfrak{Z}$  and let  $n$  be an arbitrary element of  $N(\mathfrak{Z})$ ; then  $ana^{-1}$  likewise leaves  $\mathfrak{Z}$  elementwise fixed, since  $\mathfrak{Z}$  is carried into itself by  $a$ . So  $ana^{-1}$  belongs to  $N(\mathfrak{Z})$  for arbitrary  $n$  in  $N(\mathfrak{Z})$ , i.e.  $a$  belongs to the normalizer of  $N(\mathfrak{Z})$ .

B. Let  $a$  effect no automorphism of  $\mathfrak{Z}$ ; then there is an element  $\mathfrak{a}$  of  $\mathfrak{Z}$  whose image  $\mathfrak{b}$  under  $a$  does not belong to  $\mathfrak{Z}$ . By the hypothesis made about  $\mathfrak{N}$  and  $\mathfrak{Z}$ , the irreducible equation in  $\mathfrak{Z}$  that  $\mathfrak{b}$  satisfies is satisfied by a further  $\mathfrak{c} \neq \mathfrak{b}$  in  $\mathfrak{N}$ . Then by Lemma 2 there is an automorphism  $n$  that leaves  $\mathfrak{Z}$  elementwise invariant, i.e. belongs to  $N(\mathfrak{Z})$ , but carries  $\mathfrak{b}$  into  $\mathfrak{c}$ . Under  $ana^{-1}$ , then,  $\mathfrak{a}$  is not carried into itself, i.e.  $ana^{-1}$  does not belong to  $N(\mathfrak{Z})$ , i.e.  $a$  does not belong to the normalizer of  $N(\mathfrak{Z})$  in  $N$ .

**Addendum 1:** Under the hypotheses of Theorem 6, the cardinality of the set of fields conjugate to  $\mathfrak{Z}$  is equal to the cardinality of the set of cosets of  $N$  with respect to the normalizer of  $N(\mathfrak{Z})$  in  $N$ .

For two automorphisms  $a_1$  and  $a_2$  carry  $\mathfrak{Z}$  into the same field if and only if  $\mathfrak{Z}$  is carried into itself by  $a_1a_2^{-1}$ , i.e. by Theorem 6 if  $a_1a_2^{-1}$  belongs to the normalizer of  $N(\mathfrak{Z})$  in  $N$ .

**Addendum 2:** Under the hypotheses of Theorem 6,  $\mathfrak{Z}$  is a normal field if and only if  $N(\mathfrak{Z})$  is a normal subgroup of  $N$ .

For by Theorem 1,  $\mathfrak{Z}$  must be identical with its conjugate fields over  $\mathfrak{K}$ , so the normalizer of  $N(\mathfrak{Z})$  in  $N$  must coincide with  $N$ .

**Theorem 7:** If  $\mathfrak{K}$  is an arbitrary field,  $\mathfrak{N} = \mathfrak{K}(t_1, \dots, t_n)$  a purely transcendental extension of  $\mathfrak{K}$  of degree of transcendence  $n$ <sup>\*\*\*)</sup> ( $n > 1$ , finite integer); then every function in  $\mathfrak{N}$  symmetric in  $t_1, \dots, t_n$  can be represented uniquely as a rational function of the elementary symmetric functions with coefficients in  $\mathfrak{K}$ .

*Proof:* Let  $\varphi(x) \equiv \prod_{i=1}^n (x - t_i) \equiv x^n + \sum_{i=0}^{n-1} x^i \cdot \sigma_i(t_1, \dots, t_n)$ . Then the  $\sigma_i$  are accordingly the elementary symmetric functions in  $t_1, \dots, t_n$ . Let  $\mathfrak{S}$  be the smallest field between  $\mathfrak{K}$  and  $\mathfrak{N}$  that contains  $\varphi(x)$ , i.e.  $\mathfrak{S} = \mathfrak{K}(\sigma_1, \dots, \sigma_n)$ .

Since  $\mathfrak{N} = \mathfrak{S}(t_1, \dots, t_n)$  and the  $t_i$  satisfy the equation  $\varphi(x) = 0$  in  $\mathfrak{S}$ ,  $\mathfrak{N}$  is algebraic over  $\mathfrak{S}$ . Since further  $\varphi(x)$  has only simple zeros,  $\mathfrak{N}$  is, by § 13, Theorem 8, of the first kind over  $\mathfrak{S}$ . Since finally  $\mathfrak{N}$  just suffices to break  $\varphi(x)$  up into linear factors,  $\mathfrak{N}$  is normal over  $\mathfrak{S}$  by Addendum 2 to Theorem 1.

1. Let  $\sigma = \sigma(t_1, \dots, t_n)$  be a symmetric, rational function of the  $t_i$  with coefficients in  $\mathfrak{K}$ . Since by Lemma 2, under automorphisms of  $\mathfrak{N}$  that leave  $\mathfrak{S}$  elementwise invariant, zeros of  $\varphi(x)$  must again go into zeros of  $\varphi(x)$ , every such automorphism effects a permutation of the  $t_i$  and so leaves  $\sigma$  invariant. By Theorem 2 and Theorem 3a),  $\sigma$  therefore belongs to  $\mathfrak{S}$ , i.e. is a rational function of the  $\sigma_i$  with coefficients in  $\mathfrak{K}$ .

2. Since  $\mathfrak{N}$  is algebraic over  $\mathfrak{S}$ ,  $\mathfrak{N}$  has degree of transcendence 0 over  $\mathfrak{S}$ . So by § 23, Theorem 4,  $\mathfrak{S}$  has degree of transcendence  $n$  over  $\mathfrak{K}$ , since the sum of the degrees of transcendence of  $\mathfrak{N}$  over  $\mathfrak{S}$  and of  $\mathfrak{S}$  over  $\mathfrak{K}$  must be equal to that of  $\mathfrak{N}$  over  $\mathfrak{K}$ . So the system  $\sigma_1, \dots, \sigma_n$  must be irreducible<sup>\*\*\*\*)</sup> over  $\mathfrak{K}$ , i.e. there is no algebraic relation between the  $\sigma_i$

<sup>\*)</sup> Cf. e.g. *A. Speiser: Theorie der Gruppen von endlicher Ordnung* (1923), p. 38.

<sup>\*\*)</sup>  Cf. *R. Baer: Abbildungseigenschaften algebraischer Erweiterungen*, § 2, (see p. 98, note)

<sup>\*\*\*)</sup> Cf. p. 88.

<sup>\*\*\*\*)</sup> Cf. p. 81.

with coefficients in  $\mathfrak{K}$ . So too every element of  $\mathfrak{S}$  can be represented in only one way as a rational function of the  $\sigma_i$  with relatively prime numerator and denominator.

## Appendix B

## Explanatory Notes

By Reinhold Baer and Helmut Hasse

These notes are not by Steinitz. A mark such as <sup>E 57</sup> in the text shows the place to which the note with that number refers; the page given after each note's number is the page of that place. Both are links. "Erl. n" (for Erläuterung) means note n. All references in the notes to Steinitz's text, to other notes and to Appendix A are to the pages of this edition.

1. (to p. 3) This characterization of *Galois* theory would probably no longer meet with general agreement today. That the range of *Galois* theory in its form up to now is confined to finite extensions has indeed only recently been made entirely clear. Cf. Appendix A, Main Theorem 2, p. 102. On the other hand, ways have been shown of pursuing a *Galois* theory of infinite algebraic extensions as well. — Cf. *W. Krull: Galoissche Theorie der unendlichen algebraischen Erweiterungen*, Math. Ann. vol. 100 (1928), pp. 687–698.

2. (to p. 4) For the purpose in question the distinction given, which refers to the ground field, is admittedly less essential than the distinction of extensions into those of the first and of the second kind. (Cf. § 13, say.)

3. (to p. 4) What is essentially at issue here is the so-called theorem of primitive elements. Cf. § 11, Theorem 4; § 15, Theorems 7 and 9.

4. (to p. 5) These further treatises never appeared. Nor were investigations of this kind found among *Steinitz*' papers.

5. (to p. 6) This notion is fundamental, for it is the task of algebra to study the invariants of fields under isomorphisms.

6. (to p. 6) Postulate 2. (the commutative law of addition) already follows from the remaining field postulates if one extends 6. in a corresponding way — as the renunciation of 2. requires — so that right-hand and left-hand subtraction become unique.

For if  $a, b$  are any two field elements and  $\varepsilon$  the unity of multiplication, then:

$$\begin{aligned} (a + b) \cdot (\varepsilon + \varepsilon) &= (a + b) \cdot \varepsilon + (a + b) \cdot \varepsilon && \text{by 5.} \\ &= (a + b) + (a + b) && \text{by 7.} \\ &= a + [b + (a + b)] && \text{by 1.} \end{aligned}$$

on the other hand

$$\begin{aligned} &= a \cdot (\varepsilon + \varepsilon) + b \cdot (\varepsilon + \varepsilon) && \text{by 4., 5.} \\ &= (a \cdot \varepsilon + a \cdot \varepsilon) + (b \cdot \varepsilon + b \cdot \varepsilon) && \text{by 5.} \\ &= (a + a) + (b + b) && \text{by 7.} \\ &= a + [a + (b + b)] && \text{by 1.} \end{aligned}$$

Therefore:

$$a + [b + (a + b)] = a + [a + (b + b)],$$

from which, by 6., it follows that

$$b + (a + b) = a + (b + b)$$

or, by 1.:

$$(b + a) + b = (a + b) + b$$

and finally, by the extended 6.:

$$b + a = a + b.$$

Cf. *A. Loewy*: Lehrbuch der Algebra I, Leipzig 1915, p. 41.

**7.** (to p. 6) The reason the existence of at least two elements is required is that otherwise a system consisting of 0 alone would already be a field. It is convenient to exclude this trivial special case. So as not to be left with only this special case, one must then further require in 7. that  $a \neq 0$ , since otherwise it would follow from 7., because  $0 \cdot x = 0$ , that every  $b = 0$ .

**8.** (to p. 7) The reason the zero of the system is denoted by the ordinary numeral 0 while the unity is not denoted by 1 is that the zero of the system does have all the computational properties of the number 0, whereas the unity  $\varepsilon$  of the system need not have all the properties of the number 1 — for instance not the property that  $\varepsilon + \cdots + \varepsilon \neq 0$  always. (Cf. p. 11.) The ordinary integers are used, in their meaning as counting numbers, alongside the multiples of  $\varepsilon$ .

**9.** (to p. 7) For the proof of these theorems compare, say, *H. Hasse*: Höhere Algebra I, Sammlung Göschen 931 (1926); *O. Haupt*: Einführung in die Algebra I, Leipzig 1929, chapter 9.

**10.** (to p. 7) That the residue classes modulo a prime number  $p$  form a field may be seen, for instance, as follows:

If  $a_i + m_i p$  and  $a_i$  ( $i = 1, 2$ ) are elements of the same residue class, then the same holds of the sum, difference and product, because:

$$(a_1 + m_1 p) \pm (a_2 + m_2 p) = (a_1 \pm a_2) + (m_1 \pm m_2) p$$

and

$$(a_1 + m_1 p)(a_2 + m_2 p) = a_1 a_2 + p(m_1 a_2 + m_2 a_1 + m_1 m_2 p).$$

Sum, difference and product of residue classes are therefore uniquely determined by the corresponding operations on the elements. If  $A$  is a residue class not containing 0 and  $a$  is any element of  $A$ , then  $a$  is not divisible by  $p$ , hence, since  $p$  is prime, relatively prime to  $p$ ; so there are two integers  $m$  and  $n$  with  $ma + np = 1$ . The residue class containing  $m$  is then the reciprocal of  $A$ . If finally  $b$  lies in  $B$ , then the residue class containing  $mb$  is the quotient of  $B$  by  $A$ . That the compositions of residue classes so introduced satisfy the field postulates is now easily verified. In particular the uniqueness of division follows from the primality of  $p$ .

**11.** (to p. 8) For along with  $\alpha$  and  $\beta$ ,  $\alpha \pm \beta$ ,  $\alpha \cdot \beta$ ,  $\frac{\alpha}{\beta}$  ( $\beta \neq 0$ ) also occur in all the fields of  $\mathfrak{S}$ .

**12.** (to p. 8) The special case of this theorem most important for the applications is the following:  $\mathfrak{U}$  forms a so-called **tower of fields**, that is, a well-ordered system of fields such that every field of  $\mathfrak{U}$  contains all those preceding it in the well-ordering as subfields and is contained in all those following it in the well-ordering of  $\mathfrak{U}$ . [For the notion of well-ordering cf. § 19.]

Briefly put, Theorem 2 says that under the hypotheses made the union of the fields of  $\mathfrak{U}$  is itself a field.

**13.** (to p. 8) Note in this proof that, in contrast to Theorem 1, it is not assumed that all fields of  $\mathfrak{U}$  are subfields of one definite field; that is why the composition of the elements of the union field  $\mathfrak{K}$  has first to be defined.

**14.** (to p. 8) And only then.

**15.** (to p. 8) For this final result is obtained as well if one adjoins the union of  $\mathfrak{S}_1, \mathfrak{S}_2, \dots, \mathfrak{S}_n$  all at once.

**16.** (to p. 9) The following generalization of domains of integrity, the so-called **rings**, has lately become important: in rings one gives up the existence of the unity element and the prohibition of zero divisors [that is, numbers different from zero whose product with certain numbers, likewise different from zero, vanishes]; for the rest the same laws hold as in domains of integrity.

Cf. on this *H. Hasse: Höhere Algebra I; O. Haupt: Einführung in die Algebra I.*

**17.** (to p. 9) For if  $\eta$  were a second unity, then

$$\varepsilon = \varepsilon \cdot \eta = \eta \cdot \varepsilon = \eta.$$

**18.** (to p. 9) Since it is possible to introduce a notion of divisibility in domains of integrity, the study of domains of integrity (at least of those that are not fields) is characteristic of arithmetical investigations (cf. p. 3); here, however, arithmetic is in the service of algebra.

**19.** (to p. 9) 1) is needed in addition to 2) in order to infer  $\frac{a}{\varepsilon} = a$ .

**20.** (to p. 10) How strong the requirement of finiteness of the system is can also be seen from the theorem of *MacLagan Wedderburn* (cf. *E. Artin: Hamb. Abhdlg. vol. 5 (1928), p. 245*, say), which says that every skew field consisting of only finitely many elements [that is, a field with the requirement of commutativity of multiplication given up] is after all a field with commutative multiplication.

**21.** (to p. 10) Two fields belong to the same type if and only if they are isomorphic.

**22.** (to p. 11) One might think it more reasonable to speak of characteristic  $\infty$  rather than characteristic 0, since here all the infinitely many multiples of  $\varepsilon$  are distinct, whereas for prime-number characteristic  $p$  there are only exactly  $p$  distinct ones. But the designation characteristic 0 appears natural on the following consideration: for characteristic  $p$ ,  $m\varepsilon = m'\varepsilon$  if and only if  $m \equiv m' \pmod{p}$ , i.e. if  $p$  is a divisor of  $m' - m$ . For characteristic 0 the corresponding statement then holds:  $m\varepsilon = m'\varepsilon$  if and only if  $m = m'$ , i.e.  $m \equiv m' \pmod{0}$ , that is, if 0 is a divisor of  $m' - m$ . For in the domain of the natural numbers 0 is a divisor of 0 and of nothing else.

**23.** (to p. 11) Or else thus: by p. 10, last paragraph of § 3, every finite domain of integrity is a field. Cf. also Erl. 10.

**24.** (to p. 11) For they all have the same prime field.

**25.** (to p. 12) The notion of equivalent extensions, in which one definite ground field is distinguished, is fundamental for *Galois* theory.

Other designations for the same state of affairs are:  $\mathfrak{L}$  and  $\mathfrak{L}'$  are isomorphic relative to  $\mathfrak{K}$ , or with respect to  $\mathfrak{K}$ , or over  $\mathfrak{K}$ .

**26.** (to p. 12) *An example of two extensions of a field that are not equivalent but are isomorphic* (the notions and facts used here are not set out until a later point in the text): let  $\mathfrak{K}$  be an arbitrary field and  $\mathfrak{K}_1 = \mathfrak{K}(t)$  a simple transcendental extension (cf. p. 13) of  $\mathfrak{K}$ . We extend  $\mathfrak{K}_1$  on the one hand, by solving the equation  $x^2 - t = 0$ , to a field  $\mathfrak{K}_2$ , and on the other hand, by solving the equation  $x^3 - t = 0$ , to a field  $\mathfrak{K}_3$  (the possibility and uniqueness of these extensions is shown by § 6, Theorem 2). The resulting fields are both isomorphic to  $\mathfrak{K}_1$ , hence also to each other (cf. § 5, Theorem 2); but they are not equivalent extensions of  $\mathfrak{K}_1$ , for  $[\mathfrak{K}_2 : \mathfrak{K}_1] = 2$ ,  $[\mathfrak{K}_3 : \mathfrak{K}_1] = 3$  (cf. § 7, Theorem 4).

**27.** (to p. 13) In agreement with the usual definition, an element  $x$  is therefore algebraic over the field  $\mathfrak{K}$  if and only if it satisfies an equation  $\sum_{i=0}^n c_i x^i = 0$  with coefficients  $c_i$  from  $\mathfrak{K}$  that do not all vanish.

**28.** (to p. 13) To begin with there are two logically distinct operations  $+$  and  $\cdot$ : first the merely formal ones, indicated in  $\Sigma a_k x^k$  by the sign  $\Sigma$  and by the juxtaposition  $a_k \cdot x \cdot \dots \cdot x$ ; then the operations (2.) expressly defined in the text, on the strength of which  $\mathfrak{J}$  is a domain of integrity. To prove the assertion of the text one has to reduce the first “operations” to the second. For this one has to show that from  $x$ , i.e.  $0 \cdot x^0 + \varepsilon \cdot x^1 + 0 \cdot x^2 + \dots$ , and the elements  $a_k$ , i.e.  $a_k \cdot x^0 + 0 \cdot x^1 + 0 \cdot x^2 + \dots$ , the element  $a_0 x^0 + a_1 x^1 + \dots$  is composed according to the rules (2.).

A detailed presentation is to be found in *H. Hasse: Höhere Algebra I*, chapter 1, § 4; *O. Haupt: Einführung in die Algebra I*, chapter 7, 1–4.

**29.** (to p. 14) *Euler’s* procedure is the complete analogue, for integral rational functions, of the *Euclidean* algorithm of elementary number theory.

**30.** (to p. 14) For  $\varepsilon = f(x)g_1(x) + g(x)f_1(x)$  for suitable  $g_1(x)$ ,  $f_1(x)$ ; hence  $h(x) = h(x)f(x)g_1(x) + h(x)g(x)f_1(x)$ . Further  $f(x)h(x) = g(x)h_1(x)$ , hence

$$h(x) = g(x)[h_1(x)g_1(x) + h(x)f_1(x)].$$

**31.** (to p. 14) For the assumption that  $f(x) \cdot h(x)$  and  $g(x)$  are not relatively prime leads to a contradiction with Theorem 3 if one there replaces  $g(x)$  by the common divisor.

**32.** (to p. 17) For from  $ad - bc = 0$  it would follow that either  $y$  is of degree 0 or  $y = 0$ .

**33.** (to p. 17) We therefore obtain the totality of isomorphic mappings of  $\mathfrak{K}(x)$  onto itself under which the elements of  $\mathfrak{K}$  are each assigned to themselves if we apply to the primitive element  $x$  all possible integral and fractional linear transformations with non-vanishing determinant. For, taking § 5, Theorem 2 into account, it follows that we obtain all such isomorphisms by carrying  $x$  over into an arbitrary primitive element of  $\mathfrak{K}(x)$ .

**34.** (to p. 18) That is,  $\mathfrak{K}_n$  has, in the terminology of § 23, transcendence degree  $n$  over  $\mathfrak{K}_0$ .

**35.** (to p. 18) It would in itself suffice to verify the theorem for  $n = 1$  as the start of the induction, which is trivial. The special case  $n = 2$  of our theorem is, however, needed for the general proof.

**36.** (to p. 18) The assignment  $x_1, \dots, x_n$  to  $y_{\nu_1}, \dots, y_{\nu_n}$  (in a different order) also yields an isomorphic mapping. Repeated application of Theorem 9 shows as well that any permutation of  $x_1, \dots, x_n$  again produces a system  $x_{\nu_1}, \dots, x_{\nu_n}$  of successively adjoined transcendentals in the sense of Theorem 9. Every permutation of the  $x$  therefore yields an isomorphic mapping of  $\mathfrak{K}_0(x_1, \dots, x_n)$  onto itself leaving  $\mathfrak{K}_0$  fixed.

**37.** (to p. 19) Cf. *O. Haupt*: Algebra I, chapter 11, 7.

**38.** (to p. 20) For those familiar with ideal theory:

The zero class, the principal ideal with basis  $\varphi(x)$ , is a prime ideal if and only if  $\varphi(x)$  is irreducible. Forming residue classes modulo this ideal always yields a ring, which is a field if and only if the zero class is a prime ideal. Cf. *E. Noether*: Idealtheorie in Ringbereichen, Math. Ann. vol. 83 (1921).

**39.** (to p. 20) The necessity of this condition has likewise been shown.

**40.** (to p. 22) The assignment between the elements of  $\bar{\mathfrak{L}}$  not contained in  $\bar{\mathfrak{K}}$  and those of  $\mathfrak{S}$  is even meant to be one-to-one.

This seemingly needlessly roundabout proof is explained by the fact that  $\bar{\mathfrak{L}}$  is not an extension of  $\mathfrak{K}$  but only an extension of the field  $\bar{\mathfrak{K}}$  isomorphic to  $\mathfrak{K}$ . — One could admittedly also appeal more simply to the fact that isomorphic fields are not essentially different, so that it is no restriction of generality to extend from the outset a suitable field  $\bar{\mathfrak{K}}$  isomorphic to  $\mathfrak{K}$ .

**41.** (to p. 22) As always with extensions, a smallest extension solving the problem in question is meant. That is to say, no proper subfield of  $\mathfrak{K}(j)$  contains a zero of  $\varphi(x)$ .

**42.** (to p. 22) There are, on the other hand,  $n$  linearly independent elements:  $\varepsilon, j, \dots, j^{n-1}$ . In particular the degrees of all elements of  $\mathfrak{L}$  are at most  $n$ .

This theorem is the counterpart, announced on p. 15, to Theorem 5 there on simple transcendental extensions.

**43.** (to p. 23) Since the field of all complex numbers cannot be characterized purely algebraically within its type, this being possible only with the help of statements about continuity, the designation of the theorem that this field is algebraically closed as the fundamental theorem of algebra is much disputed today. Cf. *H. Hasse*: Höhere Algebra II, p. 79. One is inclined to confer this name on *Steinitz'* theorem that every field can be extended to an algebraically closed one in one way and essentially in only one way. Cf. § 21, Theorem 9.

**44.** (to p. 23) For otherwise the  $\alpha_i$  would be linearly dependent.

**45.** (to p. 24) For if  $|c_{ik}| \neq 0$ , then the system of equations can be solved for the  $\alpha_k$ . If on the other hand  $|c_{ik}| = 0$ , then the  $\beta_i$  are linearly dependent on one another. Cf. p. 7, 1).

**46.** (to p. 24) From this theorem the so-called *Kronecker-Kneser* theorem follows easily, which says:

If the fields  $\mathfrak{L}_1$  and  $\mathfrak{L}_2$  contain the field  $\mathfrak{K}$  and are finite over it, if further  $\mathfrak{L}_1$  and  $\mathfrak{L}_2$  are at the same time contained in one field, and if  $\mathfrak{B}$  is the smallest field containing  $\mathfrak{L}_1$  and  $\mathfrak{L}_2$ , then  $\mathfrak{B}$  is finite over  $\mathfrak{L}_1$  and  $\mathfrak{L}_2$  and:

$$\begin{aligned} [\mathfrak{B} : \mathfrak{K}] &= [\mathfrak{B} : \mathfrak{L}_1] \cdot [\mathfrak{L}_1 : \mathfrak{K}] \\ &= [\mathfrak{B} : \mathfrak{L}_2] \cdot [\mathfrak{L}_2 : \mathfrak{K}]. \end{aligned}$$

**47.** (to p. 25) In particular, then,  $\mathfrak{K}(j)$  is finite over  $\mathfrak{K}$ . —  $[j : \mathfrak{K}]$  is the degree of the equation irreducible in  $\mathfrak{K}$  that  $j$  satisfies. Cf. p. 21.

The proof is most easily given by referring to § 6, Theorem 3 (together with Erl. 42).

**48.** (to p. 25) This theorem is a companion piece to § 5, Theorem 7.

On the relation of the notion of degree there to the one used here the following is to be remarked: there the degree of a rational function  $\varphi(x)$  of  $x$  was defined, and in such a way that one can equate it with  $[\mathfrak{K}(x) : \mathfrak{K}(\varphi(x))]$ , i.e. the degree of the most comprehensive field over the intermediate field. Here the degree of  $j$  is defined by  $[\mathfrak{K}(j) : \mathfrak{K}]$ , that is, by the degree of the intermediate field over the ground field. Hence there the primitive elements are those of minimal degree, here those of maximal degree. There of course  $[\mathfrak{K}(\varphi(x)) : \mathfrak{K}] = \infty$ , whereas here  $[\mathfrak{L} : \mathfrak{K}(j)]$  is likewise finite.

**49.** (to p. 25) By pp. 21–22,  $\mathfrak{K}(j_1, \dots, j_\nu) = \mathfrak{K}[j_1, \dots, j_\nu]$ , hence: every rational function of elements algebraic over  $\mathfrak{K}$  can also be represented as an integral rational function of these elements.

**50.** (to p. 26) By § 7, Theorem 1.

**51.** (to p. 26) Naturally the extension is again to be constructed so that no proper part of it has the required property.

**52.** (to p. 27) The proof of the following Theorem 1 requires only the introduction of a field  $\mathfrak{M}$  just sufficient for the complete breaking up of  $f(x)$ , but not its derivation from an extension  $\mathfrak{L}$ .

**53.** (to p. 27) Let the result obtained here be stated once more precisely, for the sake of a later application:

Let  $\pi_0$  be an isomorphism between the fields  $\mathfrak{K}_0$  and  $\overline{\mathfrak{K}}_0$ ; further let  $f(x)$  be an irreducible polynomial from  $\mathfrak{K}_0$  and  $\overline{f}(x)$  the polynomial assigned to it by  $\pi_0$ , hence irreducible, from  $\overline{\mathfrak{K}}_0$ ; finally, let  $\mathfrak{K}_1 = \mathfrak{K}_0(j)$  and  $\overline{\mathfrak{K}}_1 = \overline{\mathfrak{K}}_0(\overline{j})$  be simple extensions of  $\mathfrak{K}_0$  and  $\overline{\mathfrak{K}}_0$ , respectively, such that  $j$  and  $\overline{j}$  are zeros of  $f(x)$  and  $\overline{f}(x)$ , respectively.

Then there is an isomorphism  $\pi_1$  between  $\mathfrak{K}_1$  and  $\overline{\mathfrak{K}}_1$  which is an extension of the isomorphism  $\pi_0$ , and under which the element  $\sum_{i=0}^{n-1} c_i j^i$  (where  $n = [\mathfrak{K}_1 : \mathfrak{K}_0] = [\overline{\mathfrak{K}}_1 : \overline{\mathfrak{K}}_0]$ ) is assigned the element  $\sum_{i=0}^{n-1} \overline{c}_i \overline{j}^i$ , where  $c_i$  is from  $\mathfrak{K}_0$  and  $\overline{c}_i$  is the element of  $\overline{\mathfrak{K}}_0$  assigned to  $c_i$  by  $\pi_0$ ; in particular, then,  $j$  is assigned the element  $\overline{j}$ .

On the question of extending isomorphisms compare *R. Dedekind: Suppl. XI in Dirichlet-Dedekind: Zahlentheorie*, 4th ed. Braunschweig 1894; *R. Dedekind: Über die Permutationen des Körpers aller algebraischen Zahlen*, Festschrift aus Anl. d. 150 jähr. Bestehens d. Göttinger Ges. d. Wiss. 1901. Cf. also Appendix A, p. 96, Lemma 1 a, as well as *R. Baer: Abbildungseigenschaften algebraischer Erweiterungen*, § 3; (to appear shortly in the *Math. Zeitschr.*).

**54.** (to p. 28) With this everything is proved that has to be known in the way of algebraic facts in order to prove the theorem on the existence and unique determinacy of the algebraically closed field belonging to a field and algebraic over it. Since, however, the set-theoretic methods not set out until § 19 are needed, we postpone to a later point the proof, which can today be given considerably more simply than *Steinitz* managed.

**55.** (to p. 28) This is quite analogous to § 6, Theorem 2. — The uniqueness here is sharper than there, though, in this sense: a field may indeed contain several smallest extensions of the ground field which contain a zero of a definite polynomial from the ground field, but only a single one which contains all the zeros of the polynomial in question.

**56.** (to p. 28) For normal extensions the designation *Galois* extension field is also customary.

**57.** (to p. 28) This will be shown in Theorem 4.

**58.** (to p. 29) Equations formed with normal functions are also called *Galois* equations.

**59.** (to p. 29) Theorem 4 can also be obtained by specializing Theorem 6 on p. 29.

The converse of Theorem 4 also holds trivially.

**60.** (to p. 29) For under any permutations of the  $j$ ,  $h(x)$  goes over into itself; symmetric functions, however, can be built up from the elementary symmetric ones, that is, from the coefficients of  $f(x)$ , rationally with coefficients from  $\mathfrak{K}_0$ . (Theorem on symmetric functions.)

Cf. *O. Haupt*: Einführung in die Algebra, chapter 8; *A. Korselt*: Vereinfachter Beweis des Hauptsatzes über symmetrische Funktionen, Jahresber. D. M.-V. vol. 37 (1928), pp. 327–330.

A proof of Theorem 4 without using the theorem on symmetric functions is obtained if one bears in mind that Theorem 4 is a trivial consequence of Theorem 6, and Theorem 6 a special case of Addendum 2 to Theorem 1 of Appendix A (p. 98), which is proved without using the theorem on symmetric functions.

**61.** (to p. 29)  $\psi(x_1, x_2, \dots, x_n)$  is an integral function of the  $x_i$  with coefficients from  $\mathfrak{K}_0$  because  $\mathfrak{N}$  is obtained from  $\mathfrak{K}_0$  by successive adjunction of the algebraic elements  $j_1, j_2, \dots, j_n$  (cf. equation (6.) on p. 21 and Erl. 49).

**62.** (to p. 30) This theorem, and likewise Theorem 4, can also be proved without using the theorem on symmetric functions; deeper theorems from *Galois* theory are then needed, however. Cf. Erl. 60.

**63.** (to p. 30) The definition of the derivative of a rational function of an indeterminate  $x$  with coefficients from a field  $\mathfrak{K}$  would be more simply obtained by the following stipulations:

$$1. \quad \frac{dc}{dx} = 0, \text{ if } c \text{ is an element of } \mathfrak{K},$$

$$2. \quad \frac{dx}{dx} = 1,$$

$$3. \quad \frac{d[f(x) + g(x)]}{dx} = \frac{df(x)}{dx} + \frac{dg(x)}{dx},$$

$$4. \quad \frac{d[f(x) \cdot g(x)]}{dx} = \frac{df(x)}{dx} g(x) + \frac{dg(x)}{dx} f(x).$$

The relations

$$\begin{aligned}\frac{d \sum_{i=0}^n a_i x^i}{dx} &= \sum_{i=1}^n i a_i x^{i-1}, \\ \frac{d[f(x) - g(x)]}{dx} &= \frac{df(x)}{dx} - \frac{dg(x)}{dx}, \\ \frac{d \frac{f(x)}{g(x)}}{dx} &= \frac{g(x) \frac{df(x)}{dx} - f(x) \frac{dg(x)}{dx}}{[g(x)]^2}, \\ \frac{d}{dx} f(g(x)) &= f'(g(x)) g'(x)\end{aligned}$$

are then easily derived.

Cf. on this *B. L. v. d. Waerden*: Algebraische Theorie der Differentiation, Nieuw Archief voor Wiskunde vol. 15 (1926) pp. 111–120; *R. Baer*: Algebraische Theorie der differentierbaren Funktionenkörper I, Sitz.-Ber. d. Heidelberger Ak. d. Wiss. Math.-nat. Kl. 1927 (8), p. 15.

**64.** (to p. 34) Theorem 4, and likewise Theorem 4a on p. 34, hold only on passing to suitable extension fields.

**65.** (to p. 34) Alternatively: for  $p = 2$ ,  $-\varepsilon = +\varepsilon$ , hence  $-b = +b$ .

**66.** (to p. 35) These theorems can also be extended to rational functions without further ado by representing them as quotients of relatively prime polynomials. For if in a suitable extension field the rational function is  $R(x) = (x - \alpha_1)^{r_1} \cdots (x - \alpha_\nu)^{r_\nu}$ , where the  $r_i$  are positive or negative integers, then:

$$R(x) = f_1(x) (f_{-1}(x))^{-1} (f_2(x))^2 (f_{-2}(x))^{-2} \cdots,$$

where  $f_m(x)$  is as in the text and  $f_{-m}(x)$  is to be defined as the product of all those linear factors of  $R(x)$ , taken singly, that occur in  $R(x)$  exactly to the power  $-m$ , or  $= \varepsilon$  if there are no such linear factors.

If one now applies Theorems 5, 6, 7 to numerator and denominator of  $R(x)$ , which are after all polynomials, the validity of Theorems 5, 6, 7 follows both for the functions  $f_m(x)$  and for the functions  $f_{-m}(x)$ .

**67.** (to p. 35) In proving these theorems bear in mind that passing from  $F(x)$  to  $F'(x)$  according to the stipulations on p. 30, and likewise forming the greatest common divisor by *Euler's* procedure on p. 14, are rational operations.

**68.** (to p. 35) It does not follow from this that  $f_m(x)$  can be determined rationally, which is moreover in general impossible, since  $p^f$ -th roots occasionally still have to be extracted, e.g. for  $x^p - u = 0$  in  $\mathfrak{P}_p(u)$  on p. 37.

**69.** (to p. 36) By equation (4.) on p. 33.

**70.** (to p. 36) These theorems can of course also serve as the definition of “perfect”.

**71.** (to p. 36) Examples of perfect and imperfect fields of characteristic  $p$  are given first, before the proof of Theorems 1, 2 is completed.

**72.** (to p. 37)  $\mathfrak{P}_p$  is after all isomorphic to the field of residue classes modulo the prime number  $p$ .

**73.** (to p. 37) Theorem 2, to be proved shortly, therefore says among other things that every field  $\mathfrak{L} = \mathfrak{K}(u)$ , where  $\mathfrak{K}$  is of characteristic  $p$ , is imperfect.

**74.** (to p. 37) Cf. § 10, Theorem 1.

**75.** (to p. 37) The theorem of primitive elements is also known in the literature under the name of *Abel's theorem*.

**76.** (to p. 38) Here applying § 2, Theorem 3 is really bringing up too heavy artillery. An element  $\vartheta$  simply lies in the simple extension  $\mathfrak{K}(\vartheta)$ .

**77.** (to p. 38) For every element of  $\mathfrak{L}$  is contained in one of the  $\mathfrak{K}_i$ .

**78.** (to p. 38) The end of the proof can be arranged somewhat more simply:

If the element  $\mu$  of  $\mathfrak{K}$  has been determined as in the text, so that the  $m \cdot n$  elements  $\alpha_i + \mu\beta_k$  are all distinct, we set  $\gamma = \alpha + \mu\beta = \alpha_1 + \mu\beta_1$ . We first determine the greatest common divisor of  $g(x)$  and  $f(\gamma - \mu x)$ .

$g(x)$  has the zeros  $\beta = \beta_1, \beta_2, \dots, \beta_n$ ; the zeros of  $f(\gamma - \mu x)$  are the solutions of the equations  $\gamma - \mu x = \alpha_i$  ( $i = 1, \dots, m$ ),  $x = \frac{\alpha_1 - \alpha_i}{\mu} + \beta_1^*$ ; the question is when one of these expressions equals some  $\beta_k$ . That is the case if and only if  $\alpha_1 + \mu\beta_1 = \alpha_i + \mu\beta_k$ , and this occurs if and only if  $i = k = 1$ . So  $\beta = \beta_1$  is the only zero common to  $g(x)$  and  $f(\gamma - \mu x)$ ; their greatest common divisor is therefore  $x - \beta$ . But since this can be determined rationally, and  $g(x)$ ,  $f(\gamma - \mu x)$  are polynomials from  $\mathfrak{K}(\gamma, x)$ ,  $x - \beta$  also lies in  $\mathfrak{K}(\gamma, x)$ , i.e.  $\beta$  is an element of  $\mathfrak{K}(\gamma)$ . Since finally  $\alpha = \gamma - \mu\beta$ ,  $\alpha$  too is an element of  $\mathfrak{K}(\gamma)$ . Cf. *H. Hasse: Höhere Algebra II*, pp. 82–84.

**79.** (to p. 40) Alternatively: for  $\mathfrak{L}$  is mapped one-to-one onto a subdomain of  $\mathfrak{K}$ , hence onto a proper part of  $\mathfrak{L}$ , namely onto the domain of the  $p$ -th powers of elements of  $\mathfrak{L}$ . So  $\mathfrak{L}$  is infinite, and since  $\mathfrak{L}$  is the one-to-one image of a part of  $\mathfrak{K}$ ,  $\mathfrak{K}$  is infinite too.

**80.** (to p. 40) By equation (4.) on p. 33.

**81.** (to p. 41) For only infinite sets admit a one-to-one correspondence with a proper part of themselves.

**82.** (to p. 41) The construction of  $\mathfrak{K}^{p^{-1}}$  could in itself be carried out by repeated application of § 6, Theorem 2; but since that theorem would possibly have to be applied infinitely often, it would have become necessary to bring in set-theoretic methods of a new kind.

**83.** (to p. 41) The sequence of fields  $\mathfrak{K}^{p^n}$  is a tower of fields open in both directions:

$$\dots > \mathfrak{K}^{p^{-(n+1)}} > \mathfrak{K}^{p^{-n}} > \dots > \mathfrak{K}^{p^{-1}} > \mathfrak{K} > \mathfrak{K}^p > \dots > \mathfrak{K}^{p^n} > \mathfrak{K}^{p^{n+1}} > \dots$$

**84.** (to p. 43) The notion of root element is therefore to be understood in a more special sense than is customary.

**85.** (to p. 43) Carrying  $\mathfrak{T}$  along (instead of  $\mathfrak{L}$ ) is not needed in what follows and could therefore have been omitted.

---

<sup>\*</sup>)  $\mu$  is after all certainly  $\neq 0$  by the way it was chosen.

**86.** (to p. 44) The notion of an algebraic extension of the first kind is fundamental for *Galois* theory in so far as it gives the exact limit of validity of the fundamental theorem on the unique assignability of intermediate fields to subgroups.

Cf. Appendix A, Addendum to Main Theorem 1, p. 101.

**87.** (to p. 45) In general, though, only in a suitable extension field.

**88.** (to p. 46) The proof of Theorem 4 can be given more simply in the following way:

Let  $\mathfrak{L}$  be an algebraic extension of the perfect field  $\mathfrak{K}$  and  $\varphi(x)$  any irreducible polynomial from  $\mathfrak{L}$ . Then  $\varphi(x)$  is a divisor of an irreducible polynomial  $f(x)$  from  $\mathfrak{K}$ , as follows from § 7, Theorem 9. Since  $f(x)$  can have only simple zeros in every extension of  $\mathfrak{L}$  ( $\mathfrak{K}$  is after all perfect), the same holds of  $\varphi(x)$ , i.e.  $\mathfrak{L}$  is perfect. — With this proof Theorem 3 also becomes dispensable.

**89.** (to p. 46) This condition is not only sufficient but also necessary, as is shown.

**90.** (to p. 47) The condition in Theorem 7 also gives the limit of validity of *Abel's* theorem [on the primitive element], which no longer holds in general for finite extensions that are not of the first kind; cf. § 14.

**91.** (to p. 48) If one adds that every isomorphic map of  $\mathfrak{N}$  onto itself can be obtained by replacing the primitive element  $j_1$  by another one  $j_k$ , then the theorem on the equality of the basis degree  $[\mathfrak{N} : \mathfrak{K}]$  and the mapping degree [= the number of distinct isomorphic maps of  $\mathfrak{N}$  onto itself leaving  $\mathfrak{K}$  elementwise fixed] follows from the above.

Cf. *R. Dedekind*: XI. Suppl. in *Dirichlet-Dedekind: Zahlentheorie*, 4th ed.; *O. Haupt*: Einführung in die Algebra II, p. 578, note \*); Appendix A, Theorem 3 a), p. 99.

**92.** (to p. 48) This proves the first main theorem of *Galois* theory, which says that to every subgroup of  $\mathfrak{G}$  there corresponds one and only one intermediate field.

The second main theorem, which says that in this correspondence exactly one subgroup also corresponds to every intermediate field, yields together with the first a one-to-one correspondence of intermediate fields and subgroups. The first main theorem holds if and only if  $\mathfrak{N}$  is of the first kind over  $\mathfrak{K}$ , the second main theorem if and only if  $\mathfrak{N}$  is moreover finite over  $\mathfrak{K}$ .

Cf. Appendix A, Addendum to Main Theorem 1, p. 101, and Main Theorem 3, p. 102.

**93.** (to p. 48) For *Galois* theory the question treated here — whether all fields finite over a ground field are simple over it — is less important than the question, half answered by § 13, Theorems 7 and 8, of when all intermediate fields between a fixed ground field and a fixed overfield are simple over the ground field.

**94.** (to p. 49) By § 13, Theorem 1.

**95.** (to p. 49) On this notion cf. the corresponding notions on p. 44 and the footnote there.

**96.** (to p. 49) By Theorem 3.

**97.** (to p. 49) Since  $\delta$  is by Theorem 1 a root element over  $\mathfrak{L}_0$ .

**98.** (to p. 50) The case  $f = 0$  is trivial, because then  $\mathfrak{L} = \mathfrak{L}_0$  and consequently  $\gamma$  already has the required property.

**99.** (to p. 50) By § 13, Theorem 5.

**100.** (to p. 51) In the case  $n = 1$  it is unnecessary to require that  $t_0 \neq 0$ , since this then already follows from  $\Delta \neq 0$ .

**101.** (to p. 52)  $\mathfrak{M}_r$  is the intersection of  $\mathfrak{M}$  and  $\mathfrak{L}_r$ .

**102.** (to p. 53) The theorems cited have to be brought in because throughout this section the fields in question were assumed to be imperfect, whereas Theorem III does not assume this.

**103.** (to p. 53) An example of an imperfect field satisfying the condition of Theorem IV:

Let  $\mathfrak{P}_p$  be the prime field of prime-number characteristic  $p$ , and let  $\mathfrak{K} = \mathfrak{P}_p(t)$  be a simple transcendental extension.

$\mathfrak{K}^p$  then consists of all rational functions of  $t^p$  with coefficients from  $\mathfrak{P}_p$ , since  $a^p = a$  in  $\mathfrak{P}_p$  and equations (1.), p. 40, hold. So  $\mathfrak{K}^p = \mathfrak{P}_p(t^p)$ , and since  $\mathfrak{K} = \mathfrak{K}^p(t) > \mathfrak{K}^p$  we get  $[\mathfrak{K} : \mathfrak{K}^p] = p$ , so that  $\mathfrak{K}$  is imperfect by § 11, Theorem 2.

**104.** (to p. 54) Cf. Erl. 20.

**105.** (to p. 54) If  $n = rd$ , then

$$p^n - 1 = p^{rd} - 1 = \left( \sum_{i=0}^{r-1} p^{di} \right) (p^d - 1).$$

**106.** (to p. 55) That every subfield corresponds to a divisor of  $n$  follows simply from the fact that its degree  $d$  must divide the degree  $n$ .

**107.** (to p. 56) By Theorem 6.

**108.** (to p. 56) Being a finite field, by § 12, Theorem 2.

**109.** (to p. 56) So every finite field is simple over each of its subfields.

**110.** (to p. 57) Similar to the notion of a  $G$ -number are the ideal numbers in *Prüfer's* sense. Cf. *H. Prüfer: Neue Begründung der algebraischen Zahlentheorie*, Math. Ann. vol. 94 (1925), p. 198.

**111.** (to p. 58) The proof of Theorems 2 and 3 can be simplified as follows:

Let  $m = \prod_{i=1}^{\infty} q_i^{z_i}$  be the given  $G$ -number and  $\mathfrak{P} = \mathfrak{P}_p$  ( $p \neq 0$ ) the prime field in question. Further let  $r_n$  be the greatest common divisor of  $m$  and  $n!$ . Let the distinct ones among the numbers  $r_n$  be numbered by magnitude:  $s_1, s_2, \dots, s_i, s_{i+1}, \dots$ . Then  $s_i$  is a divisor of  $s_{i+1}$  ( $i = 1, 2, \dots$ ). We may assume that the sequence of the  $s_i$  is infinite, since otherwise the  $G$ -number in question would be an ordinary, finite number, and in that case both theorems have already been proved in § 15.

On 2. We construct a chain of fields:

1.  $\mathfrak{K}_0 = \mathfrak{P}$ .
2. Let  $\mathfrak{K}_{n-1}$  already be constructed and have type  $\mathfrak{E}_{p, s_{n-1}}$ . We then consider  $x^{p^{s_n}} - x = 0$  as an equation from  $\mathfrak{K}_{n-1}$ . By § 8, Theorem 2 there is a field  $\mathfrak{K}_n$  which is an algebraic extension field of  $\mathfrak{K}_{n-1}$  and just sufficient for the complete breaking up of this equation. By § 15, Theorem 1 this field has type  $\mathfrak{E}_{p, s_n}$ ; note in this connection § 15, Theorem 3 as well, and the fact that  $s_{n-1}$  is a divisor of  $s_n$ .

If the field  $\mathfrak{K}_n$  is constructed in this way for every integer  $n \geq 0$ , then by § 2, Theorem 2 the union  $\mathfrak{L}$  of these fields  $\mathfrak{K}_n$  is itself a field. Every finite subfield can be obtained by adjoining finitely many elements and is therefore comprised in some field  $\mathfrak{K}_n$ ; its degree is accordingly a divisor of some  $s_n$ , since  $\mathfrak{L}$  too does after all contain fields of all types  $\mathfrak{E}_{p, s_n}$ , i.e. the degree of  $\mathfrak{L}$  is the least common multiple of the numbers  $s_n$ . Since on the other hand the least common multiple of the numbers  $s_n$  is by their construction the  $G$ -number  $m$ , the absolutely algebraic field  $\mathfrak{L}$  — every field  $\mathfrak{K}_n$  is after all absolutely algebraic — has, as required, degree  $m$ .

On 3. Let  $\mathfrak{L}'$  likewise be absolutely algebraic of degree  $m$  and of characteristic  $p$ ; we want to show that  $\mathfrak{L}$  and  $\mathfrak{L}'$  are isomorphic.

We construct a chain of subfields of  $\mathfrak{L}'$ :

1.  $\mathfrak{K}'_0 = \mathfrak{P}'$ , the prime field of  $\mathfrak{L}'$ ; there is then an isomorphism  $\pi_0$  between  $\mathfrak{K}_0$  and  $\mathfrak{K}'_0$ , since  $\mathfrak{L}$  and  $\mathfrak{L}'$  have the same characteristic.
2. Let  $\mathfrak{K}'_{n-1}$  and an isomorphism  $\pi_{n-1}$  between  $\mathfrak{K}_{n-1}$  and  $\mathfrak{K}'_{n-1}$  already be constructed; then so  $\mathfrak{K}'_{n-1}$  too has type  $\mathfrak{E}_{p, s_{n-1}}$ . Then, since  $m$  is the degree of  $\mathfrak{L}'$  and  $s_n$  a divisor of  $m$ , there is a subfield  $\mathfrak{K}'_n$  of  $\mathfrak{L}'$  just sufficient for the breaking up of  $x^{p^{s_n}} - x = 0$ ; since  $s_{n-1}$  is a divisor of  $s_n$ ,  $x^{p^{s_{n-1}}} - x$  is a divisor of  $x^{p^{s_n}} - x$ , hence  $\mathfrak{K}'_{n-1}$  a subfield of  $\mathfrak{K}'_n$ . By § 8, Theorem 1 there is then an isomorphism  $\pi_n$  between  $\mathfrak{K}_n$  and  $\mathfrak{K}'_n$  which comprises  $\pi_{n-1}$ .

By § 2, Theorem 2 the union  $\overline{\mathfrak{L}'}$  of the fields  $\mathfrak{K}'_n$  so constructed is then a subfield of  $\mathfrak{L}'$ . We construct the isomorphism  $\pi$  between  $\mathfrak{L}$  and  $\overline{\mathfrak{L}'}$  as the “union isomorphism” of the isomorphisms  $\pi_n$ , as follows:

If  $a$  is any element of  $\mathfrak{L}$ , there is a smallest  $n = n(a)$  such that  $a$  is an element of  $\mathfrak{K}_n$ . By  $\pi_{n(a)}$  the element  $a$  is then assigned an element  $a'$  of  $\overline{\mathfrak{L}'}$ , and every isomorphism  $\pi_i$  with  $i \geq n(a)$  assigns  $a$  this same  $a'$ , since every isomorphism  $\pi_k$  comprises all  $\pi_i$  with  $k \geq i$ .

Then  $\pi$  assigns  $a$  precisely the  $a'$  that is assigned to  $a$  by  $\pi_{n(a)}$ . This assignment is an isomorphic one, since the  $\pi_n$  are isomorphisms and any two elements  $a_1, a_2$  of  $\mathfrak{L}$  already occur simultaneously in the field  $\mathfrak{K}_{\max[n(a_1), n(a_2)]}$ . That this isomorphism  $\pi$  also exhausts all elements of  $\overline{\mathfrak{L}'}$  follows from the fact that  $\overline{\mathfrak{L}'}$  is the union of the  $\mathfrak{K}'_n$  and the  $\pi_n$  are isomorphisms between  $\mathfrak{K}_n$  and  $\mathfrak{K}'_n$ .

It only remains, then, to show that  $\overline{\mathfrak{L}'} = \mathfrak{L}'$ . If  $a'$  is any element of  $\mathfrak{L}'$ , then  $a'$  is algebraic over  $\mathfrak{P}'$  [ $\mathfrak{L}'$  is after all an absolutely algebraic field], i.e.  $[a' : \mathfrak{P}']$  is a finite number, which by the hypothesis made about  $\mathfrak{L}'$  is a divisor of  $m$ ; so there is a number  $s_n$  such that  $[a' : \mathfrak{P}']$  is a divisor of  $s_n$ . By § 15, Theorem 5,  $a'$  is therefore an element of  $\mathfrak{K}'_n$ , which field is by construction of type  $\mathfrak{E}_{p, s_n}$ , i.e.  $a'$  is an element of  $\overline{\mathfrak{L}'}$ , i.e.  $\overline{\mathfrak{L}'} = \mathfrak{L}'$ .

The reader may now continue in the text on p. 60, at “We now wish”.

**112.** (to p. 58) Here the  $a_\nu = \alpha_\nu \cdot \varepsilon$  are to be replaced by the natural numbers  $\alpha_\nu$  between 0 and  $p - 1$  assigned to them.

**113.** (to p. 59) 1. Since what is at issue are selections from a field that is certainly countable, being absolutely algebraic, the selections can here be made constructively without applying the principle of choice.

2. In the proof we have given (cf. Erl. 111) no selection at all need be made, if one bears in mind further that  $\mathfrak{K}'_n$  is uniquely determined by the conditions imposed on it.

**114.** (to p. 64) The considerations of §§ 18, 20 and 21 are for the most part dispensable for the proof of Main Theorems 8, 9 of § 21. That proof can be carried out substantially more simply without them, admittedly with unrestrained use of the well-ordering theorem and transfinite induction (cf. § 19).

Since the considerations of §§ 18, 20 and 21 are not needed in what follows and, apart from § 18, Theorem 6, are of no independent interest, the reader may read the following in place of them. § 18, Theorem 6 is easily inferred afterwards from Main Theorem 8 of § 21. Proof of § 21, Theorem 8:

A. By *Zermelo's* well-ordering theorem there is a well-ordering of the system of polynomials  $S$ ; we keep one such fixed for the whole course of the proof.

We construct a chain of fields whose first member is  $\mathfrak{K}_0$ .

Let  $\mathfrak{K}_\mu$  already be constructed for all ordinal numbers  $\mu < \nu$  in such a way that  $\mathfrak{K}_\varrho$  is a subfield of  $\mathfrak{K}_\sigma$  whenever  $\varrho < \sigma$ , and let all the  $\mathfrak{K}_\mu$  be algebraic over  $\mathfrak{K}_0$ .

Case 1.:  $\nu$  is not a limit number. Let  $f_{\varrho(\nu)}(x)$  then be the first polynomial from  $S$  that does not yet break up into linear factors in  $\mathfrak{K}_{\nu-1}$ . [If all polynomials from  $S$  already broke up into linear factors in  $\mathfrak{K}_{\nu-1}$ , we would already have been finished with the construction.] Then by § 8, Theorem 2 there is an extension field  $\mathfrak{K}_\nu$  of  $\mathfrak{K}_{\nu-1}$  which is algebraic over  $\mathfrak{K}_{\nu-1}$  and which suffices for the breaking up of  $f_{\varrho(\nu)}(x)^*$ .

Then  $\mathfrak{K}_\nu$  is by § 7, Theorem 9 algebraic over  $\mathfrak{K}_0$  and contains all  $\mathfrak{K}_\mu$  with  $0 \leq \mu \leq \nu$ .

Case 2.:  $\nu$  is a limit number. Then by § 2, Theorem 2 the union of the fields  $\mathfrak{K}_\mu$  with  $0 \leq \mu < \nu$  is a field  $\mathfrak{K}_\nu$  which is algebraic over  $\mathfrak{K}_0$  — it consists after all only of elements algebraic over  $\mathfrak{K}_0$  — and which comprises all  $\mathfrak{K}_\mu$  with  $0 \leq \mu \leq \nu$ .

If  $\sigma$  is then the first ordinal number such that the construction step of Case 1. is no longer applicable to  $\mathfrak{K}_\sigma$  (for the construction of  $\mathfrak{K}_{\sigma+1}$ \*\*), then  $\mathfrak{K}_\sigma$  is a field of the kind sought. For in the first place  $\mathfrak{K}_\sigma$ , like all  $\mathfrak{K}_\nu$ , is algebraic over  $\mathfrak{K}_0$ ; further, all polynomials from  $S$  break up completely in  $\mathfrak{K}_\sigma$ , since in the contrary case the construction step of Case 1. would still be applicable to  $\mathfrak{K}_\sigma$ .

B. Let  $\mathfrak{L}$  now be an extension of  $\mathfrak{K}_0$  in which all polynomials from  $S$  break up completely. We then prove that there is a subfield of  $\mathfrak{L}$  which is an extension of  $\mathfrak{K}_0$  equivalent to  $\mathfrak{K}_\sigma$  and in which all polynomials from  $S$  likewise break up completely. With this our theorem will be completely proved.

To prove our assertion we construct a chain of subfields  $\mathfrak{L}_\nu$  of  $\mathfrak{L}$ :

1.  $\mathfrak{L}_0 = \mathfrak{K}_0$ ,  $\pi_0$  the identity map of  $\mathfrak{K}_0$  onto itself.
2. Let  $\mathfrak{L}_\mu$  already be constructed for all  $0 \leq \mu < \nu$  and let  $\pi_\mu$  be an isomorphism between  $\mathfrak{L}_\mu$  and  $\mathfrak{K}_\mu$  comprising  $\pi_0$ , such that  $\pi_\sigma$  is comprised by  $\pi_\varrho$  for  $\sigma < \varrho$ .

Case 1.: let  $\nu$  not be a limit number. Then, since all polynomials from  $S$  break up completely in  $\mathfrak{L}$ , there is a smallest subfield  $\mathfrak{L}_\nu$  of  $\mathfrak{L}$  comprising  $\mathfrak{L}_{\nu-1}$  which just suffices for the breaking up of  $f_{\varrho(\nu)}(x)$ . By § 8, Theorem 1 there is then an isomorphism  $\pi_\nu$  between  $\mathfrak{L}_\nu$

\*) Since  $\mathfrak{K}_\nu$  is uniquely determined by  $\mathfrak{K}_{\nu-1}$  only up to isomorphisms, an ambiguity — algebraically inessential, to be sure — arises here in the construction.

\*\*) This  $\sigma$  is at most equal to the ordinal number of the well-ordered system  $S$ .

and  $\mathfrak{K}_\nu$  comprising  $\pi_{\nu-1}$ . Clearly  $\pi_\nu$  comprises every  $\pi_\mu$  with  $0 \leq \mu \leq \nu$ , and correspondingly  $\mathfrak{L}_\nu$  every  $\mathfrak{L}_\mu$  with  $0 \leq \mu \leq \nu^*$ .

Case 2.: let  $\nu$  be a limit number. Let  $\mathfrak{L}_\nu$  then be the union of all  $\mathfrak{L}_\mu$  with  $\mu < \nu$ . By § 2, Theorem 2,  $\mathfrak{L}_\nu$  is then a field. Let  $\pi_\nu$  then be the union isomorphism of all  $\pi_\mu$  with  $0 \leq \mu < \nu$ , an isomorphism between  $\mathfrak{L}_\nu$  and  $\mathfrak{K}_\nu$  comprising all  $\pi_\mu$  with  $\mu < \nu$ .

Once  $\mathfrak{L}_\nu$ ,  $\pi_\nu$  are defined in this way for all  $0 \leq \nu \leq \sigma$ , every polynomial from  $S$  breaks up completely into linear factors in  $\mathfrak{L}_\sigma$ , which field is a subfield of  $\mathfrak{L}$ ; for this holds for  $\mathfrak{K}_\sigma$ , and because of the isomorphism  $\pi_\sigma$  comprising  $\pi_0$ ,  $\mathfrak{K}_\sigma$  and  $\mathfrak{L}_\sigma$  are equivalent extensions of  $\mathfrak{K}_0$ .

The reader may now continue in the text on p. 80 at Theorem 9.

**115.** (to p. 68) Attention may be drawn to the following more extensive presentations of set theory:

1. *A. Fraenkel*: Einführung in die Mengenlehre, 3rd ed. Berlin 1928.
2. *F. Hausdorff*: Mengenlehre, 1st and 2nd ed. Berlin 1913 and 1927.
3. *W. Sierpinski*: Leçons sur les nombres transfinis, Paris 1928 (Coll. Borel).

1. takes particular account of the foundations, 2. of the applications to point sets, while 3. is more concerned with “pure” set theory.

**116.** (to p. 68) A rigorous proof of this assertion has not been given to this day; nor, however, has anyone succeeded in proving the contrary.

**117.** (to p. 69) The ordinal number 0 is the order type of the empty set.

**118.** (to p. 70) If a complete induction ranges not merely over a totality of ordinal numbers of the form  $\alpha + n$ , where  $\alpha$  is a fixed ordinal number while  $n$  runs only through the natural numbers, then it is also called, in distinction from ordinary complete induction, **transfinite induction**.

The principle of transfinite induction is usually applied in the following form, which is equivalent to the formulation given by *Steinitz*:

- If any statement holds 1. for the ordinal number  $\alpha \leq \beta$ ,
2. for  $\nu + 1 \leq \beta$  whenever it holds for  $\nu \geq \alpha$ ,
3. for the limit number  $\nu$  with  $\beta \geq \nu > \alpha$  whenever it merely holds for all numbers  $\mu$  with  $\nu > \mu \geq \alpha$ ,

then it holds for all  $\nu$  with  $\alpha \leq \nu \leq \beta$ .

From **proof** by complete induction, **definition** by complete induction is to be carefully distinguished, though it can be brought into a similar form. Cf. on this *J. v. Neumann*: Über die Definition durch transfinite Induktion und verwandte Fragen der allgemeinen Mengenlehre, Math. Ann. vol. 99 (1928), pp. 378 ff., where a foundation is also given for the notion of ordinal number which makes no use of the somewhat suspect notion of order type.

**119.** (to p. 81) For the coefficients of  $\varphi(x)$  are rational functions of the elements of  $\mathfrak{S}$  with coefficients from  $\mathfrak{K}$ ; in each of them, therefore, only finitely many elements of  $\mathfrak{S}$  can occur.

---

<sup>\*)</sup>  $\mathfrak{L}_\nu$  is uniquely determined by  $\mathfrak{L}_{\nu-1}$ ,  $\pi_\nu$  by  $\pi_{\nu-1}$  only up to finitely many possibilities; a unique determination of  $\pi_\nu$  by  $\pi_{\nu-1}$  can, however, always be achieved by well-ordering  $\mathfrak{L}$ .

**120.** (to p. 81) The proof of Theorem 2 can also be put as follows:

Let  $\mathfrak{K}(\mathfrak{S}_1) = \mathfrak{K}_1$ ,  $\mathfrak{K}_1(\mathfrak{S}_2) = \mathfrak{K}_2$ ,  $\mathfrak{K}_2(\mathfrak{S}_3) = \mathfrak{K}_3$ . Then by hypothesis and § 7, Theorem 7,  $\mathfrak{K}_3$  is algebraic over  $\mathfrak{K}_2$  and  $\mathfrak{K}_2$  over  $\mathfrak{K}_1$ . So by § 7, Theorem 9,  $\mathfrak{K}_3$  is algebraic over  $\mathfrak{K}_1$ , and consequently the elements of  $\mathfrak{S}_3$  are algebraic with respect to  $\mathfrak{K}(\mathfrak{S}_1)$ .

**121.** (to p. 81) For if  $\mathfrak{T}$  is a subsystem of  $\mathfrak{S}$  and  $\mathfrak{T}$  is reducible over  $\mathfrak{K}$ , then there is an element  $t$  in  $\mathfrak{T}$  such that  $t$  is algebraic over  $\mathfrak{K}(\overline{\mathfrak{T}})$ , where  $\overline{\mathfrak{T}}$  is the totality of the elements of  $\mathfrak{T}$  different from  $t$ . So  $t$  is also algebraic over  $\mathfrak{K}(\overline{\mathfrak{S}})$ , where  $\overline{\mathfrak{S}}$  is the totality of the elements of  $\mathfrak{S}$  different from  $t$ ; for  $\overline{\mathfrak{T}}$  is a subsystem of  $\overline{\mathfrak{S}}$ , hence  $\mathfrak{K}(\overline{\mathfrak{T}})$  a subfield of  $\mathfrak{K}(\overline{\mathfrak{S}})$ . Consequently  $\mathfrak{S}$  is reducible over  $\mathfrak{K}$  if the subsystem  $\mathfrak{T}$  of  $\mathfrak{S}$  is.

**122.** (to p. 81) For if the system  $\mathfrak{S}$  is reducible, there is an element  $t$  in  $\mathfrak{S}$  such that  $t$  depends algebraically on  $\overline{\mathfrak{S}}$ , the totality of all elements of  $\mathfrak{S}$  different from  $t$ . By Theorem 1 there is then a finite subsystem  $\overline{\mathfrak{T}}$  of  $\overline{\mathfrak{S}}$  on which  $t$  depends algebraically. If  $\mathfrak{T}$  then consists of  $t$  and the elements of  $\overline{\mathfrak{T}}$ , then  $\mathfrak{T}$  is a finite, reducible subsystem of  $\mathfrak{S}$ .

**123.** (to p. 82) In full, the proof of Theorem 5 runs roughly as follows, where we also prove along the way that *over an arbitrary ground field there exist irreducible systems of arbitrary power*:

A. Let  $\sigma$  be an ordinal number of the given power and  $\mathfrak{K}$  the ground field in question. We construct a tower of fields:

1.  $\mathfrak{K}_0 = \mathfrak{K}$ .
2. Let  $\mathfrak{K}_\mu$  already be constructed for all  $\mu < \nu \leq \sigma$ , and in such a way that  $\mathfrak{K}_\lambda$  is a subfield of  $\mathfrak{K}_\mu$  whenever  $\lambda \leq \mu$ .

Case 1.:  $\nu$  is not a limit number. Let  $\mathfrak{K}_\nu = \mathfrak{K}_{\nu-1}(x_{\nu-1})$  then be the field arising from  $\mathfrak{K}_{\nu-1}$  by adjunction, according to § 5, Theorem 1, of the element  $x_{\nu-1}$  transcendental with respect to  $\mathfrak{K}_{\nu-1}$ . Then  $\mathfrak{K}_\nu$  is an overfield of all  $\mathfrak{K}_\mu$  with  $\mu \leq \nu$ .

Case 2.: let  $\nu$  be a limit number. Then the union  $\mathfrak{K}_\nu$  of all  $\mathfrak{K}_\mu$  with  $\mu < \nu$  is by § 2, Theorem 2 a field.

With this  $\mathfrak{K}_\nu$  is defined by complete induction for all  $0 \leq \nu \leq \sigma$ . Likewise  $x_\nu$  is defined for all  $0 \leq \nu < \sigma$ .

The totality  $\mathfrak{S}$  of the  $x_\nu$  has order type  $\sigma$ . Further,  $\mathfrak{S}$  is an irreducible system over  $\mathfrak{K}$ . We prove this by transfinite induction: let  $\mathfrak{S}_\nu$  be the system of all  $x_\mu$  with  $0 \leq \mu < \nu$ , for  $0 \leq \nu \leq \sigma$ . Then  $\mathfrak{S} = \mathfrak{S}_\sigma$ .

$\mathfrak{S}_0$  is certainly an irreducible system over  $\mathfrak{K}$ , for  $\mathfrak{S}_0$  consists only of the element  $x_0$ , transcendental over  $\mathfrak{K}$ .

Let it already be proved for all  $0 \leq \mu < \nu \leq \sigma$  that  $\mathfrak{S}_\mu$  is irreducible over  $\mathfrak{K}$ . Then  $\mathfrak{S}_\nu$  too is irreducible over  $\mathfrak{K}$ . For if  $\nu$  is not a limit number, then by construction  $x_{\nu-1}$  is transcendental over  $\mathfrak{K}(\mathfrak{S}_{\nu-1})$ , so that with  $\mathfrak{S}_{\nu-1}$ ,  $\mathfrak{S}_\nu$  too is irreducible. If on the other hand  $\nu$  is a limit number, then  $\mathfrak{S}_\nu$  is the union of all  $\mathfrak{S}_\mu$  with  $\mu < \nu$ . If  $\mathfrak{S}_\nu$  were now reducible, then by § 22, Theorem 4 there would be a finite reducible subsystem  $\{x_{\nu_i}\}$  ( $i = 1, \dots, n$ ),  $0 \leq \nu_i < \nu$ , in  $\mathfrak{S}_\nu$ . But this already belongs to  $\mathfrak{S}_{\max(\nu_1, \dots, \nu_n)+1}$ , whose index is certainly smaller than  $\nu$  and which must therefore by hypothesis be irreducible, so that it cannot contain a reducible subsystem. Contradiction! With this it is shown by transfinite induction that for all  $0 \leq \nu \leq \sigma$  the system  $\mathfrak{S}_\nu$  is irreducible over  $\mathfrak{K}$ , and in particular also that  $\mathfrak{S}_\sigma = \mathfrak{S}$  is irreducible over  $\mathfrak{K}$ .

Finally  $\mathfrak{K}_\sigma = \mathfrak{K}(\mathfrak{S})$  is the extension sought.

B. Let  $\mathfrak{K}(\mathfrak{S}_1)$ ,  $\mathfrak{K}(\mathfrak{S}_2)$  now be two purely transcendental extensions of  $\mathfrak{K}$ , and let  $\mathfrak{S}_1$  and  $\mathfrak{S}_2$  be irreducible over  $\mathfrak{K}$  and of equal power. Then there is a one-to-one map  $\varphi$  of  $\mathfrak{S}_1$  onto  $\mathfrak{S}_2$ . Further, every element of  $\mathfrak{K}(\mathfrak{S}_1)$  can be represented as a rational function in certain elements of  $\mathfrak{S}_1$  with coefficients from  $\mathfrak{K}$ . If one here replaces each of these elements of  $\mathfrak{S}_1$  by the element of  $\mathfrak{S}_2$  assigned to it by  $\varphi$ , then to every element of  $\mathfrak{K}(\mathfrak{S}_1)$  one and only one element of  $\mathfrak{K}(\mathfrak{S}_2)$  is assigned, and this assignment represents an isomorphism of these two fields. For the fact that this assignment is one-to-one follows from the fact that  $\mathfrak{S}_1$  and  $\mathfrak{S}_2$  are irreducible systems, between whose elements no algebraic relations can hold. That the assignment is an isomorphism, however, now follows simply from its definition.

If instead of one ground field one starts from isomorphic ground fields, one obtains in general the

**Theorem:** *To every field type  $\mathfrak{T}$  and every power  $\mathfrak{m}$  there is one and only one field type  $\mathfrak{T}_\mathfrak{m}$  which represents a purely transcendental extension of  $\mathfrak{T}$  and is obtained by adjoining an irreducible system of power  $\mathfrak{m}$  to  $\mathfrak{T}$ .*

**124.** (to p. 82) One can make the proof of Theorem 7 somewhat more transparent in the following way:

$a$  satisfies a certain irreducible algebraic equation  $\sum_{i=0}^n a_i x^i = 0$  with coefficients  $a_i$  from the field  $\mathfrak{K}(\mathfrak{S})$ . The  $a_i$  are therefore rational functions in certain [finitely many] elements of  $\mathfrak{S}$  with coefficients from the ground field  $\mathfrak{K}$ . It can even be assumed that the  $a_i$  are relatively prime polynomials [any denominators can after all be removed by multiplication, and any common divisors by division], so that our equation is the irreducible, primitive equation from  $\mathfrak{K}(\mathfrak{S})$ , determined uniquely up to a factor from  $\mathfrak{K}$ , which  $a$  satisfies.

The elements of  $\mathfrak{S}$  actually occurring in the  $a_i$  form a [finite] system  $\mathfrak{T}$ , of which we want to show that it has the properties stated in Theorem 7.

1.  $a$  depends algebraically on the subsystem  $\mathfrak{T}$  of  $\mathfrak{S}$  by its definition.  
 2. Let  $\mathfrak{T}'$  be a subsystem of  $\mathfrak{S}$  on which  $a$  depends algebraically. Then  $a$  satisfies an equation  $\sum_{i=0}^m b_i x^i = 0$  with coefficients  $b_i$  from  $\mathfrak{K}(\mathfrak{T}')$ . Then  $\sum_{i=0}^n a_i x^i$  is a divisor of  $\sum_{i=0}^m b_i x^i$  and, since  $\sum_{i=0}^n a_i x^i$  is an irreducible, primitive polynomial,  $\mathfrak{T}$  too is a subsystem of  $\mathfrak{T}'$ .

3. Let  $\mathfrak{T} = \{t_1, \dots, t_n\}$ . Further  $\sum_{i=0}^n a_i a^i = 0$  holds. Since the  $a_i$  are polynomials in the  $t_k$ , we can also expand the polynomial  $\sum_{i=0}^n a_i a^i$  in powers of any  $t_k$ . Let  $\sum_{i=0}^s c_i t_k^i$  be such an expansion. Then the  $c_i$  cannot all vanish, since otherwise  $a$  would depend algebraically even on the elements of  $\mathfrak{T}$  different from  $t_k$ , contrary to 2. But since  $\sum_{i=0}^s c_i t_k^i = \sum_{i=0}^n a_i a^i = 0$ , one can in  $\mathfrak{T}$  replace  $a$  by  $t_k$  and obtains an equivalent, irreducible system.

4. Let  $\mathfrak{T}'$  be any subsystem of  $\mathfrak{S}$  on which  $a$  depends algebraically. Then  $\mathfrak{T}$  is by 2. contained in  $\mathfrak{T}'$ . Let  $t$  be an element of  $\mathfrak{T}'$  not belonging to  $\mathfrak{T}$ . If one could now replace the element  $t$  in  $\mathfrak{T}'$  by  $a$ , there would be an equation  $\sum_{i=0}^q d_i x^i = 0$  satisfied by  $t$ , where the  $d_i$  are elements of the field  $\mathfrak{K}(\overline{\mathfrak{T}}, a)$ . Here  $\overline{\mathfrak{T}}$  arises from  $\mathfrak{T}'$  by omitting  $t$ . But since  $\overline{\mathfrak{T}}$  comprises  $\mathfrak{T}$  and  $a$  depends algebraically on  $\mathfrak{T}$ , hence also on  $\overline{\mathfrak{T}}$ ,  $t$  would then depend algebraically on  $\overline{\mathfrak{T}}$ , so that  $\mathfrak{S}$  would by Theorem 3 not be irreducible. Contradiction!

125. (to p. 82) By Theorem 1.

126. (to p. 84) The proof of this theorem is somewhat simpler in the following arrangement:

Let  $\mathfrak{L}$  be a field comprising  $\mathfrak{K}$ , and  $\mathfrak{S}_1$  and  $\mathfrak{S}_2$  two systems irreducible over  $\mathfrak{K}$  such that  $\mathfrak{L}$  is algebraic over  $\mathfrak{K}(\mathfrak{S}_i)$  ( $i = 1, 2$ ). *It is to be shown that  $\mathfrak{S}_1$  and  $\mathfrak{S}_2$  are of equal power.*

For the proof we well-order  $\mathfrak{S}_1$  and  $\mathfrak{S}_2$ , and this well-ordering is kept fixed in what follows:

$$\begin{aligned}\mathfrak{S}_1 &= \{a_\nu\}, & 0 \leq \nu < \alpha \\ \mathfrak{S}_2 &= \{b_\nu\}, & 0 \leq \nu < \beta.\end{aligned}$$

A chain of systems  $\mathfrak{T}_\nu$  irreducible over  $\mathfrak{K}$  is then constructed, all of which are equivalent to one another and to  $\mathfrak{S}_1$  and of equal power with them, and the last of which comprises  $\mathfrak{S}_2$ .

1.  $\mathfrak{T}_0 = \{a_{0\nu}\} = \mathfrak{S}_1$ ,  $a_{0\nu} = a_\nu$ ,  $0 \leq \nu < \alpha$ .

2. Let  $\mathfrak{T}_\varrho$  already be constructed for all  $0 \leq \varrho < \sigma$ ,  $\mathfrak{T}_\varrho = \{a_{\varrho\nu}\}$ ,  $0 \leq \nu < \alpha$ , so that the following hold:

a $_\sigma$ .) For  $0 \leq \varrho < \sigma$ ,  $\mathfrak{T}_\varrho$  consists only of elements occurring in at least one of the sets  $\mathfrak{S}_1$  and  $\mathfrak{S}_2$ .

b $_\sigma$ .) For fixed  $\nu$ , either all  $a_{\varrho\nu}$  with  $0 \leq \varrho < \sigma$  are equal to one another, or there is a  $\varrho(\nu)$  such that all  $a_{\varrho\nu}$  with  $0 \leq \varrho \leq \varrho(\nu)$  are equal to one another and all  $a_{\varrho\nu}$  with  $\varrho(\nu) + 1 \leq \varrho < \sigma$  are equal to one another.

c $_\sigma$ .) For  $0 \leq \varrho < \sigma$ ,  $\mathfrak{T}_\varrho$  is irreducible over  $\mathfrak{K}$ .

d $_\sigma$ .) For  $0 \leq \varrho < \sigma$ ,  $\mathfrak{L}$  is algebraic over  $\mathfrak{K}(\mathfrak{T}_\varrho)$ .

Case 1.: let  $\sigma$  not be a limit number. If  $\mathfrak{S}_2$  is then not a subset of  $\mathfrak{T}_{\sigma-1}$  (in the other case we would have reached the goal of our construction), then there is a first element  $b_\lambda = b_{\lambda(\sigma)}$  in  $\mathfrak{S}_2$  which does not yet occur in  $\mathfrak{T}_{\sigma-1}$ . By d $_\sigma$ .),  $b_\lambda$  is algebraically dependent on  $\mathfrak{T}_{\sigma-1}$ . By § 22, Theorem 7 there is then a finite subsystem  $\mathfrak{U}_{\sigma-1}$  of  $\mathfrak{T}_{\sigma-1}$  such that  $b_\lambda$  already depends algebraically on  $\mathfrak{U}_{\sigma-1}$  but on no proper part of  $\mathfrak{U}_{\sigma-1}$ , and this subsystem is thereby uniquely determined.  $\mathfrak{U}_{\sigma-1}$  cannot consist only of elements of  $\mathfrak{S}_2$ , since  $b_\lambda$  is an element of  $\mathfrak{S}_2$ , depends algebraically on  $\mathfrak{U}_{\sigma-1}$ , and  $\mathfrak{S}_2$  is irreducible over  $\mathfrak{K}$ . Let  $a_{\sigma-1, \nu(\lambda)}$  then be the first element of  $\mathfrak{U}_{\sigma-1}$  not belonging to  $\mathfrak{S}_2$ . We then define  $\mathfrak{T}_\sigma = \{a_{\sigma\nu}\}$  by the following equations:

$$a_{\sigma\nu} = \begin{cases} a_{\sigma-1, \nu} & \text{for } \nu \neq \nu(\lambda) \\ b_\lambda & \text{for } \nu = \nu(\lambda) \end{cases}, \quad 0 \leq \nu < \alpha.$$

It is then to be shown that the propositions a $_{\sigma+1}$ .) to d $_{\sigma+1}$ .) are likewise true: a $_{\sigma+1}$ .) and b $_{\sigma+1}$ .) are correct by construction without further ado, provided only that a $_\sigma$ .) and b $_\sigma$ .) are correct. c $_{\sigma+1}$ .) and d $_{\sigma+1}$ .) follow from § 22, Theorem 7.

Case 2.: let  $\sigma$  be a limit number. We form  $\mathfrak{T}_\sigma$  as follows:

If for all  $0 \leq \varrho < \sigma$  the  $a_{\varrho\nu}$  are equal to one another for fixed  $\nu$ , let  $a_{\sigma\nu}$  too be equal to all these  $a_{\varrho\nu}$ . In the other case there is at least one  $\varrho(\nu)$  such that all  $a_{\varrho\nu}$  with  $\varrho(\nu) + 1 \leq \varrho < \sigma$  are equal to one another; we set  $a_{\sigma\nu} = a_{\varrho(\nu)+1, \nu}$ .

Again a $_{\sigma+1}$ .), b $_{\sigma+1}$ .) are satisfied without further ado provided only that a $_\sigma$ .), b $_\sigma$ .) are.

If  $\mathfrak{T}_\sigma$  were reducible, then by § 22, Theorem 4 there would be a finite reducible subsystem  $\mathfrak{R}_\sigma$  of  $\mathfrak{T}_\sigma$ . By the construction of  $\mathfrak{T}_\sigma$  this would have to occur already in some  $\mathfrak{T}_\varrho$  with  $\varrho < \sigma$ , which is impossible, since by c $_\sigma$ .) the  $\mathfrak{T}_\varrho$  are irreducible and § 22, Theorem 3 holds. So c $_{\sigma+1}$ .) is correct.

If finally  $a$  is any element of  $\mathfrak{L}$ , then by § 22, Theorem 1 it already depends algebraically on a finite subsystem  $\mathfrak{A}_0$  of  $\mathfrak{T}_0 = \mathfrak{S}_1$ . If

$$\mathfrak{A}_0 = \{a_{0\nu_1}, \dots, a_{0\nu_n}\}, \text{ then let}$$

$$\mathfrak{A}_\varrho = \{a_{\varrho\nu_1}, \dots, a_{\varrho\nu_n}\}.$$

By construction  $a$  then depends algebraically on the  $\mathfrak{A}_\varrho$  as well; since these  $\mathfrak{A}_\varrho$  are finite systems, by b <sub>$\sigma$</sub> .) they no longer change from a certain  $\varrho$  on, so that  $\mathfrak{A}_\sigma$  is equal to one of them, i.e.  $a$  depends algebraically on the subsystem  $\mathfrak{A}_\sigma$  of  $\mathfrak{T}_\sigma$ . d <sub>$\sigma+1$</sub> .) therefore holds as well.

If  $\sigma$  is a limit number and a <sub>$\varrho$</sub> .)–d <sub>$\varrho$</sub> .) are true for all  $0 \leq \varrho < \sigma$ , one easily verifies that a <sub>$\sigma$</sub> .)–d <sub>$\sigma$</sub> .) are then true as well.

In this way we finally reach a  $\mathfrak{T}_\tau$  which contains  $\mathfrak{S}_2$  as a subsystem<sup>\*)</sup>. Further a <sub>$\tau+1$</sub> .) to d <sub>$\tau+1$</sub> .) hold, so that  $\mathfrak{S}_2 = \mathfrak{T}_\tau$  must hold; for  $\mathfrak{S}_2$  and  $\mathfrak{T}_\tau$  are both irreducible over  $\mathfrak{K}$ , and  $\mathfrak{L}$  is algebraic both over  $\mathfrak{K}(\mathfrak{S}_2)$  and over  $\mathfrak{K}(\mathfrak{T}_\tau)$ .

But with this the elements of  $\mathfrak{S}_2$  are well-ordered (namely as elements of  $\mathfrak{T}_\tau$ ) in such a way that  $\mathfrak{S}_2$  has in the new well-ordering the same order type  $\alpha$  as  $\mathfrak{S}_1$ ; in particular, then,  $\mathfrak{S}_1$  and  $\mathfrak{S}_2$  are of equal power.

The hypotheses made now say, as one easily sees, that  $\mathfrak{S}_1$  and  $\mathfrak{S}_2$  are equivalent, irreducible systems. It has been proved that they are then of equal power, i.e. § 23, Theorem 3, p. 88, at which point the reader may now read on<sup>\*\*)</sup> .

**127.** (to p. 88) Note that the systems  $\mathfrak{S}$  and  $\mathfrak{T}$  have no element in common.

**128.** (to p. 89) By Theorems 5 and 6 the problem of investigating the possible field types is reduced to finding all fields between certain ground fields and the algebraically closed fields algebraic over them. But that is the basic task of *Galois* theory.

**129.** (to p. 89) Settling this question in the affirmative would have far-reaching consequences. One could then prove that *to every prescribed finite group  $\mathfrak{G}$  there exist absolutely algebraic normal fields of characteristic 0 whose Galois group is precisely  $\mathfrak{G}$* . We carry this out below:

Let  $\mathfrak{K}$  first be an arbitrary field. Let the given group  $\mathfrak{G}$  be represented as a transitive permutation group of a suitable number  $n$  of elements (e.g. by assigning to each element the permutation of the group elements effected by multiplying by it on the right — the so-called regular representation — *Cayley's* group table). Let  $\mathfrak{L} = \mathfrak{K}(\xi_1, \dots, \xi_n)$  be a purely transcendental extension of  $\mathfrak{K}$  of transcendence degree  $n$ . Further let  $x_1, \dots, x_n$  be the elementary symmetric functions of  $\xi_1, \dots, \xi_n$  and  $\mathfrak{E} = \mathfrak{K}(x_1, \dots, x_n)$ . Then  $\mathfrak{L}$  is a normal, finite, algebraic extension of the first kind of  $\mathfrak{E}$ , and the *Galois* group of  $\mathfrak{L}$  over  $\mathfrak{E}$  is the symmetric group  $\mathfrak{S}$  on  $n$  elements (cf. on this Appendix A, Theorem 7, p. 104).

Let  $\mathfrak{J}$  now be the totality of all elements of  $\mathfrak{L}$  invariant under the permutations from  $\mathfrak{G}$ . That is a definite field between  $\mathfrak{E}$  and  $\mathfrak{L}$ . By the main theorem of *Galois* theory (cf. Main Theorem 3 of Appendix A, p. 102), applied to  $\mathfrak{L}$  over  $\mathfrak{E}$ ,  $\mathfrak{G}$  is then the totality of the permutations from  $\mathfrak{S}$  under which  $\mathfrak{J}$  remains elementwise invariant, i.e.  $\mathfrak{G}$  is the *Galois* group of  $\mathfrak{L}$  over  $\mathfrak{J}$ .

<sup>\*)</sup>  $\tau \leq \beta$ .

<sup>\*\*)</sup>  Note that with this arrangement of the proof an application of *Bernstein's* equivalence theorem becomes unnecessary; cf. also *O. Haupt: Algebra II*, chapter 23, 6, pp. 591–594; the proof printed there, going back to *E. Noether*, did not seem to fit so well into the text, however.

If now the question raised in the text is settled in the affirmative, then  $\mathfrak{J}$  is purely transcendental of transcendence degree  $n$  over  $\mathfrak{K}$ , since  $\mathfrak{J}$  lies between the purely transcendental extensions  $\mathfrak{L}$  and  $\mathfrak{E}$  of transcendence degree  $n$ . Let, say,  $\mathfrak{J} = \mathfrak{K}(j_1, \dots, j_n)$  with algebraically independent  $j_1, \dots, j_n$ .

Since  $\mathfrak{L}$  is of the first kind and finite over  $\mathfrak{E}$ , hence also over  $\mathfrak{J}$ ,  $\mathfrak{L}$  is by § 11, Theorem 4 simple over  $\mathfrak{J}$ . Let  $\vartheta$  then be a primitive element of  $\mathfrak{L}$  with respect to  $\mathfrak{J}$  and  $g(t) = 0$  the irreducible equation from  $\mathfrak{J}$  satisfied by  $\vartheta$ . Apart from  $t$ ,  $g(t)$  depends rationally on the algebraically independent elements  $j_1, \dots, j_n$ . Because of their algebraic independence these may be regarded as “independent variables”, i.e. all rational relations are preserved if arbitrary elements of  $\mathfrak{K}$  are substituted for them.

If now in particular  $\mathfrak{K}$  is the prime field of characteristic 0 [or another field over which *Hilbert's* irreducibility theorem holds], then elements of  $\mathfrak{K}$  can be substituted for  $j_1, \dots, j_n$  in such a way that  $g(t)$  remains irreducible. By this substitution the degree and the group of  $\mathfrak{L}$  over  $\mathfrak{J}$  therefore remain unchanged (the group, because it is described by the substitutions of the roots of  $g(t)$ ), i.e. the resulting field  $\overline{\mathfrak{L}}$  has over  $\overline{\mathfrak{J}} = \mathfrak{K}$  the prescribed group  $\mathfrak{G}$ .