SOME THEOREMS ON THE CONNECTION BETWEEN IDEALS AND GROUP OF A GALOIS FIELD*

BY

OYSTEIN ORE

Let K be a Galois field of order N and G the corresponding finite group. We shall in this paper study some connections between the ideals in K and the constitution of the group G.

Let $\mathfrak{A}$ be an arbitrary ideal in K. We then introduce a subgroup G_A† of G, which we call *the group of the ideal* $\mathfrak{A}$ and which is defined in the following way. The group G_A consists of all substitutions S in G having the property that for every number α in $\mathfrak{A}$ the conjugate number $\alpha' = S:\alpha$ is also a number in $\mathfrak{A}$.

When $\mathfrak{A} = \mathfrak{P}$ is a prime ideal the group G_P of $\mathfrak{P}$ is equal to the "Zerlegungs" group of $\mathfrak{P}$, studied by Dedekind‡ and Hilbert.§ It is known that the group G_P is a metacyclic group, and that the form of the prime-ideal decomposition of the corresponding rational prime p is closely connected with the properties of this group.

In §1 we study the properties of the general groups G_A and completely determine their construction. In §2 we deal with the properties of the field K_A corresponding to the group G_A, and we prove that K_A is the subfield of K of lowest degree for which there exists an exponent n, such that $\mathfrak{A}^n$ is an ideal in the field. In §3 we study another generalization of the "Zerlegungs" field of Hilbert, namely the fields wherein all numbers are congruent to a rational number (mod $\mathfrak{A}^\alpha$) for an arbitrarily great α, and for a given $\mathfrak{A}$ we determine all the fields having this property.

In another paper I shall use these results in a more elaborate study of the arithmetic of Galois fields and their subfields.

1. **Determination of the group of an ideal.** Let G_A be the group of the ideal $\mathfrak{A}$; then G_A consists of all substitutions in G transforming every number α in $\mathfrak{A}$ into another number $\alpha' = S:\alpha$ also contained in $\mathfrak{A}$. These substitutions obviously form a group, because the product SS' of two substitutions in G_A

* Presented to the Society, October 29, 1927; received by the editors in October, 1927.

† For typographical reasons, italic letters have been substituted, in subscripts and superscripts, for the corresponding German letters.

‡ R. Dedekind, *Zur Theorie der Ideale*, Göttinger Nachrichten, 1894.

§ D. Hilbert, *Grundzüge einer Theorie des Galoisschen Zahlkörpers*, Göttinger Nachrichten, 1894.

must also change α into $\alpha''=SS':\alpha$, where α'' is also contained in $\mathfrak{A}$.

When S is a substitution in G_A, then S cannot transform a number β not contained in $\mathfrak{A}$ into a number α' in $\mathfrak{A}$, because from $S:\beta=\alpha'$ it follows that the substitution S^{-1} in G_A must transform α' into β, which is evidently not possible.

When $\mathfrak{A}$ is an ideal in any subfield k of K, the group G_A obviously contains the corresponding subgroup $G^{(k)}$ of G. On the other hand, there exist ideals $\mathfrak{A}$ not contained in k, such that $\mathfrak{A}$ is invariant under all substitutions of the group $G^{(k)}$. In §2 we shall, for a given subfield k, determine all ideals in K having this property.

In particular, when $[a]=\mathfrak{A}$ is a principal ideal and a a rational integer, then G_A is equal to the complete group G. From this remark we can derive a more available criterion for the determination of the substitutions of the group G_A.

The ideal $\mathfrak{A}$ always contains rational numbers, for instance the norm $N=N(\mathfrak{A})$ of the ideal. We can further find a number α in $\mathfrak{A}$ such that the ideals

$$[N],\quad [\alpha]/\mathfrak{A}$$

are relatively prime; the principal ideals $[N]$ and $[\alpha]$ consequently have the greatest common ideal factor $\mathfrak{A}$. Let us call α a ***primary number*** in $\mathfrak{A}$. When therefore β is an arbitrary number in $\mathfrak{A}$, a number γ can always be determined such that

$$\beta \equiv \alpha\gamma \qquad (\operatorname{mod} N).$$

Consequently if a substitution S transforms α into α', where α' also belongs to $\mathfrak{A}$, the substitution S must be a substitution in G_A, because the arbitrary number β in $\mathfrak{A}$ is transformed into the number

$$\beta' = S:\beta \equiv \alpha'\gamma' \qquad (\operatorname{mod} N),$$

where β' must be a number in $\mathfrak{A}$.

THEOREM 1. *If α is a primary number in an ideal $\mathfrak{A}$, and S a substitution transforming α into α' also belonging to $\mathfrak{A}$, then S is a substitution of the group G_A of $\mathfrak{A}$.*

The group G_A consists of the substitutions of G for which the ideal $\mathfrak{A}$ is invariant. If r_A is the order and $s_A=N/r_A$ is the index of the group G_A, we can write the whole group G as a partition of co-sets corresponding to G_A,

$$G = G_A + G_AV_2 + \cdots + G_AV_{s_A},$$

where V_i are certain substitutions in G. Correspondingly we have s_A different conjugate ideals

$$\mathfrak{A} = \mathfrak{A}_1, \mathfrak{A}_2, \cdots, \mathfrak{A}_{s_A},$$

where the group of an ideal $\mathfrak{G}_i$ is

$$G_{A_i} = V_i^{-1} G_A V_i.$$

For the norm of $\mathfrak{A}$ in K we therefore have the expression

$$N(\mathfrak{A}) = (\mathfrak{A}_1 \cdots \mathfrak{A}_{s_A})^{r_A}. \tag{1}$$

We shall now examine the construction of the groups G_A and we first mention the following, almost obvious theorem:

Theorem 2. *The group G_{A^a} of a power is equal to the group G_A of $\mathfrak{A}$.*

We also easily prove

Theorem 3. *When the norms $N(\mathfrak{A})$ and $N(\mathfrak{B})$ of two ideals $\mathfrak{A}$ and $\mathfrak{B}$ are relatively prime,then the group G_C of the product $\mathfrak{C} = \mathfrak{A}\mathfrak{B}$ is equal to the greatest common subgroup (G_A, G_B) of the groups G_A and G_B.*

When namely S is a substitution in (G_A, G_B), then evidently S belongs to G_C. Conversely, if S is a substitution in G_C, then $\mathfrak{A}$ and $\mathfrak{B}$ must both be invariant with respect to S, because if

$$S{:}\mathfrak{A} = \mathfrak{A}', \quad S{:}\mathfrak{B} = \mathfrak{B}',$$

we have from the definition of G_C

$$\mathfrak{A}'\mathfrak{B}' = \mathfrak{A}\mathfrak{B}. \tag{2}$$

Now the norms $N(\mathfrak{A})$ and $N(\mathfrak{B})$ are relatively prime, so that $\mathfrak{B}$ cannot have any common factor with any of the conjugates $\mathfrak{A}'$ of $\mathfrak{A}$, and consequently we obtain from (2)

$$\mathfrak{A}' = \mathfrak{A}, \mathfrak{B}' = \mathfrak{B},$$

and S belongs to (G_A, G_B).

Theorem 3 obviously also holds for an arbitrary number of ideals, whose norms are all relatively prime. The problem of the determination of the general group G_A is therefore reduced to the case where the norm of $\mathfrak{A}$ is the power of a rational prime p, and $\mathfrak{A}$ therefore only contains prime ideals dividing p.

We now prove

Theorem 4. *If $\mathfrak{A}$ is an ideal containing only prime ideals $\mathfrak{P}$ dividing the same rational prime p, we can uniquely write $\mathfrak{A}$ in the form*

$$\mathfrak{A} = \mathfrak{A}_1^{a_1} \cdots \mathfrak{A}_r^{a_r} \tag{3}$$

where all exponents a_i are different, all $\mathfrak{A}_i$ relatively prime, and in general

$$\mathfrak{A}_i = \mathfrak{P}_i \mathfrak{P}_i' \cdots \qquad (i = 1, 2, \cdots, r)$$

is the product of different, conjugate prime ideals. Then the group G_A is equal to the greatest common subgroup of all groups G_{A_i}.

$$G_A = (G_{A_1}, G_{A_2}, \cdots, G_{A_r}). \tag{4}$$

It is obvious that a unique representation of $\mathfrak{A}$ in the form (3) always exists. If now S is a substitution contained in G', where

$$G' = (G_{\alpha_1}, \cdots, G_{\alpha_r}), \ \alpha_i = \mathfrak{A}_i^{a_i},\text{*} \tag{5}$$

is the greatest common subgroup of all the groups G_{α_i}, then $\mathfrak{A}$ is evidently invariant with respect to S, so that S is contained in G_A.* When on the other hand S is a substitution in G_A, we can prove that S leaves all ideals $\mathfrak{A}_i^{a_i}$ unaltered, and consequently belongs to G'. For if $S{:}\mathfrak{A} = \mathfrak{A}'$ is the transformed ideal of $\mathfrak{A}$, we can only have $\mathfrak{A} = \mathfrak{A}'$ if at the same time $S{:}\, \mathfrak{A}_i^{a_i} = \mathfrak{A}_i^{a_i}$ for all i, because if S transforms a prime ideal $\mathfrak{P}_1$ in $\mathfrak{A}_1$ into, for instance, the prime ideal $\mathfrak{P}_2$ in $\mathfrak{A}_2$, then the ideal $\mathfrak{A}'$ must contain the prime ideal $\mathfrak{P}_2$ to the power $\mathfrak{P}_2^{a_1}$ and consequently $\mathfrak{A} \neq \mathfrak{A}'$, contrary to the definition of S. We therefore have $G_A = G'$ and if we apply Theorem 2 to the expression (5) for G' we obtain the formula (4).

It now only remains to study the groups of ideals having the form

$$\mathfrak{A} = \mathfrak{P}_{s_1} \mathfrak{P}_{s_2} \cdots \mathfrak{P}_{s_t}, \tag{6}$$

where the prime ideals $\mathfrak{P}_s$ are all different, but factors of the same rational prime p.

If G_P is the group of an arbitrary prime ideal dividing p (the "Zerlegungs" group of $\mathfrak{P}$), we obtain from (1)

$$p^f = (\mathfrak{P}_1 \cdots \mathfrak{P}_{s_P})^{r_P}$$

and from this relation we immediately derive the well known result

$$p = (\mathfrak{P}_1 \cdots \mathfrak{P}_{s_P})^e, \ e = \frac{r_P}{f}, \tag{7}$$

where e and f denote the order and the degree of the prime ideal $\mathfrak{P} = \mathfrak{P}_1$.

The corresponding groups of the prime ideals in (7),

$$G_{P_1}, G_{P_2}, \cdots, G_{P_\pi}, \qquad \pi = s_P,$$

are all conjugate: their greatest common subgroup H is a self-conjugate

* See second foot note on page 610.

subgroup of the complete group G. We write the group G in co-sets corresponding to H:

$$(8) \qquad G = H + HV_2 + \cdots + HV_{s_H},$$

where s_H is the index of H, and

$$V_2, \cdots, V_{s_H}$$

are certain substitutions in G. By means of (8) we construct the factor group G/H of order s_H. The substitutions of H produce no permutation in the order of the prime ideals in (7),

$$\mathfrak{P}_1, \mathfrak{P}_2, \cdots, \mathfrak{P}_{s_P},$$

but all the substitutions of an arbitrary co-set HV_k produce the same permutation

$$\mathfrak{P}_{c_1}, \mathfrak{P}_{c_2}, \cdots, \mathfrak{P}_{c_\pi}, \qquad \pi = s_P,$$

among these ideals. All substitutions

$$(9) \qquad C = \begin{pmatrix} 1, 2, \cdots, s_P \\ c_1, c_2, \cdots, c_{s_P} \end{pmatrix}$$

thus obtained form a group simply isomorphic with the factor group, so we can suppose the factor group given in the form of this substitution group. It is well known that to every subgroup of the factor group corresponds uniquely a subgroup of G containing H.

By means of the factor group G/H we can easily determine the group G_A of an ideal $\mathfrak{A}$ having the form (6). The group H is evidently a subgroup of G_A. When, however, S is a substitution belonging to one of the co-sets HV_k in (8), this substitution produces the permutation C (9) among the prime ideals in (7). When therefore the ideal $\mathfrak{A}$ is to be invariant with respect to S, the substitution (9) corresponding to the co-set HV_k must have the form

$$(10) \qquad C = C_1 C_2,$$

where C_1 represents an intransitive substitution containing only the indices $s_1, \cdots, s_t$ and similarly C_2 a substitution containing only the remaining indices. The substitutions in the factor group G/H having the form (8) obviously form an intransitive subgroup of G/H and the corresponding subgroup in G must be the group G_A. So we have the following theorem:

THEOREM 5. *Let the self-conjugate group H be the greatest common subgroup of all the groups G_{P_i} corresponding to the different prime ideals $\mathfrak{P}_i$ in p, and* *let G/H denote the factor group of G corresponding to H. Then the group of an ideal*

$$\mathfrak{A} = \mathfrak{P}_{s_1} \cdots \mathfrak{P}_{s_t},$$

where all factors are different conjugate prime ideals, is the subgroup of G which corresponds to the intransitive subgroup G_A' of G/H permuting only the indices $s_1, \cdots, s_t$ inter se and correspondingly permuting the remaining indices mutually.

2. **The corresponding fields.** To the group G_A of an arbitrary ideal $\mathfrak{A}$ corresponds uniquely a certain subfield K_A of K. We call K_A *the subfield corresponding to* $\mathfrak{A}$, and we shall now study the arithmetical properties of this field.

We shall first prove a preliminary theorem concerning an arbitrary subfield k of K. Let $G^{(k)}$ be the subgroup of G corresponding to k. As we have already remarked in §1, all the ideals in k are invariant with respect to the substitutions of $G^{(k)}$, but we can also show the existence of ideals in K *not* contained in k having the same property, and our first problem is to determine all these ideals.

Let $\mathfrak{p}$ be a prime ideal in k containing a prime ideal $\mathfrak{P}$ in K as a factor. We can then determine the prime ideal decomposition of $\mathfrak{p}$ in K in the following way: Let G' be the greatest common subgroup of $G^{(k)}$ and the group G_P; then $G^{(k)}$ can be developed in co-sets corresponding to G',

$$G^{(k)} = G' + G'V_2 + \cdots + G'V_s,$$

and it follows easily that $\mathfrak{p}$ is divisible by s different prime ideals

$$\mathfrak{P}_1 = \mathfrak{P}, \mathfrak{P}_2, \cdots, \mathfrak{P}_s.$$

We therefore obtain

$$N_k(\mathfrak{P}) = \mathfrak{p}^{f_k} = (\mathfrak{P}_1 \cdots \mathfrak{P}_s)^r,$$

where N_k indicates the norm in k, f_k is the relative degree of $\mathfrak{P}$, and r the order of the group G'. Consequently we have the prime ideal decomposition*

$$\mathfrak{p} = (\mathfrak{P}_1 \cdots \mathfrak{P}_s)^{e'}, \quad e' = \frac{r}{f_k} \tag{11}$$

where the exponent e' necessarily is a divisor of N, r being the order of a subgroup of G.

If now $\mathfrak{A}$ is an ideal in K, which is invariant with respect to the group $G^{(k)}$, and we suppose $\mathfrak{A}$ to be divisible by exactly $\mathfrak{P}^\lambda$, then $\mathfrak{A}$ obviously must

* See, for example, H. Weber, *Lehrbuch der Algebra*, vol. II, on relative fields.

contain all the prime ideals $\mathfrak{P}_i$ dividing $\mathfrak{p}$ in (11) to the same power $\mathfrak{P}_i^\lambda$. Hence we can write

$$\mathfrak{A} = (\mathfrak{P}_1 \cdots \mathfrak{P}_s)^\lambda \mathfrak{B},$$

where the ideal $\mathfrak{B}$ is also invariant with respect to $G^{(k)}$, but relatively prime to $\mathfrak{p}$. By reasoning in the same way on $\mathfrak{B}$ we finally conclude that every invariant ideal can be written as a product

$$\mathfrak{A} = \prod_{\mathfrak{p}} (\mathfrak{P}_1 \cdots \mathfrak{P}_s)^\lambda \tag{12}$$

corresponding to the different prime ideals $\mathfrak{p}$ in k having common factors with $\mathfrak{A}$. Conversely, if $\mathfrak{A}$ has the form (12), it is evident that the ideal is invariant with respect to $G^{(k)}$.

The necessary and sufficient condition for an invariant ideal can also be expressed in another way. In (11) the exponent e' is a divisor of N. When we therefore form the Nth power of $\mathfrak{A}$, we see from (12) that every term

$$(\mathfrak{P}_1 \cdots \mathfrak{P}_s)^{\lambda N}$$

is equal to a certain power of the corresponding prime ideal $\mathfrak{p}$ in k, so that the ideal $\mathfrak{A}^N$ is an ideal in k.

Theorem 6. *The necessary and sufficient condition that an ideal $\mathfrak{A}$ be invariant with respect to a group $G^{(k)}$, is that there exist an exponent n such that $\mathfrak{A}^n$ is an ideal in the corresponding subfield k.*

As a corollary we see that when an ideal $\mathfrak{A}$ is invariant relative to all substitutions of the complete group G, then $\mathfrak{A}^N = [a]$ is a rational principal ideal.*

We remark that when $\mathfrak{A}$ is invariant with respect to the substitutions of the group $G^{(k)}$, then $\mathfrak{A}$ is also invariant relative to all subgroups of $G^{(k)}$, and correspondingly it is evident that the ideal $\mathfrak{A}^N$ must be an ideal in all fields having k as a subfield.

Let now K_A be the subfield of K corresponding to the group G_A. Then $\mathfrak{A}$ is evidently an invariant ideal of G_A and by Theorem 6 it therefore follows that an exponent n exists such that $\mathfrak{A}^n$ is an ideal in K_A. But by definition G_A is the greatest subgroup of G for which $\mathfrak{A}$ is invariant, and consequently K_A is the field of lowest degree which contains a power of $\mathfrak{A}$.

Theorem 7. *The field K_A corresponding to an arbitrary ideal $\mathfrak{A}$ is the subfield of lowest degree for which there exists an exponent n such that $\mathfrak{A}^n$ is an ideal*

* D. Hilbert, *Über die Zerlegung der Ideale eines Zahlenkörpers in Primideale*, Mathematische Annalen, vol. 44 (1894), p. 1.

contained in the field. Every field that contains a power of $\mathfrak{A}$ *contains* K_A *as a subfield.*

As an application we suppose that $\mathfrak{A}=\mathfrak{P}$ is a prime ideal, and hence G_P is the "Zerlegungs" group and K_P the "Zerlegungs" field, introduced by Hilbert. In this case[*] there exists a prime ideal $\mathfrak{p}_0$ in K_P of degree $f_0=1$ and order $e_0=1$ such that

$$(13) \qquad \mathfrak{p}_0 = \mathfrak{P}^e, \quad N_P(\mathfrak{P}) = \mathfrak{p}_0^f,$$

where N_P indicates the relative norm with respect to K_P. From Theorem 7 we conclude that K_P is the field of lowest degree for which an exponent n exists such that $\mathfrak{P}^n$ is an ideal in the field; every other field k having this property contains K_P as a subfield. When n is the least exponent for which $\mathfrak{P}^n$ is an ideal in k, then obviously $\mathfrak{p}=\mathfrak{P}^n$ is a prime ideal in k. In fields not containing K_P as a subfield the prime ideal $\mathfrak{p}$ which is divisible by $\mathfrak{P}$ must also contain some of the conjugates of $\mathfrak{P}$.

THEOREM 8. *The "Zerlegungs" field K_P is the field of lowest degree for which there exists an exponent n such that $\mathfrak{P}^n=\mathfrak{p}$ is a prime ideal in the field. Every other field having this property contains K_P as a subfield, and in a field not containing K_P the prime ideal $\mathfrak{p}$ divisible by $\mathfrak{P}$ must also be divisible by other prime ideals.*

3. The rational congruence-field of an ideal. The "Zerlegungs" field K_P has also another very important property. As we have already mentioned, the ideal $\mathfrak{p}_0$ in (13) is of first degree and first order. Hence, if ω_P is an arbitrary number in K_P, we have

$$\omega_P \equiv a \qquad (\text{mod } \mathfrak{p}_0),$$

where a is rational, and, because the prime p contains exactly the first power of $\mathfrak{p}_0$, it follows that a congruence

$$(14) \qquad \omega_P \equiv a \qquad (\text{mod } \mathfrak{p}_0^{\alpha})$$

also holds for all α, where the rational number a obviously depends on α. From (14) and (13) we therefore derive

THEOREM 9. *When ω_P is an arbitrary number in the "Zerlegungs" field K_P, then a congruence*

$$\omega_P \equiv a \qquad (\text{mod } \mathfrak{P}^{\alpha}).$$

holds for all α, where a is a rational number.

[*] See, for example, D. Hilbert, *Bericht über die Theorie der algebraischen Zahlen*, Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 4 (1894–95), §4.

We say that the field K_P is rational (mod $\mathfrak{p}_0^\alpha$), or also K_P is a rational congruence-field (mod $\mathfrak{p}_0^\alpha$). As a generalization of Theorem 9 we could propose to determine all subfields R_A of K, which are rational (mod $\mathfrak{A}^\alpha$), where $\mathfrak{A}$ is an arbitrary ideal in K. We denote by R_A the greatest subfield of K having this property and we see that every other rational field (mod $\mathfrak{A}^\alpha$) is a subfield of R_A. We can also suppose obviously that the ideal $\mathfrak{A}$ is the product of different prime ideals in K.

Before we examine the rational subfields of K (mod $\mathfrak{A}$), we shall give some results on an arbitrary field k, which is rational (mod $\mathfrak{A}_0^\alpha$), where

$$\mathfrak{A}_0 = \mathfrak{p}_0\mathfrak{p}_1 \cdots \mathfrak{p}_r \tag{15}$$

is an ideal in the field. Every number in k then satisfies a congruence

$$\omega \equiv a \pmod{\mathfrak{A}_0^\alpha} \tag{16}$$

and it is obvious that all the prime ideals $\mathfrak{p}_i$ in (15) must be of first degree and first order. But we can also prove that $\mathfrak{A}_0$ cannot contain two different prime ideals, for instance $\mathfrak{p}_0$ and $\mathfrak{p}_1$, dividing the same rational prime p. Because if we form the equation $f(x)=0$ satisfied by a primitive number ω in k, it follows[*] that $f(x)$ for all α has a decomposition

$$f(x) \equiv (x - a_0)(x - a_1)f_2(x) \pmod{p^\alpha},$$

where $f_2(x)$ is a rational polynomial. When the discriminant of ω_A is exactly divisible by p^δ, we obtain

$$\omega - a_0 \equiv 0 \pmod{\mathfrak{p}_0^{\alpha-\delta}}$$

and at the same time

$$\omega - a_0 \not\equiv 0 \pmod{\mathfrak{p}_1^\delta},$$

so that a congruence (16) cannot hold for all α if $\mathfrak{A}_0$ also contains $\mathfrak{p}_1$. We have therefore proved

THEOREM 10. *If the field k is rational* (mod $\mathfrak{A}_0^\alpha$), *where the ideal $\mathfrak{A}_0$ in k has the form* (15), *then every prime ideal divisor of $\mathfrak{A}_0$ is of first degree and first order, and $\mathfrak{A}_0$ cannot contain more than one prime ideal dividing the same prime p.*

A consequence of this theorem is that every field which is rational with respect to all its ideals is necessarily the rational field R, because every prime

[*] I refer to my paper *Über den Zusammenhang zwischen den definierenden Gleichungen und der Idealtheorie in algebraischen Körpern* (erste Mitteilung), Mathematische Annalen, vol. 96 (1926), Chap. II, §2.

p must be a prime ideal of the field, and the discriminant is therefore equal to 1, and by a theorem of Minkowski R is the only field having this property.

When $\mathfrak{A}_0$ has the form (15), k must be rational (mod $\mathfrak{p}_i^\alpha$) for $i=1, 2, \cdots, r$; but conversely we can conclude, that if k is rational (mod $\mathfrak{p}_i^\alpha$) for $i=1, 2, \cdots, r$, then k must be rational (mod $\mathfrak{A}_0^\alpha$). When namely $\mathfrak{p}_i$ divides the rational prime p_i, the numbers

$$0,1, \cdots, p_i^\alpha-1$$

form a complete system of incongruent numbers (mod $\mathfrak{p}_i^\alpha$), and when we put

$$M_i = \frac{(p_1 \cdots p_r)^\alpha}{p_i^\alpha}$$

the rational numbers

$$\sum_{i=1}^{r} M_i a_i \qquad (a_i = 0,1, \cdots, p_i^\alpha - 1)$$

form a complete system of incongruent numbers (mod $\mathfrak{A}_0^\alpha$). It therefore follows conversely, that when an ideal $\mathfrak{A}_0$ satisfies the conditions of Theorem 10, then the field k is necessarily rational (mod $\mathfrak{A}_0^\alpha$).

After these general remarks we return to the problem of the determination of all subfields of K that are rational (mod $\mathfrak{A}^\alpha$), where $\mathfrak{A}$ is an ideal in K. We first suppose that $\mathfrak{A}$ only contains prime ideals dividing a single prime p, so that $\mathfrak{A}$ has the form

$$\mathfrak{A} = \mathfrak{P}_1 \cdots \mathfrak{P}_t. \tag{17}$$

From Theorem 10 we conclude that in the corresponding field R_A there exists a prime ideal $\mathfrak{p}_0$ of first order and first degree containing $\mathfrak{A}$. The field R_A is obviously a subfield of all the "Zerlegungs" fields of the prime ideals $\mathfrak{P}_i$ in $\mathfrak{A}$, and consequently is also contained in their greatest common subfield. But R_A is generally not equal to this field, as the prime ideals $\mathfrak{P}_i$ can be divisors of two different prime ideals of this field.

We shall now determine the field R_A by means of the corresponding group G'. The group G' must contain the "Zerlegungs" groups G_{P_i} of all divisors $\mathfrak{P}_i$ of $\mathfrak{A}$, and conversely we see that every group G' containing all G_{P_i} corresponds to a field, where the prime ideals $\mathfrak{P}_i$ all divide prime ideals of first order and first degree.

When now in particular G_P is the "Zerlegungs" group of $\mathfrak{P}=\mathfrak{P}_1$ and

$$V_2, V_3, \cdots, V_t$$

a system of substitutions in G such that in general V_i transforms $\mathfrak{P}$ into $\mathfrak{P}_i$, we can prove

THEOREM 11. *The group G' of the field R_A is the least subgroup of G containing the system*

$$G_P + G_P V_2 + \cdots + G_P V_t$$

of co-sets in G.

It is obvious that G' contains all the groups G_{P_i} $(i=1, 2, \cdots, t)$ and in the corresponding field all $\mathfrak{P}_i$ must therefore divide prime ideals of first order and first degree, and this prime ideal $\mathfrak{p}_0$ must be the same for all $\mathfrak{P}_i$, because if $\mathfrak{p}_0$ contains $\mathfrak{P}$ it follows by application of substitutions in G' that $\mathfrak{p}_0$ is divisible by all $\mathfrak{P}_i$ $(i=1, 2, \cdots, t)$.

When, more generally, $\mathfrak{A}$ contains prime ideals dividing different primes, we can write

$$\mathfrak{A} = \mathfrak{A}_1 \mathfrak{A}_2 \cdots,$$

where every factor $\mathfrak{A}_i$ has the form (17). From a former remark it then follows that the corresponding rational field R_A (mod $\mathfrak{A}^\alpha$) is the greatest common subfield of all the fields R_{A_i} $(i=1, 2, \cdots)$.

4. **The inertial group.** I also mention finally that in the same way that we generalized the "Zerlegungs" group of Hilbert we can also obtain an *inertial* group (Trägheitsgruppe) for an arbitrary ideal $\mathfrak{A}$. The inertial group T_A consists of all substitutions T having the property that

$$T:\omega \equiv \omega \qquad (\text{mod } \mathfrak{A})$$

for every number ω in K.

It is obvious that the group T_A so defined is a subgroup of G_A. The construction of the general group T_A is simple. We obtain the following from the definition of T_A: The inertial group of a composite ideal $\mathfrak{A}$ is equal to the greatest common subgroup of the different prime ideal powers $\mathfrak{P}^a$ dividing $\mathfrak{A}$.

When $\mathfrak{A} = \mathfrak{P}$ is a prime ideal, the group T_P is the "Trägheits" group of Hilbert. When $\mathfrak{A} = \mathfrak{P}^a$, $a>1$, Hilbert introduced the notation "Verzweigungs" group (einmal, zweimal etc. überstrichene). It may perhaps be more natural and simpler to use the general conception of the inertial groups and so totally avoid the term "Verzweigungsgruppe."

There are obviously only a finite number of ideals for which T_A contains substitutions different from the identical substitution.

YALE UNIVERSITY,
NEW HAVEN, CONN.