ON THE FIELD OF ORIGIN OF AN IDEAL

H. B. MANN

IN this paper we shall consider integral ideals in finite algebraic extensions ($\mathfrak{F}$, $\mathfrak{F}_1, \ldots$) of the field of rational numbers.

Two ideals $\mathfrak{a}$, $\mathfrak{b}$ in the same field $\mathfrak{F}$ are said to be equal if and only if they contain the same numbers.

Let $\mathfrak{F}_1 \supset \mathfrak{F}_2$ and let $\mathfrak{A}$ be an ideal in $\mathfrak{F}_2$. The numbers of $\mathfrak{A}$ generate an ideal $\mathfrak{a}$ in $\mathfrak{F}_1$ and it is known that the intersection $\mathfrak{a} \cap \mathfrak{F}_2 = \mathfrak{A}$. (See for instance Hecke, *Theorie der algebraischen Zahlen*, § 37). Also if $\mathfrak{a} \subset \mathfrak{F}_1$ and $\mathfrak{b} \subset \mathfrak{F}_2$ generate the same ideal in a field containing $\mathfrak{F}_1$ and $\mathfrak{F}_2$ then they must generate the same ideal in $\mathfrak{F}_1 \cup \mathfrak{F}_2$ and thus in every field containing $\mathfrak{F}_1$ and $\mathfrak{F}_2$.

We shall therefore call two ideals $\mathfrak{a}$ and $\mathfrak{b}$ equal if they generate the same ideal in a field containing all the numbers of $\mathfrak{a}$ and of $\mathfrak{b}$. Two such ideals may therefore be denoted by the same symbol and we shall speak of an ideal $\mathfrak{a}$ without regard to a particular field. An ideal $\mathfrak{a}$ will be said to be contained in a field $\mathfrak{F}$ if it may be generated by numbers in $\mathfrak{F}$; in other words, if it has a basis in $\mathfrak{F}$.

It seems natural to try to characterize those fields which contain a given ideal $\mathfrak{a}$, and in this paper we shall find such a characterization at least in the case that a power of $\mathfrak{a}$ is a prime ideal in some extension of $\mathfrak{F}$.

A necessary and sufficient condition for an ideal $\mathfrak{a}$ to be contained in a given field $\mathfrak{F}$ will be derived in the case that $\mathfrak{a}$ is an ideal of order 1, as defined in this paper. For prime ideals of order greater than 1 a necessary and sufficient condition will also be given.

From now on we shall consider finite algebraic extensions ($\mathfrak{F}_1, \ldots$) over a field $\mathfrak{F}_1$ itself a finite algebraic extension over the field of rational numbers. Admissible subfields of $\mathfrak{F}_1$ are those containing $\mathfrak{F}$. Throughout the paper only fields containing $\mathfrak{F}$ will be considered.

Consider an ideal $\mathfrak{a} \subset \mathfrak{F}_1$. Either $\mathfrak{a}$ is not contained in any admissible subfield of $\mathfrak{F}_1$ or $\mathfrak{F}_1$ must contain an admissible subfield $\mathfrak{F}_2$ which has the property that $\mathfrak{a}$ is in $\mathfrak{F}_2$ but not in any admissible subfield of $\mathfrak{F}_2$. We therefore define:

DEFINITION 1. *If $\mathfrak{a}$ is in $\mathfrak{F}_1$ but not in any proper admissible subfield of $\mathfrak{F}_1$ then $\mathfrak{a}$ is said to originate in $\mathfrak{F}_1$ over $\mathfrak{F}$.*

Consider $\mathfrak{F}_1 \supset \mathfrak{F}_2$ and let $\mathfrak{a}$ be an ideal in $\mathfrak{F}_1$. The numbers of $\mathfrak{a}$ which lie in $\mathfrak{F}_2$ form an ideal $\mathfrak{A}$ in $\mathfrak{F}_2$. This ideal $\mathfrak{A}$ is said to correspond in $\mathfrak{F}_2$ to the ideal $\mathfrak{a}$. The ideal $\mathfrak{A}$ depends only on $\mathfrak{a}$ but not on $\mathfrak{F}_1$.

DEFINITION 2. If $\mathfrak{A} \subset \mathfrak{F}$ *corresponds to* $\mathfrak{a}$ *in* $\mathfrak{F}_1$ *and*

$$\mathfrak{A} = \mathfrak{a}^e \mathfrak{c}, \quad (\mathfrak{a}, \mathfrak{c}) = 1 \tag{1}$$

then $\mathfrak{a}$ is said to be of order e with respect to $\mathfrak{F}$.

Received September 1, 1948.

REMARK. Not every ideal has an order with respect to $\mathfrak{F}$; however, every ideal which is a prime ideal in some extension of $\mathfrak{F}$ does.

THEOREM 1. *If* $\mathfrak{a}$ *is an ideal of order* 1 *with respect to* $\mathfrak{F}$ *then* $\mathfrak{a}$ *originates in a unique subfield* $\mathfrak{F}_1$ *over* $\mathfrak{F}$. *An extension* $\mathfrak{F}' \supset \mathfrak{F}$ *contains* $\mathfrak{a}$ *if and only if it contains* $\mathfrak{F}_1$.

Proof. If $\mathfrak{a}$ does not originate in $\mathfrak{F}'$, then it must originate in some subfield of $\mathfrak{F}'$. Hence $\mathfrak{a}$ originates in at least one field.

Suppose then that $\mathfrak{a}$ originates in $\mathfrak{F}_1$ and also in $\mathfrak{F}_2$. Let $\mathfrak{F}_n$ be a normal extension of $\mathfrak{F}$ containing $\mathfrak{F}_1$ and $\mathfrak{F}_2$ and $\mathfrak{G}$ the Galois group of $\mathfrak{F}_n$ over $\mathfrak{F}$. Let $\mathfrak{H}_1$ and $\mathfrak{H}_2$ be the subgroups of $\mathfrak{G}$ leaving $\mathfrak{F}_1$ and $\mathfrak{F}_2$ respectively fixed. Since $\mathfrak{a}$ has a basis in $\mathfrak{F}_1$ and in $\mathfrak{F}_2$ it follows that $\mathfrak{a}$ is transformed into itself by the union $\mathfrak{H}_1 \cup \mathfrak{H}_2 = \bar{\mathfrak{H}}$. To $\bar{\mathfrak{H}}$ corresponds the field $\bar{\mathfrak{F}} = \mathfrak{F}_1 \cap \mathfrak{F}_2$ which certainly contains $\mathfrak{F}$. Let $\bar{\mathfrak{a}} \subset \bar{\mathfrak{F}}$ and $\mathfrak{A} \subset \mathfrak{F}$ correspond to $\mathfrak{a} \subset \mathfrak{F}_1$ then

$$
\begin{aligned}
\bar{\mathfrak{a}} &= \mathfrak{a}\mathfrak{c}' \\
\mathfrak{A} &= \bar{\mathfrak{a}}\mathfrak{d} = \mathfrak{a}\mathfrak{c}'\mathfrak{d}.
\end{aligned} \tag{2}
$$

Since $\mathfrak{c}'\mathfrak{d} = \mathfrak{c}$ by (1) and since $(\mathfrak{c}, \mathfrak{a}) = 1$ by hypothesis we must have

$$(\mathfrak{c}', \mathfrak{a}) = 1. \tag{3}$$

If

$$\bar{\mathfrak{H}} = \mathfrak{H}_1 + \mathfrak{H}_1 A_2 + \ldots + \mathfrak{H}_1 A_g \tag{4}$$

then all relative conjugate fields of $\mathfrak{F}_1$ over $\bar{\mathfrak{F}}$ are obtained each once by applying $1, A_2, \ldots, A_g$ to $\mathfrak{F}_1$. Hence since A_i transforms $\mathfrak{a}$ into itself

$$\mathfrak{a} = \mathfrak{a}^{A_2} = \ldots = \mathfrak{a}^{A_g}. \tag{5}$$

Thus

$$
\begin{aligned}
\bar{\mathfrak{a}} &= \mathfrak{a}\mathfrak{c}'^{A_i} \qquad (i = 1, \ldots, g), \\
\mathfrak{c}'^{A_i} &= \mathfrak{c}'.
\end{aligned} \tag{6}
$$

Thus

$$\mathfrak{a}^g \subset \bar{\mathfrak{F}}, \ \mathfrak{c}'^g \subset \bar{\mathfrak{F}}. \tag{7}$$

Since $\mathfrak{a}^g \subset \bar{\mathfrak{F}}$, we must have $\mathfrak{a}^g \subset \bar{\mathfrak{a}}$ and

$$\mathfrak{a}^g = \bar{\mathfrak{a}}\mathfrak{d}' = \mathfrak{a}\mathfrak{c}'\mathfrak{d}'. \tag{8}$$

Hence $\mathfrak{c}' = (1)$ since otherwise $(\mathfrak{a}, \mathfrak{c}') \neq 1$ contradicting (3). Thus by (2) $\mathfrak{a} = \bar{\mathfrak{a}}$ and since by hypothesis $\mathfrak{a}$ originates in $\mathfrak{F}_1$ and $\mathfrak{F}_2$ it follows that $\bar{\mathfrak{F}} = \mathfrak{F}_1 = \mathfrak{F}_2$.

If now $\mathfrak{a}$ is in $\mathfrak{F}'$ then $\mathfrak{F}'$ must contain a field in which $\mathfrak{a}$ originates. Hence $\mathfrak{F}'$ must contain $\mathfrak{F}_1$. Conversely if $\mathfrak{F}' \supset \mathfrak{F}_1$ then $\mathfrak{F}' \supset \mathfrak{a}$ since $\mathfrak{a} \subset \mathfrak{F}_1$.

THEOREM 2. *If* $\mathfrak{p}$ *is an ideal in any field over* $\mathfrak{F}$ *and g is the largest integer for which* $\mathfrak{p}^g$ *is a prime ideal in some extension of* $\mathfrak{F}$ *then* $\mathfrak{p}^g$ *originates in a unique extension* $\mathfrak{F}' \supset \mathfrak{F}$ *and is a prime ideal in* $\mathfrak{F}'$. *Moreover every field that contains a power of* $\mathfrak{p}$ *contains* $\mathfrak{F}'$.

Proof. Let $\mathfrak{P}$ in $\mathfrak{F}$ correspond to $\mathfrak{p}$. Since $\mathfrak{p}^g$ is a prime ideal in some field over $\mathfrak{F}$, $\mathfrak{P}$ must be a prime ideal. That is to say

$$\mathfrak{P} = \mathfrak{p}^e\mathfrak{a}, \quad (\mathfrak{p}, \mathfrak{a}) = 1. \tag{9}$$

https://doi.org/10.4153/CJM-1950-002-3 Published online by Cambridge University Press

Thus $\mathfrak{p}^e$ satisfies the conditions of Theorem 1. Let $\mathfrak{F}'$ be the unique field in which $\mathfrak{p}^e$ originates. Let $\mathfrak{p}^g$ be a prime ideal in $\mathfrak{F}''$. To $\mathfrak{p}^g$ corresponds a prime ideal in $\mathfrak{F}$ and since this prime ideal has a common factor with $\mathfrak{P}$ it must be equal to $\mathfrak{P}$. Thus since $(\mathfrak{p}, \mathfrak{a}) = 1$

$$\mathfrak{P} = (\mathfrak{p}^g)^t\mathfrak{a}, \quad e \equiv 0(g), \ (\mathfrak{p}^g, \mathfrak{a}) = 1. \tag{10}$$

Thus $\mathfrak{F}''$ contains $\mathfrak{p}^e$ hence must also contain $\mathfrak{F}'$. Moreover $\mathfrak{p}^g$ is a prime ideal in $\mathfrak{F}'$ since it is prime in $\mathfrak{F}''$ and since g is the largest power of $\mathfrak{p}$ which is prime in any field. Every field that contains a power of $\mathfrak{p}$ must contain $\mathfrak{p}^e$ hence must contain $\mathfrak{F}'$. In particular $\mathfrak{p}^g$ cannot be contained in any subfield of $\mathfrak{F}'$ and therefore originates in $\mathfrak{F}'$.

COROLLARY. *If $\mathfrak{p}$ is an ideal in some extension $\mathfrak{F}'$ of $\mathfrak{F}$ and $\mathfrak{p}^g$ is the highest power of $\mathfrak{p}$ which is a prime ideal in an admissible subfield of $\mathfrak{F}'$ then $\mathfrak{p}^g$ is the highest power of $\mathfrak{p}$ which is a prime ideal in any extension of $\mathfrak{F}$. (We may take $g = 0$ if no power of $\mathfrak{p}$ is a prime ideal in any admissible subfield of $\mathfrak{F}'$.)*

A simple example is the ideal $(\sqrt{2})$, when f is the field of rational numbers. Here $g = e = 2, f = f'$.

THEOREM 3. *If $\mathfrak{p}$ is a prime ideal in some extension of $\mathfrak{F}$ and $\mathfrak{p}^g$ is the largest power of $\mathfrak{p}$ which is a prime ideal of any extension of $\mathfrak{F}$ and if $\mathfrak{p}^h$ is a prime ideal in some extension $\mathfrak{F}_1$ of $\mathfrak{F}$ then*

$$g \equiv 0(h). \tag{11}$$

Let $\mathfrak{F}'$ be the unique field in which $\mathfrak{p}^g$ originates by Theorem 2. By the same theorem we have

$$\mathfrak{F}' \subset \mathfrak{F}_1. \tag{12}$$

To $\mathfrak{p}^h$ corresponds a prime ideal in $\mathfrak{F}'$ which has a common factor with $\mathfrak{p}^g$ and therefore must equal $\mathfrak{p}^g$ since $\mathfrak{p}^g$ is a prime ideal in $\mathfrak{F}'$. Thus

$$\mathfrak{p}^g = (\mathfrak{p}^h)^t, \ g = ht. \tag{13}$$

If $\mathfrak{p}$ is a prime ideal in some extension of $\mathfrak{F}$ but no power of $\mathfrak{p}$ is a prime ideal in any extension of $\mathfrak{F}$ then by Theorem 2 there is a unique extension of $\mathfrak{F}$ in which $\mathfrak{p}$ originates over $\mathfrak{F}$. Quite in contrast to this we shall show that if $\mathfrak{p}^g$ $(g > 1)$ is a prime ideal in some extension of $\mathfrak{F}$ then there are infinitely many extensions of $\mathfrak{F}$ in which $\mathfrak{p}$ originates and is a prime ideal. We show this by proving

THEOREM 4. *If $\mathfrak{p}$ is a prime ideal in $\mathfrak{F}$ then for every $g > 1$ there exists an ideal $\mathfrak{P}$ such that $\mathfrak{P}^g = \mathfrak{p}$. The ideal $\mathfrak{P}$ originates as a prime ideal in infinitely many fields over $\mathfrak{F}$.*

Proof. Let $\mathfrak{p} = (\alpha_1, \alpha_2)$, $\alpha_1, \alpha_2 \subset \mathfrak{F}$. We may choose

$$(\alpha_2) = \mathfrak{p}\mathfrak{c}, \quad (\mathfrak{p}, \mathfrak{c}) = 1. \tag{14}$$

https://doi.org/10.4153/CJM-1950-002-3 Published online by Cambridge University Press

Choose q prime to α_1, α_2, $\mathfrak{p}$ and to the absolute differente of $\mathfrak{F}(\zeta)$, where ζ is a primitive gth root of unity, and square free. In $\mathfrak{F}(\sqrt[g]{q\alpha_2})$ the ideal $\mathfrak{p}$ is the gth power of the ideal $\mathfrak{P} = (\alpha_1, \sqrt[g]{q\alpha_2})$, for α_1 and $\sqrt[g]{q\alpha_2}$ can have only a divisor $\overline{\mathfrak{P}}$ of $\mathfrak{p}$ in common. Thus

$$\begin{aligned} \alpha_1 &= \mathfrak{p}\mathfrak{A} \\ \sqrt[g]{q\alpha_2} &= \overline{\mathfrak{P}}\mathfrak{B} \qquad (\mathfrak{p}, \mathfrak{B}) = 1 \\ q\alpha_2 &= \overline{\mathfrak{P}}^g\mathfrak{B}^g = \mathfrak{p}\mathfrak{c}q, \qquad (\mathfrak{p}, \mathfrak{c}) = 1, \qquad \overline{\mathfrak{P}}^g = \mathfrak{p}. \end{aligned}$$

Hence $\mathfrak{P}^g = (\alpha_1, \sqrt[g]{q\alpha_2})^g = \overline{\mathfrak{P}}^g = \mathfrak{p}$.

We shall show now that $\mathfrak{F}(\sqrt[g]{q\alpha_2}) \neq \mathfrak{F}(\sqrt[g]{q'\alpha_2})$ if $(q) \neq (q')$. The numbers $q\alpha_2$ and $q'\alpha_2$ are square free in $\mathfrak{F}(\zeta)$ by assumption. Hence the polynomials $x^g - q\alpha_2$, $x^g - q'\alpha_2$ are irreducible in $\mathfrak{F}(\zeta)$ by Eisenstein's criterion. Thus 1, $\sqrt[g]{q\alpha_2}, \ldots, (\sqrt[g]{q\alpha_2})^{g-1}$ are independent over $\mathfrak{F}(\zeta)$. If $\sqrt[g]{q'\alpha_2} \subset \mathfrak{F}(\sqrt[g]{q\alpha_2})$ then

$$\sqrt[g]{q'\alpha_2} = a_0 + a_1\sqrt[g]{q\alpha_2} + \ldots + a_{g-1}(\sqrt[g]{q\alpha_2})^{g-1}$$

applying the automorphism $\sqrt[g]{q\alpha_2} \leftrightarrow \zeta\sqrt[g]{q\alpha_2}$ we get

$$\begin{aligned} \zeta^i\sqrt[g]{q'\alpha_2} &= a_0 + a_1\zeta\sqrt[g]{q\alpha_2} + \ldots + a_{g-1}\zeta^{g-1}(\sqrt[g]{q\alpha_2})^{g-1} \\ &= \zeta^i(a_0 + a_1\sqrt[g]{q\alpha_2} + \ldots + a_{g-1}(\sqrt[g]{q\alpha_2})^{g-1}). \end{aligned}$$

Because of the independence of 1, $\sqrt[g]{q\alpha_2}, \ldots, (\sqrt[g]{q\alpha_2})^{g-1}$ over $\mathfrak{F}(\zeta)$ we must have

$$\zeta^i a_j = \zeta^j a_j,\ a_j = 0 \text{ for } j \neq \text{i}.$$

Hence

$$\begin{aligned} \sqrt[g]{q'\alpha_2} &= a_i(\sqrt[g]{q\alpha_2})^i \\ q'\alpha_2 &= a_i^g(q\alpha_2)^i. \end{aligned}$$

Our choice of q and q', together with equation 14, imply that $i = 1$ and a_i must be a unit. Hence $(q) = (q')$.

Clearly we can choose infinitely many (q) which are square free and prime to α_1, α_2, $\mathfrak{p}$ and the absolute differente of $\mathfrak{F}(\zeta)$. For instance all but a finite number of rational primes fulfill this condition.

The ideal $(\alpha_1, \sqrt[g]{q\alpha_2})$ is moreover a prime ideal since it lies in a field of degree g over $\mathfrak{F}$ and its gth power is a prime ideal in $\mathfrak{F}$. For the same reason it also originates in $\mathfrak{F}$ since it cannot lie in any field of degree less than g over $\mathfrak{F}$.

Theorem 4 shows among other things: If $\mathfrak{p}^h$, $h > 1$, is a prime ideal in $\mathfrak{F}'$ over $\mathfrak{F}$ then $\mathfrak{p}$ originates in infinitely many fields over $\mathfrak{F}$. For let $\mathfrak{p}^g$ be the highest power of $\mathfrak{p}$ which is a prime ideal in some extension of $\mathfrak{F}$. Let $\mathfrak{F}''$ be the unique field over $\mathfrak{F}$ in which $\mathfrak{p}^g$ originates and let $\mathfrak{p}$ originate in some field $\mathfrak{F}_1$ over $\mathfrak{F}''$. By Theorem 4 there are infinitely many such fields. We must show that $\mathfrak{p}$ originates in $\mathfrak{F}_1$ over $\mathfrak{F}$. If $\mathfrak{p}$ lies in $\mathfrak{F}_2$ over $\mathfrak{F}$ where $\mathfrak{F}_1 \supseteq \mathfrak{F}_2$, then $\mathfrak{F}_2 \supseteq \mathfrak{F}''$ by Theorem 2 and hence $\mathfrak{F}_1 = \mathfrak{F}_2$ since $\mathfrak{p}$ originates in $\mathfrak{F}_1$ over $\mathfrak{F}''$. Thus $\mathfrak{p}$ also originates in $\mathfrak{F}_1$ over $\mathfrak{F}$.

https://doi.org/10.4153/CJM-1950-002-3 Published online by Cambridge University Press

Theorem 2 characterizes completely the fields over $\mathfrak{F}$ which contain a given prime ideal $\mathfrak{p}$ if no power of $\mathfrak{p}$ is a prime ideal in a field over $\mathfrak{F}$. However in the case that some $\mathfrak{p}^h$ $(h > 1)$ is a prime ideal in a field over $\mathfrak{F}$ we obtain only the necessary condition that every field containing $\mathfrak{p}$ must contain the field in which $\mathfrak{p}^g$ originates where $\mathfrak{p}^g$ is defined in Theorem 2. A stronger necessary but still not sufficient condition is as follows:

THEOREM 5. *If $\mathfrak{p}$ originates in $\mathfrak{F}'$ over $\mathfrak{F}$, $\mathfrak{p}^g = \mathfrak{P}$ is the highest power of $\mathfrak{p}$ which is a prime ideal in some subfield of $\mathfrak{F}'$ and if $\mathfrak{p}^g$ originates in $\mathfrak{F}''$ then $\mathfrak{F}' = \mathfrak{F}''(\alpha)$, where α satisfies an irreducible equation*

$$x^m + a_1x^{m-1} + \ldots + a_m = 0 \tag{13}$$

of degree $m = gr$ (r integral) with coefficients in $\mathfrak{F}''$ such that

$$a_{lg+k} \equiv 0(\mathfrak{P}^{l+1}), \ \ k > 0, \tag{14}$$
$$a_{rg} \not\equiv 0(\mathfrak{P}^{r+1}).$$

Proof. From Theorem 2 we have $\mathfrak{F}'' \subset \mathfrak{F}'$. Let $\alpha \subset \mathfrak{p}$, α non $\subset \mathfrak{p}^2$, $\alpha \subset \mathfrak{F}'$. Since $\mathfrak{p}$ originates in $\mathfrak{F}'$ and since in every field between $\mathfrak{F}''$ and $\mathfrak{F}'$ the ideal $\mathfrak{p}$ corresponds to a power of $\mathfrak{p}$ we must have $\mathfrak{F}' = \mathfrak{F}''(\alpha)$. Let $(\mathfrak{F}'/\mathfrak{F}'') = m$ and observe that the conjugates of α over $\mathfrak{F}''$ are all exactly divisible by $\mathfrak{p}$. Hence the $(lg + k)$th, $(k > 0)$, symmetric function of these conjugates is divisible by $\mathfrak{p}^{lg+k}$ and since it is in $\mathfrak{F}''$ it must be divisible by $\mathfrak{P}^{l+1}$. Moreover the last coefficient is exactly divisible by $\mathfrak{p}^m$. If $\mathfrak{p} = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_s^{e_s}$ is the prime decomposition of $\mathfrak{p}$ in $\mathfrak{F}'$ and f_i the degree of $\mathfrak{p}_i$ then $\mathfrak{p}_i$ is of multiplicity ge_i with respect to $\mathfrak{P}$ and hence

$$m = ge_1f_1 + \ldots + ge_sf_s = gr \qquad (r \text{ integral}). \tag{15}$$

This proves Theorem 5.

THEOREM 6. *Let $\mathfrak{p}^g = \mathfrak{P}$ and let g and $\mathfrak{F}''$ be defined as in Theorem 5. The ideal $\mathfrak{p}$ lies in $\mathfrak{F}'$ over $\mathfrak{F}$ if and only if $\mathfrak{F}' \supset \alpha$ where $\alpha^g = \beta$ satisfies an irreducible equation*

$$\beta^r + a_1\beta^{r-1} + \ldots + a_r = 0, \ a_i \equiv 0(\mathfrak{P}^i), \ a_r \not\equiv 0(\mathfrak{P}^{r+1}), \text{ over } \mathfrak{F}''. \tag{16}$$

First let $\mathfrak{p}$ lie in $\mathfrak{F}'$, then there exists in $\mathfrak{F}'$ an α such that $\alpha \equiv 0(\mathfrak{p})$, $\alpha \not\equiv 0(\mathfrak{p}^2)$. By Theorem 2 we have $\alpha \subset \mathfrak{F}' \subset \mathfrak{F}''$. Clearly $\alpha^g = \beta$ and all its conjugates over $\mathfrak{F}''$ are exactly divisible by $\mathfrak{P}$ and the necessity of the condition 16 follows.

On the other hand consider $\mathfrak{F}''(\alpha)$ where $\alpha^g = \beta$ satisfies an irreducible equation 16. Let γ be a number with ideal denominator $\mathfrak{P}$. Then $\gamma\beta$ satisfies an equation

$$(\gamma\beta)^r + \gamma a_1(\gamma\beta)^{r-1} + \ldots + \gamma^r a_r = 0 \tag{17}$$

with integral coefficients. Hence $\beta \equiv 0(\mathfrak{P})$. Moreover since $a_r \not\equiv 0(\mathfrak{P}^{r+1})$ it follows that $\beta = \mathfrak{P}\mathfrak{b}$, $(\mathfrak{P}, \mathfrak{b}) = 1$. Consider the ideal $(\alpha, \mathfrak{P})$. If

$$\mathfrak{P} = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_s^{e_s} \tag{18}$$
$$\alpha = \mathfrak{P}_1^{h_1} \ldots \mathfrak{P}_s^{h_s}\mathfrak{c}, \qquad (\mathfrak{p}_1, \mathfrak{c}) = 1$$

it follows that $e_i = gh_i$. Hence $(\alpha, \mathfrak{P})^g = \mathfrak{P}$.

https://doi.org/10.4153/CJM-1950-002-3 Published online by Cambridge University Press

Thus $\mathfrak{F}''(\alpha)$ contains $\mathfrak{p}$ and so does every field over $\mathfrak{F}''(\alpha)$.

Suppose an ideal $\mathfrak{p}$ a power of which is a prime ideal in some field over $\mathfrak{F}$ is given in any field $\mathfrak{F}_1$ over $\mathfrak{F}$ and we are required to find all extensions of $\mathfrak{F}$ which contain $\mathfrak{p}$. We proceed as follows. We first find the largest power say $\mathfrak{p}^g = \mathfrak{P}$ of $\mathfrak{p}$ which is a prime ideal in any admissible subfield of $\mathfrak{F}_1$. Next we determine the smallest admissible subfield containing $\mathfrak{P}$. Let this field be $\mathfrak{F}''$. We then obtain all fields which contain $\mathfrak{p}$ as all extensions of all $\mathfrak{F}''(\alpha)$ where α^g satisfies an equation of the form 16.

Ohio State University

https://doi.org/10.4153/CJM-1950-002-3 Published online by Cambridge University Press