THE MEANING OF THE FORM CALCULUS IN CLASSICAL IDEAL THEORY

BY
HARLEY FLANDERS

1. **Introduction.** One of the interesting tools in algebraic number theory is the Gauss-Kronecker theorem on the content of a product of forms. This result is used in various ways. For example the fact that the unique factorization of ideals carries over to finite algebraic extensions was, in the past, proved using this tool [3]. Modern proofs not using the form theory have been constructed from several points of view, we refer to [2; 6; 7; 9]. Actually, in his *Grundzüge* [5], Kronecker gave a development of the arithmetic of number fields (and more general domains) in which the form theory plays the central role, while the ideal theory of Dedekind is very much in the shadows. This is not taken very seriously in our time, however Weyl [8] cast this development of Kronecker into a version more accessible to the modern reader. Finally, the Kronecker theorem on forms is useful in showing that the most natural definition of the norm of an ideal, norm equals the product of conjugates, always yields an ideal in the ground field.

In many situations it is extremely convenient, indeed almost imperative, to have a principal ideal ring instead of a Dedekind ring. The usual modern device for passing to this technically vastly simpler situation is to localize either by passing to p-adic completions or by forming the quotient ring with respect to the complement of a finite set of prime ideals. The form theory has not generally been looked upon as a tool for accomplishing this reduction to principal ideals, none-the-less, this is precisely what it accomplishes; and this is what we propose to discuss here. In a certain sense it accomplishes the task much better than does localization because with localization the bulk of the structure of the ideal group is lost, whereas with forms this structure is preserved down to the finest detail.

What we shall do is simply gather together several more or less known facts and interpret them in terms of the ideal theory of rational function fields related to the given Dedekind domain. The full Kronecker theory does indeed apply to more general domains, whose applications are, however, somewhat problematical, and so we shall limit ourselves to the Dedekind domains(1).

Received by the editors April 24, 1959.

(1) After this paper was prepared, it was brought to the author's attention by Professor Zassenhaus that similar considerations were discussed in Professor Artin's lectures some years ago.

2. **Preliminaries.** In this section we simply state most of the known things we shall deal with and settle on a notation.

Let $\mathfrak{o}$ be an integral domain with classical (Dedekind) ideal theory. This means that each ideal $\mathfrak{a}$ is a unique product $\mathfrak{a}=\mathfrak{p}_1\mathfrak{p}_2\cdots$ of prime ideals. If $k=Q(\mathfrak{o})$ is the quotient field of $\mathfrak{o}$, it also means that the fractional ideals of k w.r.t. $\mathfrak{o}$ form a group. This entails the ascending chain condition so that each fractional ideal is finitely generated. If $f(x)\in k[x]$, $(x)=(x_1, x_2, \cdots)$, is a polynomial with coefficients $a_1, a_2, \cdots$, the content of f is the ideal.

$$\mathrm{Ct}\,(f) = (a_1, a_2, \cdots)$$

generated by these coefficients. The Kronecker theorem then asserts that $f\to\mathrm{Ct}\,(f)$ is multiplicative:

$$\mathrm{Ct}\,(fg) = (\mathrm{Ct}\,f)(\mathrm{Ct}\,g).$$

Because of this the content of a rational function can be defined by

$$\mathrm{Ct}\,(f/g) = (\mathrm{Ct}\,f)(\mathrm{Ct}\,g)^{-1}.$$

Now let K be a finite extension of k and let $\mathfrak{O}$ be the ring of elements of K integral over $\mathfrak{o}$. Then each element of K is the quotient of an element of $\mathfrak{O}$ over an element of $\mathfrak{o}$ and, more serious, the ring $\mathfrak{O}$ has classical ideal theory. If $(x)=(x_1, x_2, \cdots)$ is a set of independent variables, the algebraic structure of the extension $K(x)/k(x)$ mimics that of K/k, in particular $[K(x): k(x)] = [K: k]$, and the restriction of the norm function $N_{K(x)/k(x)}$ to K is precisely $N_{K/k}$. The same holds for the trace and for the field (characteristic) equation of an element. In view of this we may shorten the notation by using $N_{K/k}$ for the norm, even when applied to $K(x)$.

In lifting an ideal to the over-field, one can never lose it, as follows from the important fact that

$$(\mathfrak{a}\mathfrak{O})\cap k = \mathfrak{a}$$

for each ideal $\mathfrak{a}$ of k. This is often considered a deeper fact than it is, probably because some of the older treatments of the classical ideal theory place heavy emphasis on showing that each ideal divides an element. Since $\mathfrak{a}\leqq(\mathfrak{a}\mathfrak{O})\cap k$, we have $\mathfrak{a}=[(\mathfrak{a}\mathfrak{O})\cap k]\mathfrak{c}$ with $\mathfrak{c}\leqq\mathfrak{o}$. Hence $\mathfrak{a}\leqq\mathfrak{a}\mathfrak{c}\mathfrak{O}$, $\mathfrak{a}^{-1}\mathfrak{a}\leqq\mathfrak{a}^{-1}\mathfrak{a}\mathfrak{c}\mathfrak{O}$, $\mathfrak{o}\leqq\mathfrak{c}\mathfrak{O}$, $\mathfrak{c}^{-1}\leqq\mathfrak{O}$, $\mathfrak{c}^{-1}\leqq\mathfrak{O}\cap k=\mathfrak{o}$, $\mathfrak{c}=\mathfrak{o}$, $\mathfrak{a}=(\mathfrak{a}\mathfrak{O})\cap k$. Because of this, there is no harm in using the same symbol $\mathfrak{a}$ to denote $\mathfrak{a}$ and $\mathfrak{a}\mathfrak{O}$.

If $\mathfrak{A}$ is an ideal in K and $[K: k]=n$, the norm of $\mathfrak{A}$ is defined by

$$N_{K/k}\mathfrak{A} = \mathfrak{A}_1\cdots\mathfrak{A}_n,$$

the product of the conjugates of $\mathfrak{A}$. This computation takes place in a finite extension N of K, however the answer is actually an ideal in k—and here is where we use forms: there is a polynomial $F(x)\in K[x]$ such that $\mathrm{Ct}\,(F)=\mathfrak{A}$. We have $N_{K/k}\mathfrak{A}=\mathfrak{A}_1\cdots\mathfrak{A}_n=(\mathrm{Ct}\,F_1)(\mathrm{Ct}\,F_2)\cdots(\mathrm{Ct}\,F_n)=\mathrm{Ct}\,(F_1\cdots F_n)$

$=\mathrm{Ct}\,(N_{K/k}F)$. But $N_{K/k}F(x)\in k(x)$, so its content is an ideal in k. The definition of the norm as product of conjugates tells us that the norm is a homomorphism:

$$N_{K/k}(\mathfrak{AB}) = (N\mathfrak{A})(N\mathfrak{B})$$

and that $N_{K/k}\mathfrak{a}=\mathfrak{a}^n$ for $\mathfrak{a}$ in k.

It is also true that $N\mathfrak{A}$ is the ideal in k generated by all norms of elements of $\mathfrak{A}$, and this provides a strictly rational, albeit clumsy, alternative definition of the norm.

If $\mathfrak{p}$ is a prime ideal in $\mathfrak{o}$, and

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

is its factorization in $\mathfrak{O}$ into primes, then taking norms yields

$$n = e_1 f_1' + \cdots + e_r f_r', \qquad N_{K/k}\mathfrak{P}_i = \mathfrak{p}^{f_i'}, \qquad f_i' \geqq 1.$$

We have $\mathfrak{P}_i \cap k = \mathfrak{p}$ and e_i is the ramification order of $\mathfrak{P}_i$ in K/k. In certain circumstances it is correct to designate f_i' the residue class degree of $\mathfrak{P}_i$ in K/k.

Actually, $\mathfrak{p}$ is maximal in $\mathfrak{o}$ so that $k_\mathfrak{p}=\mathfrak{o}/\mathfrak{p}$ is a field, the residue class field of $\mathfrak{p}$. If $\mathfrak{P}$ is one of the primes in K lying over $\mathfrak{p}$, then there is a natural imbedding $k_\mathfrak{p}\leqq K_\mathfrak{P}$ and $f=[K_\mathfrak{P}\colon k_\mathfrak{p}]$. This number f, the true residue class degree of P in K/k is bounded by n.

A few of the harder things, which are actually fairly transparent for principal ideal rings, are these. First of all $f_i\leqq f_i'$ so that $\sum e_i f_i \leqq n$. Actually,

$$\sum e_i f_i = \dim_{k_\mathfrak{p}} (\mathfrak{O}/\mathfrak{O}\mathfrak{p}) \leqq [K\colon k] = n.$$

There is equality in certain cases. For example if K/k is a separable extension, or if k is a $\mathfrak{p}$-adic field. Conditions for equality are given in [9].

3. **The rational function ring.** Let us fix attention on one ring $\mathfrak{o}$ with classical ideal theory, its quotient field k, and the rational function field $k(x)=k(x_1, x_2, \cdots)$, which is naturally the quotient field of $\mathfrak{o}[x]$. We consider the domain

$$\mathfrak{o}_x = \{r(x) \in k(x) \mid \mathrm{Ct}\, r \leqq \mathfrak{o}\}.$$

That this really is a ring is a consequence of the following.

LEMMA 1. $\mathrm{Ct}\,(r+s)\leqq(\mathrm{Ct}\, r, \mathrm{Ct}\, s)$.

Proof. It is obvious when r and s are polynomials; in general, it follows from writing r and s with a common denominator.

Next, let $S=S_x$ denote the (multiplicatively closed) set

$$S = \{g(x) \in \mathfrak{o}[x] \mid \mathrm{Ct}\, g = \mathfrak{o}\}.$$

LEMMA 2. *We have*

$$\mathfrak{o}_x = \mathfrak{o}[x]_S.$$

Proof. Clearly, each element of the quotient ring is in $\mathfrak{o}_x$. Conversely, if $r(x) \in \mathfrak{o}_x$, we may write $r(x) = f(x)/g(x)$ with f, $g \in \mathfrak{o}[x]$. We select a polynomial $h \in \mathfrak{o}[x]$ so that $(\mathrm{Ct}\, g)(\mathrm{Ct}\, h) = (b)$ is principal. Then $g(x)h(x) = bv(x)$ with $v(x) \in \mathfrak{o}[x]$, $\mathrm{Ct}\,(v) = \mathfrak{o}$. Since $r \in \mathfrak{o}_x$, we have $\mathrm{Ct}\, g \leqq \mathrm{Ct}\, f$, $(b) \leqq \mathrm{Ct}\,(fh)$, $fh = bu$ with $u(x) \in \mathfrak{o}[x]$, $r = u/v \in \mathfrak{o}[x]_S$.

From this follows the evident corollary.

COROLLARY. *We have*

$$k(x) = k[x]_S.$$

Now let $[K: k] = n$ and let $\mathfrak{O}$ denote the ring of elements of K integral over $\mathfrak{o}$. Then $[K(x): k(x)] = n$ and $\mathfrak{O}_x$ is perfectly well defined in $K(x)$.

LEMMA 3. *As in Lemma 2, let S denote the set of polynomials in $\mathfrak{o}[x]$ of content $\mathfrak{o}$. Then*

$$\mathfrak{O}_x = \mathfrak{O}[x]_S$$

and, indeed, this ring is the integral closure of $\mathfrak{o}_x$ in $K(x)$.

Proof. It is clear that $\mathfrak{O}[x]_S \leqq \mathfrak{O}_x$. By Lemma 2, if $R(x) \in \mathfrak{O}_x$, then $R(x) = F(x)/G(x)$, where F, $G \in \mathfrak{O}[x]$, $\mathrm{Ct}\, G = \mathfrak{O}$. We have $g(x) = N_{K/k}G(x) = G(x)H(x)$, $H(x) \in \mathfrak{O}[x]$ and $\mathrm{Ct}\, g(x) = \mathfrak{o}$, $g(x) \in S$. Consequently, $R(x) = F(x)H(x)/g(x)$ is in $\mathfrak{O}[x]_S$.

Now let $R(x) \in \mathfrak{O}_x$ so that $R(x) = F(x)/g(x)$, $F(x) \in \mathfrak{O}[x]$, $g(x) \in \mathfrak{o}[x]$, $\mathrm{Ct}\,(g) = \mathfrak{o}$. Since each coefficient of $F(x)$ is integral over $\mathfrak{o}$, F is integral over $\mathfrak{o}[x]$, and a fortiori over $\mathfrak{o}_x$. But $g(x)$ is a unit in $\mathfrak{o}_x$, hence $R(x)$ is integral over $\mathfrak{o}_x$.

On the other hand, assume $R(x)$ is integral over $\mathfrak{o}_x$, say

$$R^m + r_1(x)R^{m-1} + \cdots + r_m(x) = 0$$

with $r_i(x) \in \mathfrak{o}_x$. It follows from Lemma 1 that

$$(\mathrm{Ct}\, R)^m \leqq (\mathrm{Ct}\,(r_1R^{m-1}), \cdots, \mathrm{Ct}\,(r_m)) \leqq ((\mathrm{Ct}\, R)^{m-1}, (\mathrm{Ct}\, R)^{m-2}, \cdots, \mathfrak{O}).$$

It follows easily that the ideal $\mathrm{Ct}\,(R)$ of the field K w.r.t. the Dedekind ring $\mathfrak{O}$ is an integral ideal—any prime ideal in the denominator of $\mathrm{Ct}\, R$ would appear to a lower power on the left than on the right. Thus $\mathrm{Ct}\,(R) \leqq \mathfrak{O}$, $R \in \mathfrak{O}_x$.

It is an evident corollary that $\mathfrak{o}_x$ itself is integrally closed.

4. **The main results.** These are stated in this section; the proofs are given in the next.

THEOREM A. *The domain $\mathfrak{o}_x$ is a principal ideal ring.*

If $\bar{\mathfrak{a}}$ is any fractional ideal of $k(x)$ w.r.t. $\mathfrak{o}_x$, we set

$$\mathrm{Ct}\,\bar{\mathfrak{a}} = \text{g.c.d. } (\mathrm{Ct}\,r(x); r(x) \in \bar{\mathfrak{a}}).$$

Thus $\bar{\mathfrak{a}} \to \mathrm{Ct}\,\bar{\mathfrak{a}}$ is a mapping on the group of fractional ideals of $k(x)$ onto that of k. We note that $\bar{\mathfrak{a}} \leqq \mathfrak{o}_x$ implies $\mathrm{Ct}\,\bar{\mathfrak{a}} \leqq \mathfrak{o}$.

THEOREM B. *The mapping* $\bar{\mathfrak{a}} \to \mathfrak{a} = \mathrm{Ct}\,\bar{\mathfrak{a}}$ *is an isomorphism of the ideal group of* $k(x)$ *onto that of* k. *The semi-group of integral ideals of* $\mathfrak{o}_x$ *is mapped onto that of* $\mathfrak{o}$, *prime ideals corresponding.*

This mapping is characterized in the following way:

$$\bar{\mathfrak{a}} \to \mathfrak{a} = \mathrm{Ct}\,\bar{\mathfrak{a}} = \bar{\mathfrak{a}} \cap k, \qquad \mathfrak{a} \to \bar{\mathfrak{a}} = \mathfrak{o}_x\mathfrak{a}.$$

Suppose that $\mathfrak{a}$ *is an integral ideal and* $\mathfrak{a} \leftrightarrow \bar{\mathfrak{a}}$. *Then there is a natural isomorphism*

$$\mathfrak{o}_x/\bar{\mathfrak{a}} \approx (\mathfrak{o}/\mathfrak{a})[x]_T$$

where T *is the set of nondivisors of zero in* $(\mathfrak{o}/\mathfrak{a})[x]$. *This isomorphism is induced by the natural extension of* $\mathfrak{o} \to \mathfrak{o}/\mathfrak{a}$ *to* $\mathfrak{o}[x]$. *In particular, for a prime ideal* $\mathfrak{p}$, *the residue class fields correspond according to*

$$k(x)_{\bar{\mathfrak{p}}} = \mathfrak{o}_x/\bar{\mathfrak{p}} \approx (\mathfrak{o}/\mathfrak{p})(x) = k_{\mathfrak{p}}(x).$$

SUPPLEMENT TO THEOREM B. *If* $\mathfrak{o}$ *is the valuation ring of a (discrete) valuation* V, *then* $\mathfrak{o}_x$ *is the valuation ring for the natural extension of* V *to* $k(x)$:

$$V(\sum a_i M_i) = \min (Va_i),$$

where the M_i *are distinct monomials.*

This result shows the connection with the known characterization of Dedekind rings in terms of valuations. (See [6] and the forthcoming second volume of [9].)

Now let $[K: k] = n$ and let $\mathfrak{O}$ be the ring of integral elements of K w.r.t. $\mathfrak{o}$.

THEOREM C. *The diagram*

$$\begin{array}{ccc} [\textit{Ideal group of } K(x)] & \xrightarrow{\mathrm{Ct}} & [\textit{Ideal group of } K] \\ \downarrow N_{K(x)/k(x)} & & \downarrow N_{K/k} \\ [\textit{Ideal group of } k(x)] & \xrightarrow{\mathrm{Ct}} & [\textit{Ideal group of } k] \end{array}$$

is commutative.

If $\mathfrak{P}$ *is a prime ideal of* $\mathfrak{O}$, $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}$, *then the ramification order* e *in* $\mathfrak{p} = \mathfrak{P}^e \cdots$, *the norm degree in* $N_{K/k}\mathfrak{P} = \mathfrak{p}^f$, *and the residue class degree in* $[K_T: k_{\mathfrak{p}}] = f$ *coincide respectively with those of the pair* $\overline{\mathfrak{P}}$, $\bar{\mathfrak{p}}$.

If K/k *is a separable extension, then the differents and discriminants correspond*:

$$\mathfrak{D}_{K(x)/k(x)} = \overline{\mathfrak{D}}_{K/k}, \qquad \mathfrak{d}_{K(x)/k(x)} = \overline{\mathfrak{d}}_{K/k}.$$

If K/k is a galois extension, and we make the natural identification of $\mathfrak{G}(K/k)$ with $\mathfrak{G}(K(x)/k(x))$, then the various Hilbert sub-groups of $\mathfrak{G}$, splitting, inertial, etc., with respect to a prime are the same for K/k as for $K(x)/k(x)$. The Hilbert "elements" of K and $K(x)$ correspond.

The Hilbert "element" of an automorphism σ is the ideal

$$E_\sigma = \gcd\{A - \sigma A \mid A \in \mathfrak{O}\}.$$

5. **Proofs of the theorems.** We begin with Theorem B by showing first that $\mathrm{Ct}\,\bar{\mathfrak{a}} = \bar{\mathfrak{a}} \cap k$. If $b \in \bar{\mathfrak{a}} \cap k$, then $b \in k(x)$ and $b = \mathrm{Ct}\, b \in \mathrm{Ct}\,\bar{\mathfrak{a}}$, hence $\bar{\mathfrak{a}} \cap k \leqq \mathrm{Ct}\,\bar{\mathfrak{a}}$. Conversely, let $r(x) \in \bar{\mathfrak{a}}$ and $a = \mathrm{Ct}\, r(x)$. Then $\mathrm{Ct}\,[a/r(x)] = \mathfrak{o}$, $a/r(x) \in \mathfrak{o}_x$, $a \in r(x)\mathfrak{o}_x \leqq \bar{\mathfrak{a}}$, $a \in \bar{\mathfrak{a}} \cap k$, $\mathrm{Ct}\,\bar{\mathfrak{a}} \leqq \bar{\mathfrak{a}} \cap k$.

Now let $\bar{\mathfrak{a}} \to \mathfrak{a} = \mathrm{Ct}\,\bar{\mathfrak{a}} = \bar{\mathfrak{a}} \cap k$. We shall prove that $\mathfrak{o}_x\mathfrak{a} = \bar{\mathfrak{a}}$. Clearly $\mathfrak{o}_x\mathfrak{a} \leqq \bar{\mathfrak{a}}$. Let $r(x) \in \bar{\mathfrak{a}}$. By Lemma 2, Corollary, $r(x) = f(x)/g(x)$ where $f(x) \in k[x]$ and $g(x)$ is a unit in $\mathfrak{o}_x$. Thus $f(x) \in \bar{\mathfrak{a}}$. We write $f(x) = \sum a_i M_i$ where the M_i are distinct monomials and have $\mathrm{Ct}\, f = (a_1 \cdots) \leqq \mathfrak{a}$. Since $M_i \in \mathfrak{o}[x] \leqq \mathfrak{o}_x$, $f(x) = \sum a_i M_i \in \mathfrak{o}_x\mathfrak{a}$, hence $r(x) \in \mathfrak{o}_x\mathfrak{a}$, $\bar{\mathfrak{a}} \leqq \mathfrak{o}_x\mathfrak{a}$, $\bar{\mathfrak{a}} = \mathfrak{o}_x\mathfrak{a}$.

Next, suppose $\mathfrak{a}$ is an ideal of k and $\bar{\mathfrak{a}} = \mathfrak{o}_x\mathfrak{a}$. We shall prove $\bar{\mathfrak{a}} \cap k = \mathfrak{a}$. It is clear that $\mathfrak{a} \leqq \bar{\mathfrak{a}} \cap k$. If $a \in \bar{\mathfrak{a}} \cap k$, then $a = \sum a_i r_i(x)$, $a_i \in \mathfrak{a}$, $r_i(x) \in \mathfrak{o}_x$. We may use Lemma 2 again to write the $r_i(x)$ as fractions with common denominator a unit of $\mathfrak{o}_x$, $r_i(x) = f_i(x)/g(x)$, so that $a = (\sum a_i f_i(x))/g(x)$, $(a) = \mathrm{Ct}\,(\sum a_i f_i) \leqq (a_1, \cdots, a_n) \leqq \mathfrak{a}$, $\bar{\mathfrak{a}} \cap k \leqq \mathfrak{a}$, $\bar{\mathfrak{a}} \cap k = \mathfrak{a}$.

The fact that the mapping $\bar{\mathfrak{a}} \leftrightarrow \mathfrak{a}$ is a one-one correspondence as asserted is now apparent. The multiplicative character of this correspondence is most easily seen from

$$\mathfrak{a}\mathfrak{b} \to \mathfrak{o}_x(\mathfrak{a}\mathfrak{b}) = (\mathfrak{o}_x\mathfrak{a})(\mathfrak{o}_x\mathfrak{b}) = \bar{\mathfrak{a}}\bar{\mathfrak{b}},$$

while the assertion about prime ideals is therefore evident.

Now let $\mathfrak{a}$ be an integral ideal, $\mathfrak{a} \leftrightarrow \bar{\mathfrak{a}}$. Let ϕ denote the canonical mapping $\mathfrak{o} \to \mathfrak{r} = \mathfrak{o}/\mathfrak{a}$. We prolong this in the obvious way to a mapping ϕ on $\mathfrak{o}[x]$ onto $\mathfrak{r}[x]$, and investigate $\phi(S)$. Our assertion is that

$$\phi(S) = T = \{\text{nondivisors of zero of } \mathfrak{r}[x]\}.$$

If $g(x) \in S$ so that $\mathrm{Ct}\, g = \mathfrak{o}$, then ϕg is certainly a nonzero divisor. In fact $(\phi g)(\phi h) = 0$ implies $\phi(gh) = 0$, $gh \in \mathfrak{a}[x]$, $\mathrm{Ct}\, g\ \mathrm{Ct}\, h \leqq \mathfrak{a}$, $\mathrm{Ct}\, h \leqq \mathfrak{a}$, $\phi h = 0$. Conversely let $\phi h \in T$. We claim that $(\mathrm{Ct}\, h, \mathfrak{a}) = \mathfrak{o}$. For otherwise $\mathfrak{a} \leqq (\mathrm{Ct}\, h, \mathfrak{a}) < \mathfrak{o}$ and there will exist an ideal $\mathfrak{b}$, $\mathfrak{a} < \mathfrak{b} \leqq \mathfrak{o}$, $\mathfrak{b}(\mathrm{Ct}\, h, \mathfrak{a}) \leqq \mathfrak{a}$. We then pick a polynomial $f(x)$ such that $\mathrm{Ct}\, f = \mathfrak{b}$ and $\mathrm{Ct}\,(fh) \leqq \mathfrak{a}$, $(\phi f)(\phi h) = 0$, $\phi f \neq 0$, contrary to the hypothesis that ϕh is not a zero-divisor. Thus $(\mathrm{Ct}\, h, \mathfrak{a}) = \mathfrak{o}$. This implies $(\mathrm{Ct}\, h, a) = \mathfrak{o}$ for some $a \in \mathfrak{a}$. If m exceeds $\deg h$, then $\mathrm{Ct}\,(h + ax_1^m) = \mathfrak{o}$ and $g = h + ax_1^m \equiv h \pmod{\mathfrak{a}}$ so that $g \in S$, $\phi g = \phi h$, establishing our assertion above.

It is an easy consequence of this that ϕ induces a homomorphism on

$\mathfrak{o}_x = \mathfrak{o}[x]_S$ onto $\mathfrak{r}_T$. If $r(x)$ is in the kernel, $r(x) = f(x)/g(x)$ as in Lemma 2, then $\phi f(x) = 0$, $f(x)$ has coefficients in $\mathfrak{a}$, and so $r(x) \in \bar{\mathfrak{a}}$, and conversely. Finally, ϕ induces

$$\phi\colon \mathfrak{o}_x/\bar{\mathfrak{a}} \approx (\mathfrak{o}/\mathfrak{a})[x]_T.$$

In case $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ are prime ideals, $\mathfrak{o}/\mathfrak{p}$ is a field $k_\mathfrak{p}$ and T consists of all non-zero polynomials so that the right-hand side is the rational function field $k_\mathfrak{p}(x)$.

The supplement follows easily from the definitions.

We may dispose of Theorem A easily. If $\bar{\mathfrak{a}}$ is an ideal of $k(x)$, then by Theorem B, $\bar{\mathfrak{a}} = \mathfrak{a}\mathfrak{o}_x$ for $\mathfrak{a} = \mathrm{Ct}\,\bar{\mathfrak{a}}$. If $\mathfrak{a} = (a_1, \cdots, a_n)$ and $f(x)$ is any polynomial with coefficients a_i, then $\mathrm{Ct}\, f = \mathfrak{a}$, hence $\bar{\mathfrak{a}} = (f(x))$.

In view of this, the first assertion of Theorem C is clear. In fact if $\mathfrak{A}$ is an ideal of K, $\mathfrak{A} = (A_1, \cdots)$, and $F(x)$ has coefficients $A_1, \cdots$, then $\overline{\mathfrak{A}} = (F)$, $N\,\mathrm{Ct}\,\overline{\mathfrak{A}} = N\mathfrak{A} = \mathrm{Ct}\, NF = \mathrm{Ct}\, N\overline{\mathfrak{A}}$. The statements about the ramification order and various degrees follow from this and the results of Theorem B.

In the separable case, the different may be defined by

$$\mathfrak{D}^{-1}_{K/k} = \{A \in K \mid S_{K/k}(A\mathfrak{O}) \leqq \mathfrak{o}\},$$

where S is the trace function. We have

$$(\mathfrak{D}_{K(x)/k(x)})^{-1} = \{R(x) \in K(x) \mid S[R(x)\mathfrak{O}_x] \leqq \mathfrak{o}_x\}.$$

Setting $R(x) = F(x)/g(x)$ according to Lemma 3, and using the linearity of the trace, we have

$$\begin{aligned}(\mathfrak{D}_{K(x)/k(x)})^{-1} &= \{R(x) \mid S[R(x)\mathfrak{O}] \leqq \mathfrak{o}_x\} \\ &= \{R(x) \mid S[F(x)\mathfrak{O}] \leqq \mathfrak{o}_x\} \\ &= \{R(x) \mid F(x) \in \mathfrak{D}^{-1}_{K/k}[x]\} = (\overline{\mathfrak{D}}_{K/k})^{-1}.\end{aligned}$$

This gives the correspondence between differents, that for discriminants is obtained by taking norms.

The results on galois extension will now be routine to those familiar with the Hilbert theory. We merely mention that the characterizations of the various Hilbert subfields in terms of maximality properties relative to the factorization of the prime in question makes the results transparent.

6. **Further remarks.** We first note an evident consequence of Theorem A.

COROLLARY. *The adjunction of sets of variables is transitive*:

$$(\mathfrak{o}_x)_y = \mathfrak{o}_z, \qquad z = \{x, y\}.$$

For the typical element of $(\mathfrak{o}_x)_y$ is a rational function of the form $P(x, y)/G(x, y)$ where $P, G \in \mathfrak{o}_x[y]$ and the content in $\mathfrak{o}_x$ of $G(x, y)$ is $\mathfrak{o}_x$. Clearing the denominators puts this into the form $f(x, y)/g(x, y)$ where $f,\ g \in \mathfrak{o}[x, y]$ and $\mathrm{Ct}\, g = \mathfrak{o}$.

The considerations of Theorems B and C carry over to modules in the following way. Suppose $\mathfrak{M}$ is a subset of K which is an $\mathfrak{o}$-module. Then $\mathfrak{M}_x = \mathfrak{o}_x\mathfrak{M}$ is the $\mathfrak{o}_x$-module it generates in $K(x)$. We assert that $\mathfrak{M}_x \cap K = \mathfrak{M}$.

To prove this we observe first the easy part, $\mathfrak{M} \leqq \mathfrak{M}_x \cap K$, and pass to the reverse inclusion. Suppose $A \in \mathfrak{M}_x \cap K$. Then $A = f(x)/g(x)$, where $f(x) \in \mathfrak{M}[x]$, $g(x) \in \mathfrak{o}(x)$, and $\mathrm{Ct}\, g = \mathfrak{o}$. Equating coefficients, we deduce that $A \in \mathfrak{o}\mathfrak{M} = \mathfrak{M}$.

The part of Theorem C dealing with the different now carries over to complementary modules. Suppose K/k is a separable extension and that $\mathfrak{M}$ is a finite $\mathfrak{o}$-submodule of K which contains a basis of K over k. The complementary module $\mathfrak{M}'$ is defined by $\mathfrak{M}' = \{A \in K \mid S_{K/k}(A\mathfrak{M}) \leqq \mathfrak{o}\}$. We now assert that $(\mathfrak{M}_x)' = (\mathfrak{M}')_x$. The proof is similar to that in §5 for the different.

The connection between the discriminant and ramification is relatively easy to see in the Kummer case [8, p. 75, ff.] because of the special type of integral basis. The following statements show a partial connection between this and the general case.

PROPOSITION 1. *If $\omega_1, \cdots, \omega_n$ is an integral basis of $\mathfrak{O}$ over $\mathfrak{o}$, then it is also an integral basis of $\mathfrak{O}_x$ over $\mathfrak{o}_x$. More generally, if an ideal $\mathfrak{A}$ of K has an ideal basis $\alpha_1, \cdots, \alpha_n$ over $\mathfrak{o}$, then $\mathfrak{A}_x$ has the same ideal basis over $\mathfrak{o}_x$.*

Proof. Suppose $\mathfrak{A} = \mathfrak{o}\alpha_1 \oplus \cdots \oplus \mathfrak{o}\alpha_n$. By Lemma 3, $\mathfrak{O}_x = \mathfrak{o}_x\mathfrak{O}$, so by Theorem B, $\mathfrak{A}_x = \mathfrak{O}_x\mathfrak{A} = \mathfrak{o}_x\mathfrak{O}\mathfrak{A} = \mathfrak{o}_x\mathfrak{A} = \mathfrak{o}_x\alpha_1 \oplus \cdots \oplus \mathfrak{o}_x\alpha_n$.

An extension K/k is called *locally separable everywhere* if each residue class field extension $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ is separable.

PROPOSITION 2. *Suppose K/k is a separable extension which is locally separable everywhere. Let $\omega_1, \cdots, \omega_n$ be an integral basis of $\mathfrak{O}$ over $\mathfrak{o}$ and set*

$$\xi = \omega_1 x_1 + \cdots + \omega_n x_n$$

so that $\xi \in K(x)$, $x = (x_1, \cdots, x_n)$. Then

$$1, \xi, \xi^2, \cdots, \xi^{n-1}$$

is an integral basis of $\mathfrak{O}_x$ over $\mathfrak{o}_x$.

The proof of this fact can be lifted from Theorem 35 of Hilbert [4] and is closely connected with the relation between the different and the elements. We intend to return to this subject at a later date.

As a consequence we have the following.

PROPOSITION 3. *Let K/k be a separable extension which is locally separable everywhere. Then for a suitable $x = (x_1, \cdots)$, the ring $\mathfrak{O}_x$ has an integral basis of the form $1, \xi, \cdots, \xi^{n-1}$ over $\mathfrak{o}_x$.*

For we simply adjoin t. Then $\mathfrak{o}_t$ is a principal ideal ring, hence $\mathfrak{O}_t$ has an integral basis over $\mathfrak{o}_t$. Now Proposition 2 applies; we adjoin n other variables $x_1, \cdots, x_n$ and take $x = (t, x_1, \cdots, x_n)$.

Another result which shows the usefulness of forms is this.

PROPOSITION 4. *Suppose* $\omega_1, \cdots, \omega_n$ *is an integral basis of* $\mathfrak{O}$ *over* $\mathfrak{o}$ *and that* $\alpha_1, \cdots, \alpha_n$ *is an ideal basis of* $\mathfrak{A}$ *over* $\mathfrak{o}$. *Suppose also that* $\alpha_i = \sum a_{ij}\omega_j$, $a_{ij} \in k$. *Then*

$$N_{K/k}\mathfrak{A} = (\det \mid a_{ij} \mid).$$

Proof. In case $\mathfrak{A} = (A)$ is a principal ideal, then $A\omega_1, \cdots, A\omega_n$ is also an ideal basis of $\mathfrak{A}$ which we may use in place of the basis α since the two are related by a unimodular substitution. But from $A\omega_i = \sum a_{ij}\omega_j$ we have $N\mathfrak{A} = (NA) = (\det \mid a_{ij} \mid)$.

In the general case we simply adjoin a variable x, pass to $\mathfrak{O}_x$, which is a principal ideal ring, and then use Theorem C.

It is clear that a slightly more general result is available. Suppose $\mathfrak{A}$ and $\mathfrak{B}$ have ideal bases $\alpha_1, \cdots, \alpha_n$; $\beta_1, \cdots, \beta_n$ resp., and that $\alpha_i = \sum a_{ij}\beta_j$. Then $N(\mathfrak{A}\mathfrak{B}^{-1}) = (\det \mid a_{ij} \mid)$.

7. **Conclusion.** The real meaning of Theorems B and C is that the arithmetic structure of k and its finite extensions which centers around the ideal group carries over to an identical structure for the rational function field, and the correspondence between ideals is the most natural one. This is not really surprising in view of the fact that we are adjoining independent variables in an essentially algebraic situation. All this gives real significance to the role of forms in classical ideal theory. Theorem A which asserts that the ideal theory in the rational function field is the simplest one can hope for, principal ideal theory, accounts precisely for the success of the technique of forms.

REFERENCES

1. H. Flanders, *Remark on Kronecker's theorem on forms*, Proc. Amer. Math. Soc. vol. 3 (1952) p. 197.

2. H. Grell, *Über die Gültigkeit der gewöhnlichen Idealtheorie in endlichen algebraischen Erweiterungen erster und zweiter Art*, Math. Z. vol. 40 (1935–1936) pp. 503–505.

3. E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig, 1923.

4. D. Hilbert, *Theorie der algebraischen Zahlkörper*, *Gesammelte Abhandlungen* I, 1932; also Jber. Deutsch. Math. Verein. vol. 4 (1897) pp. 175–546.

5. L. Kronecker, *Grundzüge einer arithmetischen Theorie der algebraischen Grössen*, Berlin, 1882.

6. O. F. G. Schilling, *Theory of valuations*, New York, 1950.

7. B. L. Van der Waerden, *Moderne algebra* II, Berlin, 1940.

8. H. Weyl, *Algebraic theory of numbers*, Princeton, 1940.

9. O. Zariski and P. Samuel, *Commutative algebra* I, New York, 1958.

UNIVERSITY OF CALIFORNIA,
BERKELEY, CALIFORNIA