RADICAL MODULES OVER A DEDEKIND DOMAIN

A. FRÖHLICH

To the memory of TADASI NAKAYAMA

A radical of a field K is a non zero element of a given algebraic closure some positive power of which lies in K. The group $R(K)$ of radicals reflects properties of the field K and is in turn easily determined as an extension of the multiplicative group K^* of non zero elements of K. The elements of the quotient group $R(K)/K^*$ are then conveniently identified with certain subspaces of the algebraic closure, the radical spaces of K (cf. § 1). What we are here concerned with is the corresponding arithmetic situation, in which we start with a Dedekind domain $\mathfrak{o}$ with quotient field K. The role of the radicals is taken over by the radical modules. These form a group $\mathfrak{R}(\mathfrak{o})$ which contains the group of fractional ideals of $\mathfrak{o}$ (cf. § 4).

The ideal theory of $\mathfrak{o}$ is equivalent with its valuation theory. Although the same is no longer strictly true, when translated into the new context, there is still a close connection between the "valuations" of $R(K)$ and the theory of radical modules (cf. § 3, 4). There is also the new feature, to which there is no analogue in the valuation theory of $\mathfrak{o}$, that each discrete valuation gives rise to a character of the radical spaces, i.e. of $R(K)/K^*$. These characters can in a natural manner be lifted back to real valued functions. On the basis of the theory of integral radical modules—the analogue to the integral ideals—one then obtains the conductor of a radical space (§ 6), which plays an important role in the ramification theory.

The group $\mathfrak{R}(\mathfrak{o})$ differs from $R(K)$ in presenting a genuine divisibility problem. We shall show, in § 5, that a radical module is divisible by n if and only if its image under a canonical map onto the ideal class group of $\mathfrak{o}$ is divisible by n. Looking at it the other way round, one obtains in terms of $\mathfrak{R}(\mathfrak{o})$ an essentially local, necessary and sufficient condition for the class of a fractional ideal of $\mathfrak{o}$ to be an n-th power. As an application of this criterion we shall then give a

Received July 24, 1965.

new proof for the theorem that the class of a discriminant is a square.

In the group of fractional ideals the base ring $\mathfrak{o}$ itself is the only torsion element, and the only unit (integral ideal with integral inverse). On the other hand $\mathfrak{R}(\mathfrak{o})$ has proper torsion elements and proper units. We shall show that these coincide (cf. § 7).

The principal application, which I shall give here is to the ramification theory of pure extensions (cf. § 8, with the algebraic background in § 2). This constitutes a generalization of some results of an earlier paper (cf. [3]), where only normal, i.e. Abelian pure extensions had been considered. The precise translation to the language of [3] can be read off from example 2 in § 2.

Elsewhere I shall introduce "arithmetic resolvents" for normal extensions of the quotient field of a Dedekind domain. These associate with each "integral representation" of the Galois group an object which will turn out to be a radical module. It was this application which first motivated my interest in radical modules.

1. Radical subspaces

The multiplicative group of non zero elements of a field K will always be denoted by K^*. Let K be a field, L an extension field of K. The *radicals* of L/K, i.e. the elements α of L^* for which some power α^n $(n>0)$ lies in K^*, form a subgroup of L^*, to be denoted by $R(L/K)$, which contains K^*.

For subgroups M and N of the additive group of L we define the *module product* MN to be the additive subgroup of L which is generated by the element products $\alpha\beta$, with $\alpha\in M$ and $\beta\in N$. A *radical subspace* P of L/K is a K-submodule of L, which is of K-rank 1 and which under the module product satisfies an equation

$$P^n = K,$$

for some natural n. The radical subspaces of L/K then form an Abelian group under the module product, which will be denoted by $\mathfrak{R}(L/K)$. The map $\alpha\mapsto\alpha K$ defines a homomorphism $R(L/K)\to\mathfrak{R}(L/K)$, and the sequence

$$1\to K^*\to R(L/K)\to\mathfrak{R}(L/K)\to 1 \tag{1.1}$$

is exact.

The pairs L/K form a category, a morphism $L/K\to L'/K'$ being given by an

injective homomorphism $L \to L'$ of fields which maps K into K'. One clearly has

1.1. PROPOSITION. *The sequence* (1.1) *is a functor of* L/K.

If $L' \supset L \supset K$ *then the sequence*

$$1 \to \mathfrak{R}(L/K) \to \mathfrak{R}(L'/K) \to \mathfrak{R}(L'/L) \tag{1.2}$$

is exact. If moreover L *is algebraically closed in* L' *then the maps*

$$R(L/K) \to R(L'/K),\ \mathfrak{R}(L/K) \to \mathfrak{R}(L'/K)$$

are isomorphisms.

From this proposition it follows that if $\overline{K}$ is an algebraic closure of K, then the groups $R(L/K)$ may be viewed as subgroups of

$$R(K) = R(\overline{K}/K)$$

and the groups $\mathfrak{R}(L/K)$ as subgroups of

$$\mathfrak{R}(K) = \mathfrak{R}(\overline{K}/K).$$

We shall adopt this point of view throughout, and shall use the symbols $\overline{K}$, $R(K)$ and $\mathfrak{R}(K)$ in the present connotation. The elements of $\mathfrak{R}(K)$ will be called the *radical spaces of* K.

2. Pure extensions

If $\mathfrak{G}$ is a subgroup of $\mathfrak{R}(K)$ then the sum

$$K(\mathfrak{G}) = \sum_{\mathfrak{G}} P \tag{2.1}$$

of submodules of $\overline{K}$ is a field. We shall call $K(\mathfrak{G})$ a *pure extension* of K (by $\mathfrak{G}$) if this sum is direct.

2.1. PROPOSITION. *Suppose that* $K(\mathfrak{G})$ *is a pure extension of* K *by* $\mathfrak{G}$. *If* $\mathfrak{H}$ *is a subgroup of* $\mathfrak{G}$ *then* $L = K(\mathfrak{H})$ *is a pure extension of* K *by* $\mathfrak{H}$, *contained in* $K(\mathfrak{G})$, *and*

$$\mathfrak{H} = \mathfrak{G} \cap \mathfrak{R}(L/K).$$

If $\overline{\mathfrak{G}}$ *is the image of* $\mathfrak{G}$ *in* $\mathfrak{R}(L)$ *then the sequence*

$$1 \to \mathfrak{H} \to \mathfrak{G} \to \overline{\mathfrak{G}} \to 1 \tag{2.2}$$

is exact and

$$K(\mathfrak{H}) = L(\overline{\mathfrak{G}})$$

is a pure extension of L by $\overline{\mathfrak{G}}$.

Proof. It is immediately obvious that the sum over $\mathfrak{H}$ is direct, i.e. that $L = K(\mathfrak{H})$ is pure. It is clearly a subfield of $K(\mathfrak{G})$. If $P \in \mathfrak{G} \cap \mathfrak{N}(L/K)$, i.e. $P \subset \sum_{\mathfrak{H}} Q$ then $P = Q$ for some $Q \in \mathfrak{H}$, by the directness of the sum (2.1). The exactness of (2.2) is thus a consequence of the exactness of (1.2). Now however we see that each $\overline{P} \in \overline{\mathfrak{G}}$ is the sum over a coset of $\mathfrak{G}$ mod $\mathfrak{H}$, and so the sum over $\overline{\mathfrak{G}}$ is obtained by grouping together terms of (2.1), i.e. it is direct.

In the sequel we denote by $|\mathfrak{G}|$ the order of $\mathfrak{G}$ and by $(L : K)$ the degree over K of an extension field L.

2.2. Proposition. *$K(\mathfrak{G})$ is a pure extension of K by $\mathfrak{G}$ if and only if, for all finite subgroups $\mathfrak{H}$ of $\mathfrak{G}$, $K(\mathfrak{H})$ is a pure extension of K by $\mathfrak{H}$.*

If $\mathfrak{G}$ is a finite group, then a necessary and sufficient condition for $K(\mathfrak{G})$ to be a pure extension of K by $\mathfrak{G}$ is that

$$(K(\mathfrak{G}) : K) = |\mathfrak{G}|.$$

Proof. The last assertion is trivial. For the first part of the proposition one only has to note that $\mathfrak{G}$ is a torsion group, hence the union of its finite subgroups $\mathfrak{H}$. Consequently $K(\mathfrak{G})$ is the composite of the subfields $K(\mathfrak{H})$.

Let $\alpha \in R(K)$, and let $\mathfrak{G}$ be the cyclic group generated by αK. Then $K(\mathfrak{G}) = K(\alpha)$ and we have clearly

2.3. Proposition. *$K(\mathfrak{G})$ is pure, if and only if the minimal polynomial of α over K is pure, i.e. of form $X^n - a$.*

We mention one other proposition, which in conjunction with 2.3. yields a description of the finite pure extensions.

2.4. Proposition. *Let $\mathfrak{G}$ be the direct product of subgroups $\mathfrak{G}_1$ and $\mathfrak{G}_2$, each of which gives rise to a pure extension of K. Then $K(\mathfrak{G})$ is a pure extension of K by $\mathfrak{G}$ if and only if the fields $K(\mathfrak{G}_1)$ and $K(\mathfrak{G}_2)$ are linearly disjoint over K.*

This follows from the definition of linear disjointness (cf. [7] Ch. II).

Examples. 1. Let a be an element of K and let S be a multiplicatively closed set of natural numbers, such that for all $n \in S$ the polynomial $X^n - a$ is irreducible in $K[X]$. Then there is a subgroup $\mathfrak{G}$ of $\mathfrak{N}(K)$ with the following

properties: (i) $K(\mathfrak{G})$ is a pure extension of K by $\mathfrak{G}$, (ii) $K(\mathfrak{G})$ is the composite of the root fields K_n of the polynomials $X^n - a$, for $n \in S$. More precisely, if $\mathfrak{G}_n$ is the subgroup of $\mathfrak{G}$ of elements in $\mathfrak{G}$ which are annihilated by n, then $K(\mathfrak{G}_n) = K(\alpha_n)$ where $\alpha_n^n = a$.

To see this let (as throughout this paper) $\mathbf{Z}$ be the ring of integers. Denote by $\mathbf{Z}_S$ the quotient ring of $\mathbf{Z}$ with respect to S. As $R(K)$ is an injective Abelian group the homomorphism $\mathbf{Z} \to K^*$ which takes 1 into a can be extended to a homomorphism $\mathbf{Z}_S \to R(K)$. $\mathfrak{G}$ is then the image of the homomorphism $\mathbf{Z}_S \to R(K) \to \mathfrak{R}(K)$.

2. Let L be a finite or infinite, normal, separable extension of K with Galois group Γ. Let $\mathfrak{G}$ be the group of continuous homomorphisms $\Gamma \to K^*$, for the discrete group K^* and the profinite group Γ. For each $\phi \in \mathfrak{G}$ the elements α of L with

$$\alpha\gamma = \alpha\phi(\gamma), \text{ all } \gamma \in \Gamma$$

form a radical subspace L_ϕ. The map $\phi \mapsto L_\phi$ is an injective homomorphism $\mathfrak{G} \to \mathfrak{R}(K)$, i.e. we may view $\mathfrak{G}$ as embedded in $\mathfrak{R}(K)$. By the normal basis theorem $K(\mathfrak{G})$ is then a pure extension of K by $\mathfrak{G}$.

3. Let K have prime characteristic p and let L be a purely inseparable extension. Then $\mathfrak{R}(L/K) = L^*$. Let $\{\alpha_i\}$ be a p-basis of $K^{1/p} \cap L$ over K and let $\mathfrak{G}$ be the group generated by the subspaces $\alpha_i K$. Then $K(\mathfrak{G})$ is a pure extension.

3. Valuations

Let in the sequel the symbol $\mathbf{P}$ stand for the multiplicative group of positive real numbers. A *valuation* of $R(K)$ is a function ψ, defined on $R(K) \cup 0$ with values in $\mathbf{P} \cup 0$, so that

(i) The restriction ψ_K of ψ to K is a valuation of K.

(ii) The restriction of ψ to a radical subspace P is a norm of the K-module P with respect to ψ_K.

(iii) The restriction of ψ to $R(K)$ defines a homomorphism $R(K) \to \mathbf{P}$.

In the sequel we shall always use the same symbol both for valuations of $R(K)$ (or of K), and for the associated homomorphisms $R(K) \to \mathbf{P}$ (or $K^* \to \mathbf{P}$).

3.1. Proposition. *For every valuation ϕ of K there is a unique valuation ϕ^**

of $R(K)$ *with* $\phi_K^* = \phi$.

For every subgroup G *of* $R(K)$ *the restriction of* ϕ^* *to* G *is already uniquely determined by the property that it defines a homomorphism* $G \to \mathbf{P}$, *which extends the homomorphism* $K^* \to \mathbf{P}$.

Proof. $\mathbf{P}$ is a torsion free, injective Abelian group. Hence the diagram with exact row

$$\begin{array}{ccccc} 1 & \longrightarrow & K^* & \longrightarrow & G \\ & & \downarrow & & \\ & & \mathbf{P} & & \end{array}$$

can in a unique manner be completed to a commutative diagram

$$\begin{array}{ccc} K^* & \longrightarrow & G \\ \downarrow & \swarrow & \\ \mathbf{P} & & \end{array}$$

The proposition is an immediate consequence of this observation.

Remarks 1. If L is purely inseparable over K, i.e. $L^* = R(L/K)$ we obtain a valuation of L.

2. The unique extension of the trivial valuation of K is the trivial valuation of $R(K)$, which from now on will be excluded from consideration.

3. The extensions of equivalent valuations ϕ and $\psi = \phi^s (s > 0)$ are equivalent, i.e. $\psi^* = \phi^{*s}$. It is left to the reader to convince himself that the objects we shall associate with valuations depend effectively only on the equivalence class.

From the last proposition we obtain a commutative diagram

$$\begin{array}{ccccc} K^* & \longrightarrow & R(K) & \longrightarrow & \mathfrak{R}(K) \\ \downarrow & & \downarrow \phi^* & & \downarrow \hat{\phi} \\ \mathrm{Im}\phi & \longrightarrow & \mathbf{P} & \longrightarrow & \mathbf{P}/\mathrm{Im}\phi \end{array} \qquad (D(K, \phi)) \tag{3.1}$$

Now let $\theta : K \to K'$ be an embedding of fields and let ψ be a valuation of K' which extends the given valuation ϕ of K. We then obtain commutative diagrams

$$\begin{array}{ccccc} K^* & \longrightarrow & R(K) & \longrightarrow & \mathfrak{R}(K) \\ \downarrow & & \downarrow & & \downarrow \\ K'^* & \longrightarrow & R(K') & \longrightarrow & \mathfrak{R}(K') \end{array} \tag{3.2}$$

and

$$\begin{array}{ccccc} \mathrm{Im}\,\phi & \longrightarrow & \mathbf{P} & \longrightarrow & \mathbf{P}/\mathrm{Im}\,\phi \\ \downarrow & & \| & & \downarrow \\ \mathrm{Im}\,\psi & \longrightarrow & \mathbf{P} & \longrightarrow & \mathbf{P}/\mathrm{Im}\,\psi \end{array} \tag{3.3}$$

and we have

3.2. PROPOSITION. *The diagrams* (3.2) *and* (3.3) *define a homomorphism*

$$D(K,\ \phi) \to D(K',\ \phi')$$

of diagrams (3.1).

From now on we consider a discrete valuation ϕ of K. In this case it is preferable to use the language of "exponential valuations". The exponential valuation v, associated with ϕ, is a surjective homomorphism

$$K^* \to \mathbf{Z} \text{ (additive)}$$

extended to a map

$$K \to \mathbf{Z} \cup \infty$$

by the rule $v(0) = \infty$, and connected with ϕ by equations

$$\phi(a) = \rho^{-v(a)} \text{ for all } a \in K^*,$$

where ρ is a fixed real number > 1. Let $\mathbf{R}$ be the additive group of real numbers. Diagram (3.1) now takes on the form of a commutative diagram

$$\begin{array}{ccccc} K^* & \longrightarrow & R(K) & \longrightarrow & \mathfrak{R}(K) \\ \downarrow v & & \downarrow v^* & & \downarrow \hat{v} \\ \mathbf{Z} & \longrightarrow & \mathbf{R} & \longrightarrow & \mathbf{R}/\mathbf{Z} \end{array} \tag{3.4}$$

and we shall use the symbols v^* and $\hat{v}$ always to denote the homomorphisms given in this manner.

We now define for a radical space P of K the *ramification index* $\hat{e}(P)$ by

$$\hat{e}(P) = \text{order of } \hat{v}(P) \text{ in } \mathbf{R}/\mathbf{Z}, \tag{3.5}$$

and the *invariant* $u(P)$ as the real number with

$$\begin{cases} 0 \leq u(P) < 1, \\ \hat{v}(P) = u(P) \bmod \mathbf{Z}. \end{cases} \tag{3.6}$$

3.3. PROPOSITION. *If* $\hat{e}(P) = 1$ *then*

$$u(P) = u(P^{-1}) = 0.$$

If $\hat{e}(P)>1$ *then*

$$u(P)>0,\ u(P^{-1})>0$$

and

$$u(P)+u(P^{-1})=1.$$

Proof. Obvious.

3.4. COROLLARY. *For* $r\in Z$

$$u(P^r)+u(P^{-r})\leq u(P)+u(P^{-1}).$$

Proof. $\hat{e}(P)$ divides $\hat{e}(P^r)$. Hence if $\hat{e}(P)=1$ then $\hat{e}(P^r)=1$. Now apply the proposition.

We now give another interpretation of $u(P)$. We shall, for any non empty subset S of $R(K)\cup 0$, write

$$v^*(S)=\inf_{x\in S} v^*(x). \tag{3.7}$$

If $S=(0)$, then $v^*(S)=\infty$. If v^* is not bounded below on S, then $v^*(S)=-\infty$. Otherwise $v^*(S)\in\mathbf{R}$.

Now let

$$E_P=[x\in P\,|\,v^*(x)\geq 0]. \tag{3.8}$$

Then we have

3.5. PROPOSITION. $u(P)=v^*(E_P)$.

Proof. The set of values of v^* on P is the coset $\hat{v}(P)$ of $\mathbf{R}$ mod $\mathbf{Z}$ (cf. (3.4)), and $u(P)$ is the least positive number in that coset.

Now let again K' be an extension field of K and let ϕ' be a discrete valuation of K' extending ϕ. For the associated exponential valuations we then have a commutative diagram

$$\begin{array}{ccc} K^* & \xrightarrow{v} & \mathbf{Z} \\ \downarrow & & \downarrow e \\ K^{*\prime} & \xrightarrow{v'} & \mathbf{Z} \end{array} \tag{3.9}$$

where the natural number e is the ramification index of valuation theory.

3.6. PROPOSITION. *If* $P\in\mathfrak{R}(K)$ *then*

$$\hat{e}(PK') = \hat{e}(P)/(\hat{e}(P),\ e),$$
$$u(PK') \equiv e \cdot u(P) \pmod{\mathbf{Z}}.$$

Proof. Translating 3.2. into the language of exponential valuations, we derive from (3.9) a commutative diagram

$$\begin{array}{ccc} \mathfrak{R}(K) & \longrightarrow & \mathbf{P}/\mathbf{Z} \\ \downarrow & & \downarrow e \\ \mathfrak{R}(K') & \longrightarrow & \mathbf{P}/\mathbf{Z} \end{array}$$

which immediately yields the proposition.

3.7. COROLLARY. *If $P \in \mathfrak{R}(K'/K)$ then $\hat{e}(P)$ divides e.*

Proof. $PK' = K'$ and $\hat{e}(K') = 1$.

3.8. COROLLARY. *If $e = 1$ then*

$$\hat{e}(PK') = \hat{e}(P)$$
$$u(PK') = u(P).$$

This last Corollary applies in particular to the v-adic completion K' of K.

4. Radical modules

We consider from now on a Dedekind domain $\mathfrak{o}$. To avoid wasting time on trivialities we shall assume $\mathfrak{o}$ not to be a field. We shall then use the following notations. $\mathfrak{F}(\mathfrak{o})$ is the group of fractional ideals of $\mathfrak{o}$, always in the sense of non-zero fractional ideal. The symbol $\mathfrak{p}$ always stands for a maximal ideal of $\mathfrak{o}$. The associated exponential valuation of the quotient field K of $\mathfrak{o}$ will be denoted by $v_{\mathfrak{p}}$, and the subscript $\mathfrak{p}$ also indicates the associated objects as defined in § 3, $\mathfrak{o}_{\mathfrak{p}}$ is the valuation ring of $v_{\mathfrak{p}}$, i.e. the local ring of $\mathfrak{o}$ at $\mathfrak{p}$ (in K).

Let L be an extension field K of $\mathfrak{o}$. A *radical module of* $L/\mathfrak{o}$ is a non zero, finitely generated $\mathfrak{o}$-submodule M of some radical subspace P of L/K. M will then span P, i.e. $P = MK$. Recalling the definition of the module product in § 1, we have

4.1. THEOREM. *The radical modules in $L/\mathfrak{o}$ form an Abelian group $\mathfrak{R}(L/\mathfrak{o})$ under the module product, which contains $F(\mathfrak{o})$. The map $M \mapsto MK$ is a homomor-*

phism $\mathfrak{R}(L/\mathfrak{o}) \to \mathfrak{R}(L/K)$ *and the sequence*

$$1 \to \mathfrak{F}(\mathfrak{o}) \to \mathfrak{R}(L/\mathfrak{o}) \to \mathfrak{R}(L/K) \to 1 \tag{4.1}$$

is exact.

The map $a \mapsto a\mathfrak{o}$ *is a homomorphism* $R(L/K) \to \mathfrak{R}(L/\mathfrak{o})$ *and the diagram*

$$\begin{array}{ccc} K^* & \longrightarrow & R(L/K) \\ \downarrow & & \downarrow \quad \searrow \\ \mathfrak{F}(\mathfrak{o}) & \longrightarrow & \mathfrak{R}(L/\mathfrak{o}) \quad \nearrow \mathfrak{R}(L/K) \end{array} \tag{4.2}$$

commutes.

Proof. The following facts are immediately obvious: (i) $\mathfrak{R}(L/\mathfrak{o})$ is a commutative monoid and the maps involving it are monoid homomorphisms. (ii) $\mathfrak{F}(\mathfrak{o})$ is the inverse image in $\mathfrak{R}(L/\mathfrak{o})$ of the identity K of $\mathfrak{R}(L/K)$ under the map $\mathfrak{R}(L/\mathfrak{o}) \to \mathfrak{R}(L/K)$. (iii) The diagram (4.2) commutes. But (iii), together with the exactness of (1.1) implies that the map $\mathfrak{R}(L/\mathfrak{o}) \to \mathfrak{R}(L/K)$ is surjective. Now it follows from (i) and (ii) that $\mathfrak{R}(L/\mathfrak{o})$ is in fact a group.

The pairs $L/\mathfrak{o}$ form a category, a morphism $L/\mathfrak{o} \to L'/\mathfrak{o}'$ being given by an injective homomorphism $L \to L'$ which maps $\mathfrak{o}$ into $\mathfrak{o}'$.

4.2. Proposition. *The sequence* (4.1) *and the diagram* (4.2) *are functors of* $L/\mathfrak{o}$.

If $L \subset L'$ *then the map* $\mathfrak{R}(L/\mathfrak{o}) \to \mathfrak{R}(L'/\mathfrak{o})$ *is injective. If moreover* L *is algebraically closed in* L' *then it is surjective.*

Proof. The first assertion is obvious. For the remainder use the exactness of (4.1) together with 1.1.

In view of the last proposition we shall view the groups $\mathfrak{R}(L/\mathfrak{o})$ as embedded in the group

$$\mathfrak{R}(\mathfrak{o}) = \mathfrak{R}(\overline{K}/\mathfrak{o}),$$

$\overline{K}$ being as always an algebraic closure of K. An element of this group is a *radical module* over $\mathfrak{o}$.

We shall now establish the connection with § 3. Recalling the definition of $v_{\mathfrak{p}}^*(M)$ (cf. (3.7)) we have

4.3. Proposition. *The map* $M \mapsto v_{\mathfrak{p}}^*(M)$ *is a homomorphism* $\mathfrak{R}(\mathfrak{o}) \to \mathbf{R}$ *of groups and the diagrams*

$$\begin{array}{ccccc} \mathfrak{F}(\mathfrak{o}) & \longrightarrow & \mathfrak{R}(\mathfrak{o}) & \longrightarrow & \mathfrak{R}(K) \\ \downarrow v_{\mathfrak{p}} & & \downarrow v_{\mathfrak{p}}^* & & \downarrow \hat{v}_{\mathfrak{p}} \\ \mathbf{Z} & \longrightarrow & \mathbf{R} & \longrightarrow & \mathbf{R}/\mathbf{Z} \end{array} \tag{4.3}$$

and

$$\begin{array}{ccc} R(K) & \longrightarrow & \mathfrak{R}(\mathfrak{o}) \\ & \searrow \quad \swarrow & \\ & \mathbf{R} & \end{array} \tag{4.4}$$

commute.

Proof. By the defining property (ii) of a valuation of $R(K)$ (cf. § 3), the function $v_{\mathfrak{p}}^*$ of $R(K) \cup 0$ satisfies the relations

$$\begin{cases} v_{\mathfrak{p}}^*(\alpha+\beta) \geqq \inf v_{\mathfrak{p}}^*(\alpha),\ v_{\mathfrak{p}}^*(\beta) \\ v_{\mathfrak{p}}^*(a\alpha) = v_{\mathfrak{p}}(a) + v_{\mathfrak{p}}^*(\alpha) \end{cases} \tag{4.5}$$

for α, β in a fixed radical subspace P and for $a \in K$. It follows that if the radical module M is generated over $\mathfrak{o}$ by elements $\alpha_1, \ldots, \alpha_n$ then

$$v_{\mathfrak{p}}^*(M) = \inf_i v_{\mathfrak{p}}^*(\alpha_i). \tag{4.6}$$

As a first consequence one now deduces easily that the map $M \to v_{\mathfrak{p}}^*(M)$ is a homomorphism as indicated. Secondly one sees that $v_{\mathfrak{p}}^*(M)$ actually lies in the coset $\hat{v}_{\mathfrak{p}}(MK)$ of $\mathbf{R}$ mod $\mathbf{Z}$, i.e. that the right hand square in (4.3) commutes. The other commutativity relations are obvious.

4.4. Proposition. *Let $\alpha \in R(K)$, $M \in \mathfrak{R}(\mathfrak{o})$, $P \in \mathfrak{R}(K)$. Then for almost all $\mathfrak{p}$*

$$v_{\mathfrak{p}}^*(\alpha) = 0,\ v_{\mathfrak{p}}^*(M) = 0,\ \hat{v}_{\mathfrak{p}}(P) = 0.$$

Proof. Let $\alpha \in R(K)$, $\alpha^n \in K^*$ $(n>0)$. Then $v_{\mathfrak{p}}^*(\alpha) = 0$ whenever $v_{\mathfrak{p}}(\alpha^n) = 0$, i.e. for almost all $\mathfrak{p}$. Hence $\hat{v}_{\mathfrak{p}}(\alpha K) = 0$ for almost all $\mathfrak{p}$. To show that $v_{\mathfrak{p}}^*(M) = 0$ for almost all $\mathfrak{p}$, use (4.6).

4.5. Corollary. *For a given radical space P of K let F be the set of functions f from the maximal ideals $\mathfrak{p}$ of $\mathfrak{o}$ to the real numbers, such that*

(i) *$f(\mathfrak{p})$ lies in the coset $\hat{v}_{\mathfrak{p}}(P)$ of* $\mathbf{R}$ mod $\mathbf{Z}$

(ii) *$f(\mathfrak{p}) = 0$ for almost all $\mathfrak{p}$.*

Let furthermore G be the set of radical modules $M \subset P$. The map $M \to f_M$, where

$$f_M(\mathfrak{p}) = v_{\mathfrak{p}}^*(M),$$

is a bijection $G \to F$.

Proof. That $f_M \in F$ follows from 4.3 and 4.4. If $f_M = f_N$ then $MN^{-1} \in \mathfrak{F}(\mathfrak{o})$ and, by 4.3, $v_\mathfrak{p}(MN^{-1}) = 0$ for all $\mathfrak{p}$, i.e. $MN^{-1} = \mathfrak{o}$ and so $M = N$. Thus $M \mapsto f_M$ is an injection. To see that it is also a surjection, consider a function $f \in F$. Choose some $M \in G$ and let I be the fractional ideal with

$$v_\mathfrak{p}(I) = f(\mathfrak{p}) - v_\mathfrak{p}^*(M).$$

Then $f = f_N$ for $N = MI$.

We now consider the localisation maps $g_\mathfrak{p} : \mathfrak{R}(\mathfrak{o}) \to \mathfrak{R}(\mathfrak{o}_\mathfrak{p})$. In the direct product $\prod_\mathfrak{p} \mathfrak{R}(\mathfrak{o}_\mathfrak{p})$ (over all $\mathfrak{p}$) we single out the elements N with the following properties: (i) There is a radical subspace P dependent on N, but not on $\mathfrak{p}$, so that the $\mathfrak{p}$-components $N(\mathfrak{p})$ are all contained in P, (ii) for almost all $\mathfrak{p}$, $v_\mathfrak{p}^*(N(\mathfrak{p})) = 0$. These elements form a group $\prod^* \mathfrak{R}(\mathfrak{o}_\mathfrak{p})$. From 4.3 and 4.5 we then have

4.6. COROLLARY. *The localisation maps $g_\mathfrak{p}$ give rise to an isomorphism*

$$\mathfrak{R}(\mathfrak{o}) \cong \prod^* \mathfrak{R}(\mathfrak{o}_\mathfrak{p}).$$

5. Divisibility

The groups $R(K)$ and $\mathfrak{R}(K)$ are divisible, but the group $\mathfrak{R}(\mathfrak{o})$ presents genuine divisibility problems, which will be dealt with in the present section. Recall that an element g of an Abelian group G is said to be *divisible* by the natural number n if $g \in G^n$.

We shall write $\mathfrak{C}(\mathfrak{o})$ for the ideal class group of $\mathfrak{o}$, i.e. for the cokernel of the map $K^* \to \mathfrak{F}(\mathfrak{o})$.

5.1. THEOREM. *There is a unique homomorphism*

$$cl : \mathfrak{R}(\mathfrak{o}) \to \mathfrak{C}(\mathfrak{o})$$

which makes the diagram

(5.1)
$$\begin{array}{ccccccc} R(K) & \longrightarrow & \mathfrak{R}(\mathfrak{o}) & \longrightarrow & \mathfrak{C}(\mathfrak{o}) & \longrightarrow & 1 \\ & & \uparrow & \nearrow & & & \\ & & \mathfrak{F}(\mathfrak{o}) & & & & \end{array}$$

commutative, and its row exact.

A radical module M is divisible in $\mathfrak{R}(\mathfrak{o})$ by n if and only if $cl(M)$ is divisible

in $\mathfrak{C}(\mathfrak{o})$ *by* n.

Proof. The first part follows from the exactness of the sequences (1.1) and (4.1) and the commutativity of (4.2). The second part follows from the exactness of the row in (5.1) and the fact that $R(K)$ is a divisible group.

One can identify the map $cl : \mathfrak{R}(\mathfrak{o}) \to \mathfrak{C}(\mathfrak{o})$ in module theoretic terms. In fact $cl(M)$ is precisely the Steinitz invariant of M, which occurs in the theory of finitely generated, projective $\mathfrak{o}$-modules.

5.2. COROLLARY. *A fractional ideal* I *of* $\mathfrak{o}$ *is* n*-th power of a radical module if and only if* $cl(I)$ *is* n*-th power of an ideal class.*

Using 4.6 one can restate this criterion for $cl(I)$ to be an n-th power in almost entirely local terms.

5.3. COROLLARY. $cl(I)$ *is an* n*-th power if and only if there exists a radical space* $P \in \mathfrak{R}(K)$, *and for each* $\mathfrak{p}$ *a radical module* $M(\mathfrak{p}) \in \mathfrak{R}(\mathfrak{o}_\mathfrak{p})$ *so that*

$$KM(\mathfrak{p}) = P$$

and

$$M(\mathfrak{p})^n = I\mathfrak{o}_\mathfrak{p}.$$

For, the last equation will then also imply that, for almost all $\mathfrak{p}$, $v_\mathfrak{p}^*(M(\mathfrak{p})) = 0$.

As an illustration we give yet another proof of the theorem on the ideal class of a discriminant. (In the case of algebraic number fields see ([5] Th. 177), for the general case see [1], and [6] (Ch. III, § 2).)

5.4. PROPOSITION. *Let* L *be a finite, separable, algebraic extension field of* K *and let* $\mathfrak{d}$ *be the discriminant over* $\mathfrak{o}$ *of the integral closure of* $\mathfrak{o}$ *in* L. *Then* $cl(\mathfrak{d})$ *is a square.*

Proof. Let σ_i run through the distinct homomorphisms of L into the algebraic closure $\overline{K}$ which leave K element wise fixed and let $t : L \to K$ be the trace. If $\{\alpha_k\}$ is a K-basis of L we have the determinantal equation

$$(\det(\alpha_k\sigma_i))^2 = \det t(\alpha_k\alpha_j). \tag{5.2}$$

The K-module $P = K \det(\alpha_k\sigma_i)$ does not depend on the choice of basis, and by (5.2) $P^2 = K$.

Now choose in particular $\{\alpha_k\}$ as an $\mathfrak{o}_\mathfrak{p}$-basis of the integral closure of $\mathfrak{o}_\mathfrak{p}$

in L. Then

$$M(\mathfrak{p}) = \mathfrak{o}_\mathfrak{p} \det(\alpha_k \sigma_i)$$

is a radical module in $\mathfrak{R}(\mathfrak{o}_\mathfrak{p})$ with

$$KM(\mathfrak{p}) = P,$$

which by (5.2) satisfies the equation

$$M(\mathfrak{p})^2 = \mathfrak{d}\mathfrak{o}_\mathfrak{p}.$$

Now apply 5.3, to get the Proposition.

6. Integral radical modules and the conductor of a radical space

We are here concerned with arithmetic properties of radical modules. This will lead us to a function which associates with every radical space P an ideal $\hat{f}(P)$ of $\mathfrak{o}$.

A radical module M is *integral* if its elements are integral (over $\mathfrak{o}$), i.e. if all $\mathfrak{p}$, $v_\mathfrak{p}^*(M) \geqq 0$. These modules form a monoid, generating $\mathfrak{R}(\mathfrak{o})$.

6.1. THEOREM. *Each radical subspace P contains a unique maximal integral radical module*

$$E_P = [\alpha \in P \mid v_\mathfrak{p}^*(\alpha) \geqq 0 \text{ for all } \mathfrak{p}], \tag{6.1}$$

with values

$$v_\mathfrak{p}^*(E_P) = u_\mathfrak{p}(P). \tag{6.2}$$

The product

$$\hat{f}(P) = E_P E_{P^{-1}} \tag{6.3}$$

is a square free integral ideal of $\mathfrak{o}$. A maximal ideal $\mathfrak{p}$ divides $\hat{f}(P)$ if and only if $e_\mathfrak{p}(P) > 1$, i.e. $v_\mathfrak{p}^*(E_P) > 0$.

For $r \in \mathbf{Z}$, $\hat{f}(P^r)$ divides $\hat{f}(P)$. In particular if P and Q generate the same cyclic subgroup of $\mathfrak{R}(K)$ then $\hat{f}(P) = \hat{f}(Q)$.

Proof. By the definition of $u_\mathfrak{p}(P)$ (cf. (3.6)) this lies in the coset $\hat{v}_\mathfrak{p}(P)$ of $\mathbf{R}$ mod $\mathbf{Z}$ and, by 4.4, $u_\mathfrak{p}(P) = 0$ for almost all $\mathfrak{p}$. Hence by 4.5 the equations (6.2) determine a unique radical module $E_\mathfrak{p}$, which by 3.5 satisfies (6.1.).

The remainder of the theorem now follows from the fact that $E_P E_{P^{-1}} \in \mathfrak{F}(\mathfrak{o})$ and from 3.3 and 3.4.

$\hat{f}(P)$ is called the *conductor of P over $\mathfrak{o}$*.

6.2. PROPOSITION. (i) *$\hat{f}(P)\mathfrak{o}_\mathfrak{p}$ is the conductor of P over $\mathfrak{o}_\mathfrak{p}$.*

(ii) *If $K_\mathfrak{p}$ is the $\mathfrak{p}$-adic completion of K and $\bar{\mathfrak{o}}_\mathfrak{p}$ its valuation ring, then $\hat{f}(P)\bar{\mathfrak{o}}_\mathfrak{p}$ is the conductor of $P\bar{\mathfrak{o}}_\mathfrak{p}$ over $\bar{\mathfrak{o}}_\mathfrak{p}$.*

Proof. (i) follows from 4.6 and (ii) from 3.8.

7. Units and torsion

We now establish a connection between the arithmetic properties of $\mathfrak{R}(\mathfrak{o})$ and its torsion properties.

A radical module M is a *unit* if both M and M^{-1} are integral.

7.1. THEOREM. *Each unit radical module is of form E_P.*

The unit radical modules form a sub-group $\mathfrak{U}(\mathfrak{o})$ of $\mathfrak{R}(\mathfrak{o})$, and

$$\mathfrak{U}(\mathfrak{o}) = \bigcap_\mathfrak{p} \operatorname{Ker} v_\mathfrak{p}^*. \tag{7.1}$$

The homomorphism

$$\mathfrak{U}(\mathfrak{o}) \to \mathfrak{R}(\mathfrak{o}) \to \mathfrak{R}(K)$$

gives rise to an isomorphism

$$\mathfrak{U}(\mathfrak{o}) \cong \bigcap_\mathfrak{p} \operatorname{Ker} \hat{v}_\mathfrak{p}. \tag{7.2}$$

$\mathfrak{U}(\mathfrak{o})$ *coincides with the torsion group of* $\mathfrak{R}(\mathfrak{o})$.

Proof. M is a unit if and only if for all $\mathfrak{p}$.

$$v_\mathfrak{p}^*(M) \geqq 0,\ v_\mathfrak{p}^*(M^{-1}) \geqq 0,$$

i.e.

$$v_\mathfrak{p}^*(M) = 0.$$

This immediately yields (7.1) and the fact that a unit is of form E_P.

The group $\mathfrak{U}(\mathfrak{o}) \cap \mathfrak{F}(\mathfrak{o})$ is trivial. Hence by the exactness of (4.1) the map $\mathfrak{U}(\mathfrak{o}) \to \mathfrak{R}(K)$ is injective, and by (7.1) and the commutativity of (4.3) its image is contained in $\bigcap_\mathfrak{p} \operatorname{Ker} \hat{v}_\mathfrak{p}$. On the other hand if $\hat{v}_\mathfrak{p}(P) = 0$ for all $\mathfrak{p}$, then $u_\mathfrak{p}(P) = 0$ and so by (6.2) E_P is a unit whose image is P. We have thus established the isomorphism (7.2).

We know in particular that $\mathfrak{U}(\mathfrak{o})$ admits an injection into the torsion group $\mathfrak{R}(K)$ and is thus itself a torsion group. Conversely each $v_\mathfrak{p}^*$ induces a homo-

morphism of the torsion group of $\mathfrak{R}(\mathfrak{o})$ into $\mathbf{R}$, which must be null. Hence by (7.1) the torsion group of $\mathfrak{R}(\mathfrak{o})$ is contained in $\mathfrak{U}(\mathfrak{o})$, and so coincides with $\mathfrak{U}(\mathfrak{o})$.

8. Ramification of pure extensions

In this section we consider a separable, finite, pure extension $L = K(\mathfrak{G})$ of K by a subgroup $\mathfrak{G}$ of $\mathfrak{R}(K)$. The degree $(L : K)$ is then not a multiple of the characteristic of K, and we may thus view it as an ideal of $\mathfrak{o}$. The integral closure of $\mathfrak{o}$ in L will be denoted by $\mathfrak{O}$ and, in keeping with tradition, the discriminant of $\mathfrak{O}$ over $\mathfrak{o}$ by $\mathfrak{d}(L/K)$. The symbol $\mathfrak{P}$ stands for maximal ideals of $\mathfrak{O}$, and $e_{\mathfrak{P}}$ denotes the ramification index relative to $\mathfrak{P} \cap \mathfrak{o} = \mathfrak{p}$. The residue class field extension $\mathfrak{O}/\mathfrak{P}$ of $\mathfrak{o}/\mathfrak{p}$ is not assumed to be separable. If it is, and if the characteristic of $\mathfrak{o}/\mathfrak{p}$ does not divide $e_{\mathfrak{P}}$ then $\mathfrak{P}$ is said to be *tamely ramified* (over K).

By abuse of notation we write

$$\hat{\mathfrak{d}}(L/K) = \prod_{P \in \mathfrak{G}} \hat{f}(P), \tag{8.1}$$

and

$$\hat{e}_{\mathfrak{p}}(L/K) = \sup_{P \in \mathfrak{G}} \hat{e}_{\mathfrak{p}}(P). \tag{8.2}$$

$\hat{\mathfrak{d}}(L/K)$, as well as $\mathfrak{d}(L/K)$, is an integral ideal of $\mathfrak{o}$.

The sum

$$\hat{\mathfrak{O}} = \sum_{P \in \mathfrak{G}} E_P \tag{8.3}$$

of $\mathfrak{o}$-submodules of L is direct. $\mathfrak{O}$ is a finitely generated $\mathfrak{o}$-module which spans L over K, and hence the module index $[\mathfrak{O} : \hat{\mathfrak{O}}]$ is defined, (cf. [2], [4]). It is an integral ideal, as clearly $\hat{\mathfrak{O}} \subset \mathfrak{O}$. In fact $\hat{\mathfrak{O}}$ is an order of $\mathfrak{o}$ in L.

8.1. THEOREM. (i) $\mathfrak{d}(L/K)\,([\mathfrak{O} : \hat{\mathfrak{O}}]^2) = \hat{\mathfrak{d}}(L/K)((L : K)^{(L:K)})$.

In particular

$\mathfrak{d}(L/K)$ *divides* $\hat{\mathfrak{d}}(L/K)((L : K)^{(L:K)})$.

(ii) $\hat{\mathfrak{d}}(L/K)$ *divides* $\mathfrak{d}(L/K)$

and

$[\mathfrak{O} : \hat{\mathfrak{O}}]^2$ *divides* $(L : K)^{(L:K)}$

(iii) *The following conditions are equivalent*

(a) *Each maximal ideal* $\mathfrak{P}$ *of* $\mathfrak{O}$ *is tamely ramified over* K.

(b) $\hat{\mathfrak{d}}(L/K) = \mathfrak{d}(L/K)$

(c) $[\mathfrak{O} : \hat{\mathfrak{O}}]^2 = (L : K)^{(L:K)}$

(iv) *If* $\mathfrak{P}$ *is a maximal ideal of* $\mathfrak{O}$ *with* $\mathfrak{P} \cap \mathfrak{o} = \mathfrak{p}$ *then*

$$\hat{e}_{\mathfrak{p}}(L/K) \text{ divides } e_{\mathfrak{P}}.$$

If all $\mathfrak{P}$ *are tamely ramified over* K *then*

$$\hat{e}_{\mathfrak{p}}(L/K) = e_{\mathfrak{P}}.$$

Proof. Without loss of generality we may assume $\mathfrak{o}$ to be a local ring with the single non zero prime ideal $\mathfrak{p}$. We shall first establish a series of Lemmas. The residue class degree of a maximal ideal $\mathfrak{P}$ of $\mathfrak{O}$ in L/K will be denoted by $f_{\mathfrak{P}}$ and the natural numbers $r_{\mathfrak{P}}$ are defined by the equations

$$v_{\mathfrak{P}}(\mathfrak{D}) = r_{\mathfrak{P}} - 1$$

for the values of the different $\mathfrak{D}$ of $\mathfrak{O}/\mathfrak{o}$.

8.2. LEMMA. $v_{\mathfrak{p}}(\mathfrak{d}(L/K)) = \sum_{\mathfrak{P}} f_{\mathfrak{P}}(r_{\mathfrak{P}} - 1)$.

Proof. Standard.

8 3. LEMMA. $r_{\mathfrak{P}} \geqq e_{\mathfrak{P}}$, *with equality holding if and only if* $\mathfrak{P}$ *is tamely ramified.*

For a proof without hypothesis on the separability of residue class field extensions see e.g. [4].

Let in the sequel g denote the order of the kernel of the map $\mathfrak{G} \to \mathbf{R}/\mathbf{Z}$ induced by $\hat{v}_{\mathfrak{p}}$.

8.4. LEMMA. $\hat{e}_{\mathfrak{p}}(L/K)$ *divides* $e_{\mathfrak{P}}$ *and* $g \geqq \sum_{\mathfrak{P}} f_{\mathfrak{P}}$.

Also

$$g = \sum_{\mathfrak{P}} f_{\mathfrak{P}}$$

if and only if

$$\hat{e}_{\mathfrak{p}}(L/K) = e_{\mathfrak{P}}$$

for all $\mathfrak{P}$.

Proof. $\hat{e}_{\mathfrak{p}}(L/K)$ is the order of $\mathrm{Im}\,[\mathfrak{G} \to \mathbf{R}/\mathbf{Z}]$. By 3.7, $\hat{e}_{\mathfrak{p}}(L/K)$ thus divides $e_{\mathfrak{P}}$. By 2.2,

$$\hat{e}_{\mathfrak{p}}(L/K)\, g = (L : K) (= |\mathfrak{G}|).$$

Also

$$\sum_{\mathfrak{P}} e_{\mathfrak{P}} f_{\mathfrak{P}} = (L : K).$$

Hence

$$g = \sum_{\mathfrak{P}} (e_{\mathfrak{P}}/\hat{e}_{\mathfrak{p}}(L/K)) f_{\mathfrak{P}}.$$

The Lemma now easily follows from this formula.

8.5. LEMMA.

$$v_{\mathfrak{p}}(\hat{\mathfrak{d}}(L/K)) = (L : K) - g.$$

Proof. By 6.1, the conductor $\hat{f}(P)$ has value $\mathfrak{o}$ for precisely g of the spaces P, and has value $\mathfrak{p}$ for the other $(L : K) - g = |\mathfrak{G}| - g$ spaces.

Let $\mathfrak{H}$ be a subgroup of $\mathfrak{G}$. By 2.1, $L_1 = K(\mathfrak{H})$ is a subfield of L, containing K, and if $\overline{\mathfrak{G}}$ is the image of $\mathfrak{G}$ in $\mathfrak{R}(L_1)$ then $L = L_1(\overline{\mathfrak{G}})$ is a pure extension of L_1 by $\overline{\mathfrak{G}}$. In this situation we have

8.6. LEMMA. *If L_1/K is non ramified then*

$$\hat{\mathfrak{d}}(L/K) = N_{L_1/K}\, \hat{\mathfrak{d}}(L/L_1)$$

where $N_{L_1/K}$ is the ideal norm.

Proof. The elements Q of $\overline{\mathfrak{G}}$ are the spaces PL_1 ($P \in \mathfrak{G}$), each counted $|\mathfrak{H}| = (L_1 : K)$ times (cf. 2.1). Therefore

$$\hat{\mathfrak{d}}(L/L_1)^{(L_1:K)} = \prod_{\mathfrak{G}} \hat{f}(PL_1). \tag{8.4}$$

Now consider a fixed space $P \in \mathfrak{G}$. Let $\mathfrak{O}_1$ be the integral closure of $\mathfrak{o}$ in L_1. If $\bar{\mathfrak{p}}$ is a maximal ideal of $\mathfrak{O}_1$ then its ramification index over $\mathfrak{p}$ has value 1 and consequently, by 3.8,

$$\hat{e}_{\bar{\mathfrak{p}}}(PL_1) = \hat{e}_{\mathfrak{p}}(P).$$

By 6.1, this implies that

$$v_{\bar{\mathfrak{p}}}(\hat{f}(PL_1)) = v_{\mathfrak{p}}(f(P)).$$

This being true for all $\bar{\mathfrak{p}}$, we now deduce from the equation

$$\prod \bar{\mathfrak{p}} = \mathfrak{p}\mathfrak{O}_1$$

that

$$f(PL_1) = f(P)\mathfrak{O}_1.$$

Hence

$$\prod_{\mathfrak{G}} f(PL_1) = \hat{\mathfrak{d}}(L/K)\mathfrak{O}_1.$$

Comparing with (8.4) and taking norms we obtain

$$N_{L_1/K}(\hat{\mathfrak{d}}(L/L_1))^{(L_1:K)} = N_{L_1/K}(\hat{\mathfrak{d}}(L/K)\mathfrak{O}_1) = \hat{\mathfrak{d}}(L/K)^{(L_1:K)}$$

and this gives us the Lemma.

Now we return to the proof of the theorem. Note that the first assertion under (iv) is contained in 8.4.

Let t be the trace $L \to K$, $\{\beta_i\}$ a free $\mathfrak{o}$-basis of $\mathfrak{O}$ and select for each P an element α_P so that $E_P = \mathfrak{o}\alpha_P$. Then the α_P form a free $\mathfrak{o}$-basis of $\hat{\mathfrak{O}}$. It follows (cf. [4]) that the determinant quotient

$$(\det t(\beta_i\beta_j))^{-1} \det t(\alpha_P\alpha_Q)$$

generates the ideal $[\mathfrak{O} : \hat{\mathfrak{O}}]^2$. Also

$$\mathfrak{o} \det t(\beta_i\beta_j) = \mathfrak{d}(L/K).$$

To establish 8.1 (i) we shall have to show that

$$\mathfrak{o} \det t(\alpha_P\alpha_Q) = \hat{\mathfrak{d}}(L/K)((L : K)^{(L:K)}). \tag{8.5}$$

In fact, if $PQ \neq K$ then

$$t(\alpha_P\alpha_Q) = 0,$$

while on the other hand

$$\mathfrak{o}\alpha_P\alpha_{P^{-1}} = \hat{f}(P),$$

and so

$$\mathfrak{o}t(\alpha_P\alpha_{P^{-1}}) = \hat{f}(P)(L : K).$$

The last equation implies (8.5).

To establish (ii), we recall that $\sum e_{\mathfrak{P}}f_{\mathfrak{P}} = (L : K)$, and get

$$\begin{aligned} v_{\mathfrak{p}}(\mathfrak{d}(L/K)) &= \sum_{\mathfrak{P}} f_{\mathfrak{P}}(r_{\mathfrak{P}} - 1) && \text{(by 8.2)} \\ &\geqq \sum_{\mathfrak{P}} f_{\mathfrak{P}}(e_{\mathfrak{P}} - 1) && \text{(by 8.3)} \\ = (L : K) - \sum_{\mathfrak{P}} f_{\mathfrak{P}} &\geqq (L : K) - g && \text{(by 8.4)} \\ &= v_{\mathfrak{p}}(\hat{\mathfrak{d}}(L/K)) && \text{(by 8.5)} \end{aligned}$$

Thus $\hat{\mathfrak{d}}(L/K)$ divides $\mathfrak{d}(L/K)$, and by (i) $[\mathfrak{O} : \hat{\mathfrak{O}}]^2$ will divide $(L : K)^{(L:K)}$. Moreover this string of inequalities, in conjunction with the criteria for equality in 8.3 and 8.4, shows that the equation $\hat{\mathfrak{d}}(L/K) = \mathfrak{d}(L/K)$ implies firstly that each maximal ideal $\mathfrak{P}$ of $\mathfrak{O}$ is tamely ramified, and secondly that always $\hat{e}_{\mathfrak{p}}(L/K)$

$= e_{\mathfrak{P}}$. As by (i) the conditions (b) and (c) are clearly equivalent, it only remains for us to show that (a) implies (b).

Assume then that all maximal ideals of $\mathfrak{O}$ are tamely ramified over K. If $\mathfrak{o}/\mathfrak{p}$ is of prime characteristic p let $\mathfrak{H}$ be the p-Sylowgroup of $\mathfrak{G}$, otherwise let $\mathfrak{H} = 1$. The maximal ideals of the integral closure of $\mathfrak{o}$ in $L_1 = K(\mathfrak{H})$ are tamely ramified over K. In the case when $\mathfrak{o}/\mathfrak{p}$ has prime characteristic p, $(L_1 : K)$ is a power of p. Therefore L_1 is non ramified over K. The same is trivially true when $\mathfrak{o}/\mathfrak{p}$ has characteristic zero. Thus $\mathfrak{d}(L_1/K) = \mathfrak{o}$, and hence by the tower formula for discriminants

$$\mathfrak{d}(L/K) = N_{L_1/K}\,\mathfrak{d}(L/L_1). \tag{8.6}$$

By 8.6,

$$\hat{\mathfrak{d}}(L/K) = N_{L_1/K}\,\hat{\mathfrak{d}}(L/L_1). \tag{8.7}$$

On the other hand, the degree $(L : L_1) = |\mathfrak{G}/\mathfrak{H}|$ is not a multiple of the residue class field characteristic and hence

$$\hat{\mathfrak{d}}(L/L_1) = \hat{\mathfrak{d}}(L/L_1)((L : L_1)^{(L:L_1)}).$$

By the divisibility relations under (i) and (ii) it then follows that

$$\hat{\mathfrak{d}}(L/L_1) = \mathfrak{d}(L/L_1)$$

and hence by (8.6), (8.7) that

$$\hat{\mathfrak{d}}(L/K) = \mathfrak{d}(L/K).$$

Literature

[1] A. Fröhlich, Discriminants of algebraic number fields, Math. Z., **74**, 18-28 (1960).
[2] A. Fröhlich, Ideals in an extension field as modules over the algebraic integers in a finite number field, Math Z., **74**, 28-38 (1960).
[3] A. Fröhlich, The module structure of Kummer extensions over Dedekind domains, Journ. f.d. reine u. ang. Math., **209**, 39-53 (1962).
[4] Local fields, Proceedings of the Summer school on algebraic number theory, Brighton 1965, to be published by Academic Press.
[5] E. Hecke, Algebraische Zahlen, 1923.
[6] J-P. Serre, Corps locaux, 1962.
[7] Zariski-Samuel, Commutative algebra, Vol. I, 1958.

King's College, London