

A GENERALIZATION OF THE RIEMANN-ROCH THEOREM

BY
H. F. MATTSON

1. Introduction

In this paper¹ a Riemann-Roch theorem is proved for a module, over a function field K , which is under the action of simple algebras over K . Specialization of this module leads on one hand to the Riemann-Roch theorem of E. Witt [16] for simple algebras over K , and on the other hand to an extension of A. Weil's Riemann-Roch theorem for matrices over function fields [15], in the case that his "signature" is taken to be identically 1. In each case the constant field is allowed to be arbitrary.

There is also a brief account (in §2), partly new in method, of the arithmetic of simple algebras over K . In §3 our generalization of the Riemann-Roch theorem is proved for a certain module over the function field K . In §4 this module is taken to be a simple algebra A over K ; a restriction of the definition of divisor then leads to a suitably specific form of the Riemann-Roch theorem for A . Related questions—the different, the Riemann-Hurwitz formula, and a genus-like invariant of A —are then discussed. Finally, in §5, it is shown that our Riemann-Roch theorem for A implies that of Witt [16]. The paper concludes with a theorem extending the generalized Riemann-Roch theorem of Weil [15] (when his "signature" is trivial) for matrices over function fields.

Part of the origin of this kind of investigation is in the papers of Hecke [7, 8], Chevalley and Weil [3], and Weil [14], which are concerned with the problem of decomposing into its irreducible parts a certain natural representation of $G/H(N)$, where G is the modular group and $H(N)$ the subgroup of matrices congruent (mod N) to the identity, as linear transformations of the space of "cusp forms" of type $(2, N)$. Since there is a natural isomorphism between this space of cusp forms and the differentials of the first kind of the associated function field $K_{H(N)}$, the problem can be transformed to one in terms of matrices over $K_{H(N)}$.

The methods used here are those of linear topology and duality, first applied to this kind of problem by K. Iwasawa in [10] and particularly [9]. The proofs in §3 are direct generalizations of the proofs of Iwasawa for the corresponding theorems about K . Indeed, much of this paper may be thought of as the tensor product of the appropriate spaces over K with [9].

I wish to thank Professor Iwasawa for suggesting to me the problems dealt with here. As I have indicated, his works [9] and [10] made these problems

Received April 22, 1959; received in revised form August 18, 1960.

¹ This paper is an extension of the author's Ph.D. thesis, submitted to Massachusetts Institute of Technology in May, 1955. Part of the work on this paper was done while the author was employed at the Air Force Cambridge Research Center, Bedford, Massachusetts.

easy to solve. I have also profited from several discussions with Professor Iwasawa and with my friend Peter Schweitzer, from whom I have received valuable advice and encouragement. Finally, I wish to thank the referee for several very helpful suggestions.

For the preliminaries, let K denote a function field² with field of constants F . Let \mathfrak{M} denote the set of prime divisors of K , ν_P the normalized exponential valuation belonging to $P \in \mathfrak{M}$, K_P the completion of K with respect to P , $\mathfrak{o}_P \subset K_P$ the ring of local integers, \mathfrak{p}_P the local prime ideal, $\mathfrak{R}_P = \mathfrak{o}_P/\mathfrak{p}_P$ the residue-class-field, and $n_P = [\mathfrak{R}_P:F]$ the local degree.

The ring R of valuation vectors of K is defined as the weak direct sum of the K_P in the sense that for almost all P , the component a_P of the valuation vector a must belong to \mathfrak{o}_P . In R we define the subring \mathfrak{o} as the direct sum of the \mathfrak{o}_P . We then take the set of all $a\mathfrak{o}$, where a runs through the regular elements of R , as a fundamental system of neighborhoods of 0 in R , defining thereby a linear topology³ on R , under which R even becomes a topological ring. K is a discrete subfield of R ; and there exists an open linearly compact subspace W such that $R = K + W$, a topological direct sum (cf. [9, 10]). A character of R is a continuous, F -linear mapping of R into F , F having the discrete topology. The space $X(R)$ of all such characters, with the (linearly) compact-open topology, is a linearly topologized vector space over F . A nontrivial character of R which vanishes on K will be called an *admissible* character of R . If χ is such a character, then a fundamental result of [9, 10] is that R is self-dual under the pairing $(a, b) = \chi(ab)$, $a, b \in R$.

We shall so often need the following result from the theory of linear topologies that we state it here as

LEMMA 1.1. *A linearly topologized space is finite-dimensional if and only if it is linearly compact and discrete.*

Let S_0 be a skew-field of finite rank over the center K . For each prime divisor P of K , define S_{0P} to be the tensor product $K_P \otimes S_0$ over K . Then, although S_{0P} is not always a skew-field, it is a normal simple algebra with K_P as center.⁴ As such, S_{0P} is isomorphic to the full $\mu_P \times \mu_P$ matrix algebra over some skew-field S_P with K_P as center; and S_P is uniquely determined up to a K_P -isomorphism.

The valuation ν_P of K_P can be extended uniquely to S_P , via, for instance, the norm of the regular representation of S_P/K_P . We denote by ν_P the

² By the term "function field," we mean a field K , containing a subfield F , (relatively) algebraically closed in K , and containing an element x not in F , such that $K/F(x)$ has finite degree.

³ A vector space over F is linearly topologized if its additive group is a topological group for which some collection of linear subspaces serves as a fundamental system of neighborhoods of 0 . For the theory of such spaces, including the duality theorem, see Lefschetz [11, pp. 72-83]. The analogue of the "second isomorphism theorem" for these spaces is proved in [9].

⁴ For the structure theory of algebras assumed in this paper, see, for example, [2].

uniquely determined normalized exponential valuation of S_P which results from this extension. S_P is complete with respect to v_P . We have the result that $[S_P:K_P] = e_P f_P$, where e_P is the local ramification index and f_P the local rank of S_P/K_P . We define \mathcal{O}_P to be the ring of elements in S_P with non-negative valuation, \mathfrak{P}_P to be the maximal ideal of non-units in \mathcal{O}_P , and $\mathfrak{S}_P = \mathcal{O}_P/\mathfrak{P}_P$, the local skew-field at P . \mathfrak{S}_P is of finite rank f_P over \mathbb{R}_P .

It will also be useful to recall the following well-known result from the theory of valuations: Let $w_1, \dots, w_f \in \mathcal{O}_P$ be representatives of a basis of $\mathfrak{S}_P/\mathbb{R}_P$, and let $t \in S_P$ be a prime element for P , i.e., $v_P(t) = 1$. Then we have

LEMMA 1.2.⁵ *The $e_P f_P$ elements $w_i t^j$, with $1 \leq i \leq f_P$ and $0 \leq j \leq e_P - 1$, form a basis of S_P/K_P ; and if $a \in S_P$ is written $a = \sum a_{ij} w_i t^j$, with $a_{ij} \in K_P$, then, for every integer m , $v_P(a) \geq m e_P$ if and only if all $v_P(a_{ij}) \geq m$.*

LEMMA 1.3. *If the skew-field S_P has rank $m_P'^2$ over the center K_P , then $e_P \mid m_P'$ and $m_P' \mid f_P$, [18].*

Proof. If t is a prime element for P , then $K_P(t)/K_P$ has ramification index e_P , which divides its degree, which in turn divides m_P' [1, p. 53]. Since $e_P \mid m_P'$, we have $m_P'^2 = e_P f_P$ dividing $m_P' f_P$, or $m_P' \mid f_P$.

Let A be an algebra over the center k . The reduced trace T of A/k is always nontrivial if A is semisimple (in fact, the discriminant is nonzero).⁶ In particular, T is a k -linear mapping of A to k such that $T(ab) = T(ba)$ for all $a, b \in A$.

2. The arithmetic of simple algebras over function fields

In this section we present a brief account of the maximal orders⁷ and ideals of a normal simple algebra A over K . The results are known (cf. [5] and [12]), but some of the present proofs are simpler than the older ones.

We first define the ring \tilde{A} of valuation vectors of A as the tensor product $\tilde{A} = R \otimes A$ of R and A over K . If u_1, \dots, u_n is a basis of A/K , then $\tilde{A} = R \otimes u_1 + \dots + R \otimes u_n$; thus we may give \tilde{A} the linear topology of a direct sum of copies of R . This topology makes \tilde{A} a topological ring and is independent of the basis of A/K chosen above.

Let x be an element of K not in F . Call a prime divisor P of K *finite* if $v_P(x) \geq 0$. An order of A relative to $F[x]$ is a subring of A , finitely generated over $F[x]$, containing $F[x]$, and spanning $A/F(x)$. In this section Q will always denote that prime divisor of $F(x)$ obtained by projecting to $F(x)$ that $P \in \mathfrak{M}$ which is mentioned in the same context as Q . R_0 is defined as the ring of valuation vectors of $F(x)$, \mathfrak{o}_0 the ring of integers of R_0 , and \mathfrak{o}_Q the local integers of the completion $F(x)_Q$. One of the basic results of the

⁵ See, for example, the proof of Theorem 5, p. 61, of [17].

⁶ For the definition and properties of the reduced trace, see [1, pp. 122-125].

⁷ An account of orders and their ideals will be found in [4, Ch. VI].

classical theory is that R is topologically isomorphic to the tensor product $R_0 \otimes K$ over $F(x)$, the latter having the direct-sum topology; we write⁸

$$(2.1) \quad R = R_0 \otimes_{F(x)} K.$$

We now prove, letting \tilde{A}_P denote $K_P \otimes A$, the P -component of \tilde{A} ,

THEOREM 2.1. *The maximal orders of \tilde{A}_P relative to \mathfrak{o}_P are the same as those relative to \mathfrak{o}_Q and consist of all the maximal open linearly compact subrings of \tilde{A}_P .*

Proof. Let L be a maximal open linearly compact subring of \tilde{A}_P . Then $L + \mathfrak{o}_P + \mathfrak{o}_P L$ is an open linearly compact subring of \tilde{A}_P , so that $L \supset \mathfrak{o}_Q$. L spans \tilde{A}_P/K_P since it is open, and L is finitely generated over \mathfrak{o}_P by Lemma 1.1.

Conversely, if E is a maximal order of \tilde{A}_P for \mathfrak{o}_P , then E is trivially open and is linearly compact as a finitely generated space over \mathfrak{o}_P . If $L \supset E$ is an open linearly compact subring, then by the previous argument L is an order of \tilde{A}_P , since we used the maximality only to prove $L \supset \mathfrak{o}_P$. Therefore $L = E$, Q.E.D.

We now investigate the relation between the orders of $A/F(x)$ and those of $\tilde{A}_P/F(x)_Q$. We state but do not prove

LEMMA 2.1. *If J is an order of A relative to $F[x]$ and P a finite prime, then the closure L of J in \tilde{A}_P is an open linearly compact subring of \tilde{A}_P containing \mathfrak{o}_Q .*

LEMMA 2.2. *If J is a maximal order of A relative to $F[x]$ and P a finite prime, then the closure L of J in \tilde{A}_P is a maximal order of \tilde{A}_P .*

Proof. By the previous lemma, we know that L is an order of \tilde{A}_P . To prove L maximal, let L' be an order of \tilde{A}_P containing L . Following [5] and [12], we define J' as the set of all $a \in A \cap L'$ such that for some integer α , $p(x)^\alpha a \in J$, where $p(x)$ is the irreducible polynomial from $F[x]$ giving rise to the prime divisor Q . Notice that J' is a subring of A containing J and hence spanning $A/F(x)$. Also, for some integer $\beta > 0$, we have $J' \subset p(x)^{-\beta} J$, since J' is contained in the linearly compact subspace L' ; thus J' is finitely generated over $F[x]$ as a submodule of $p(x)^{-\beta} J$. Therefore J' is an order of A ; since J is maximal, $J' = J$.

Now suppose there is an element a in L' not in L . Letting u_1, \dots, u_m be a basis of $A/F(x)$, we write $a = \sum a_i u_i$, $a_i \in F(x)_Q$. We can find elements $b_i \in F(x)$ close enough to the a_i so that $b = \sum b_i u_i$ is also in L' but not in L , since L is closed and L' is open. This b is in A . There is a $g \in F[x]$ such that $g \cdot b \in J$, and we may factor g as $g = p(x)^\alpha h$, where $h \in F(x)$ is prime to $p(x)$. Then $hb \in L'$; and, since h is a unit in \mathfrak{o}_Q and L is an \mathfrak{o}_Q -module,

⁸ That (2.1) holds even when x is not a separating element of K was proved by Iwasawa in [10, §3].

$h^{-1}L \subset L$, which implies $hb \notin L$. But hb is in $J' = J \subset L$, a contradiction. Therefore $L' = L$, Q.E.D.

LEMMA 2.3. *Let u_1, \dots, u_m be any basis of $A/F(x)$ and define, for each $P \in \mathfrak{M}$, $E_P = \mathfrak{o}_Q u_1 + \dots + \mathfrak{o}_Q u_m$. Then for almost all P , E_P is a maximal order of \tilde{A}_P and equals $\mathfrak{o}_P u_1 + \dots + \mathfrak{o}_P u_m$.*

Proof. Let J be any maximal order of A relative to $F[x]$, J_P the closure of J in \tilde{A}_P . By Lemma 2.2, J_P is a maximal order of \tilde{A}_P for almost all P . Let $J = F[x]b_1 + \dots + F[x]b_n$ for some $b_1, \dots, b_n \in A$, and let each $b_i = \sum_j c_{ij} u_j$, where $c_{ij} \in F(x)$. Then the matrix (c_{ij}) has no column consisting entirely of zeros. Since $J_P = \mathfrak{o}_Q b_1 + \dots + \mathfrak{o}_Q b_n$, it follows that $J_P = E_P$ for almost all P , Q.E.D.

THEOREM 2.2. *For each finite prime P , let L_P be a maximal order of \tilde{A}_P such that almost all $L_P = \mathfrak{o}_P u_1 + \dots + \mathfrak{o}_P u_m$, where the u 's form a basis of $A/F(x)$. Let J denote the intersection of all $A \cap L_P$. Then J is a maximal order of A relative to $F[x]$.*

Proof. Using the topological properties established up to now, one first proves that J is an order of A . Then Lemma 2.2 implies that J is a maximal order. We omit the details.

In order to clarify later parts of this paper, and to make a convenience rigorous, we now discuss isomorphisms between \tilde{A} and the matrix ring arising naturally from \tilde{A} . That is, each \tilde{A}_P is a normal simple algebra over K_P and is therefore algebraically isomorphic to the full matrix algebra $r_P \times r_P S_P$ over some skew-field S_P with K_P as center. If A is isomorphic to the full matrix algebra $r \times r S_0$ over the skew-field S_0 , then $K_P \otimes S_0 \cong \mu_P \times \mu_P S_P$ for some integer μ_P , so that $r_P = r\mu_P$. We define \tilde{S}_P to be $r_P \times r_P S_P$ and \tilde{S} to be the weak direct sum

$$\tilde{S} = \sum'_{P \in \mathfrak{M}} \tilde{S}_P$$

in the sense that each matrix in \tilde{S} must have almost all its P -components taken from $r_P \times r_P \mathcal{O}_P$, in the notation of §1. \tilde{S} can be given two topologies, one in which a fundamental system of neighborhoods of 0 consists of the subspaces of the form XI , where X is a regular element of \tilde{S} and I is the direct sum $\sum r_P \times r_P \mathcal{O}_P$, another which the direct-sum topology of each \tilde{S}_P gives rise to; that these topologies are actually the same is a consequence of Lemma 1.2.

Let us agree to denote $r_P \times r_P \mathcal{O}_P$ by I_P in what follows. An element U of \tilde{S} (or of \tilde{S}_P) is said to be *unitary* if it is a regular element of \tilde{S} (or of \tilde{S}_P) such that both U and U^{-1} are in I (or I_P). We shall need the decomposition [13, p. 107] of a regular matrix $C \in \tilde{S}_P$ as

$$(2.2) \quad C = U(\delta_{ij} t^{e_i})V,$$

where U and V are unitary in \tilde{S}_P , δ_{ij} is the Kronecker delta, t is a prime element for P , and the e_i are rational integers.

We now have

LEMMA 2.4. *A maximal open linearly compact subring of \tilde{S}_P is always of the form $C^{-1}I_P C$, where C is a regular element of \tilde{S}_P .*

For a proof, see Hasse, [5, pp. 519–520].

This lemma enables one to prove rather easily

THEOREM 2.3. *There is a topological K -isomorphism of \tilde{A} onto \tilde{S} . Any topological automorphism of \tilde{S} onto \tilde{S} transforms almost all I_P onto themselves.*

Now let J_1 and J_2 be maximal orders of A relative to $F[x]$. Let M be a left-ideal for J_1 and a right-ideal for J_2 . Let M_P denote the closure of M in \tilde{A}_P , and similarly for J_1^P, J_2^P . For each finite P let L_P be a maximal order of \tilde{A}_P such that almost all L_P are equal to $\mathfrak{o}_P u_1 + \cdots + \mathfrak{o}_P u_n = E_P$, for a fixed basis u_1, \dots, u_n of A/K .

THEOREM 2.4. *For each finite P , M_P is an open linearly compact left-module for J_1^P and right-module for J_2^P ; almost all $M_P = E_P$. Conversely, the intersection with A of such M_P 's is an ideal of A relative to $F[x]$; in particular, our original ideal M is the intersection of its components M_P . Each M_P has the form $C_P^{-1}L_P C_P'$, where C_P and C_P' are regular elements of \tilde{A}_P such that almost all $C_P^{-1}L_P C_P' = L_P = E_P$.*

We omit the proof of this theorem, as well as that of the following

THEOREM 2.5. *The maximal open linearly compact subrings of \tilde{A} are all conjugate to each other in \tilde{A} . They are the direct sums of their P -components.*

3. A general Riemann-Roch theorem

Let V be a finite-dimensional vector space over the function field K . Let V' denote the dual space to V . As spaces of valuation vectors of V and V' , we define $\tilde{V} = R \otimes_K V$ and $\tilde{V}' = R \otimes_K V'$. The natural pairing $\langle v, v' \rangle_0 = v'(v)$ of V and V' to K can be extended uniquely by continuity to a pairing of \tilde{V} and \tilde{V}' to R : $\langle \tilde{v}, \tilde{v}' \rangle$ is a continuous, R -bilinear map of $\tilde{V} \times \tilde{V}'$ into R . Letting χ be an admissible character of R , we define

$$(3.1) \quad [v, v'] = \chi(\langle v, v' \rangle), \quad v \in \tilde{V}, \quad v' \in \tilde{V}'$$

and obtain thereby a continuous F -bilinear map of $\tilde{V} \times \tilde{V}'$ into F .

THEOREM 3.1. *The mapping $f: \tilde{V} \rightarrow X(\tilde{V}')$ of \tilde{V} to the character space of \tilde{V}' given by $f(\tilde{v}) = [\tilde{v}, \]$ is a topological isomorphism onto; that is, the dual pairing (3.1) is topological. Under this pairing, the annihilator $A(V)$ of V is V' .*

Proof. For any basis $\{v_i\}$ of V/K , let $\{v'_i\}$ be the dual basis of V'/K . With respect to these (or any) bases, \tilde{V} and \tilde{V}' are immediately seen to be paired as direct sums of copies of the self-dual space R (see §1). But $[\ , \]$ becomes this very pairing when expressed in terms of these bases. This ob-

ervation also shows immediately that $A(V) = V'$, since $A(K) = K$ under the pairing of R to itself mentioned in §1, Q.E.D.

If M is an open linearly compact subspace of \tilde{V} , then $M \cap V$ is finite-dimensional over F , by Lemma 1.1. Thus we may define for such M

$$l(M) = \dim_F(M \cap V),$$

and similarly for such subspaces of \tilde{V}' .

We introduce the unique function $\nu(\quad, \quad)$ defined on ordered pairs of open linearly compact subspaces of \tilde{V} such that

$$(3.2) \quad \begin{aligned} \text{(i)} \quad & \nu(M_1, M_2) + \nu(M_2, M_3) = \nu(M_1, M_3), \\ \text{(ii)} \quad & \nu(M_1, M_2) = \dim_F(M_1/M_2) \quad \text{if } M_1 \supset M_2. \end{aligned}$$

The existence and uniqueness of this ν -function are quite easy to prove;⁹ and it follows that

$$(3.3) \quad \nu(M_1, M_2) = \nu_1(\pi M_1, \pi M_2) + \nu_2(M_1 \cap V, M_2 \cap V),$$

where ν_1 and ν_2 are the analogous ν -functions for the spaces \tilde{V}/V and V , respectively, and π is the natural map from \tilde{V} onto \tilde{V}/V .

Now let M' be the annihilator with respect to the dual pairing (3.1) of the divisor M of \tilde{V} . M' is open in \tilde{V}' by the continuity of $[\quad, \quad]$ and is linearly compact as the dual space to the discrete space \tilde{V}/M . By Theorem 3.1, the annihilator of $M \cap V$ is the (closed) subspace $M' + V'$ of \tilde{V}' ; therefore

$$(3.4) \quad l(M) = \dim_F(\tilde{V}'/(M' + V')),$$

since $\tilde{V}'/(M' + V')$ is dual to the finite-dimensional space $M \cap V$.

We shall now restate (3.3) in terms of l . We have

$$\begin{aligned} \nu_1(\pi M_1, \pi M_2) &= -\nu_1(\tilde{V}/V, \pi M_1) + \nu_1(\tilde{V}/V, \pi M_2) \\ &= -\dim_F(\tilde{V}/(M_1 + V)) + \dim_F(\tilde{V}/(M_2 + V)) \\ &= -l(M'_1) + l(M'_2), \end{aligned}$$

by (3.2) and (3.4). Also, $\nu_2(M \cap V, 0) = l(M)$, so that we may put (3.3) as

THEOREM 3.2. *For any two open linearly compact subspaces M_1, M_2 of \tilde{V} , we have*

$$\nu(M_1, M_2) = l(M_1) - l(M'_1) - (l(M_2) - l(M'_2)),$$

where M'_1 and M'_2 are the annihilators of M_1 and M_2 , respectively, with respect to the dual pairing (3.1).

Let A and B be simple algebras of finite rank over the center K . Assume now that V is a unitary left A -, right B -module. Then V' is naturally a left B -, right A -module, and the pairing $\langle \quad, \quad \rangle_0$ satisfies $\langle avb, v' \rangle_0 = \langle v, bv'a \rangle_0$ for all $a \in A, b \in B, v \in V$, and $v' \in V'$.

⁹ For proofs of these properties of the ν -function, see [10, §1].

There is a unique way to make \tilde{V} a unitary left \tilde{A} -, right \tilde{B} -module (with the action denoted for the moment by a dot) such that

$$\begin{aligned} s \cdot v &= v \cdot s = s \otimes v, & s \in R, \quad v \in V, \\ a \cdot v &= av, \quad v \cdot b = vb, & a \in A, \quad b \in B, \quad v \in V. \end{aligned}$$

The map of $\tilde{A} \times \tilde{V} \times \tilde{B}$ to \tilde{V} which sends $(\tilde{a}, \tilde{v}, \tilde{b})$ into $\tilde{a} \cdot \tilde{v} \cdot \tilde{b}$ is then continuous. The analogous result holds for \tilde{V}' . Furthermore, there is a unique R -bilinear pairing $\langle \cdot, \cdot \rangle$ of \tilde{V} and \tilde{V}' to R such that $\langle v, v' \rangle = \langle v, v' \rangle_0$ for $v \in V, v' \in V'$. $\langle \cdot, \cdot \rangle$ is then a continuous map of $\tilde{V} \times \tilde{V}'$ into R such that $\langle \tilde{a}\tilde{v}\tilde{b}, \tilde{v}' \rangle = \langle \tilde{v}, \tilde{b}\tilde{v}'\tilde{a} \rangle$ for $\tilde{a} \in \tilde{A}, \tilde{v} \in \tilde{V}$, etc. Finally, we have

LEMMA 3.1. *If A acts faithfully on V , then so does \tilde{A}_P on \tilde{V}_P .*

Proof. The result follows immediately from the general structure theorem for such modules (see [2, p. 46]), which says that if A is K -isomorphic to the full matrix ring $r \times rS_0$ over the skew-field S_0 , then V is K -isomorphic to $r \times r_1S_0$, for some r_1 , and the action of A on V is given by the usual matrix multiplication. On tensoring with K_P we get the desired result.

We shall now prove a formula which, in some cases, allows us to compute $\nu(M_1, M_2)$. Let M_2 be a given open linearly compact subspace of \tilde{V} ; suppose furthermore that M_2 is an \mathfrak{o} -module, which implies in particular that it is the direct sum of its P -components. Then the same properties hold for the subspace $M_1 = a^{-1}M_2b$, where a and b are regular elements of \tilde{A} and \tilde{B} , respectively. We shall compute $\nu(M_1, M_2)$.

First assume $M_1 \supset M_2$. Then $\nu(M_1, M_2) = \dim_P M_1/M_2$, and it will suffice to compute the F -dimension ρ_P of the P -component M_{1P}/M_{2P} ; for then $\nu(M_1, M_2) = \sum_P \rho_P$.

LEMMA 3.2. *Let the subspace M_P of \tilde{V}_P be an open, linearly compact \mathfrak{o}_P -module. Then there exists a basis $\{w_j\}$ of \tilde{V}_P/K_P such that $M_P = \sum \mathfrak{o}_P w_j$.*

Proof. The lemma follows immediately from part 1 of [13, §108] when we observe that the openness of M_P implies that M_P contains a basis of \tilde{V}_P/K_P .

We can now proceed to compute ρ_P , on the assumption that $M_{1P} = (a^{-1}M_2b)_P \supset M_{2P}$. Let w_1, \dots, w_n be the basis of \tilde{V}_P/K_P contained in M_{2P} described in Lemma 3.2. With respect to this basis, the operation at P of a^{-1} and b leads to a nonsingular $n \times n$ matrix (α_{ij}) over K_P as follows:

$$a_P^{-1} w_i b_P = \sum_{j=1}^n \alpha_{ij} w_j, \quad \alpha_{ij} \in K_P, \quad i = 1, \dots, n.$$

Then

$$M_{1P} = \sum_i \mathfrak{o}_P (a_P^{-1} w_i b_P) = \left\{ \sum_{i,j} \mathfrak{a}_i \alpha_{ij} w_j ; \mathfrak{a}_i \in \mathfrak{o}_P \right\}.$$

If we express M_{1P} as a set of n -tuples, the coefficients with respect to the basis w_1, \dots, w_n , we find

$$M_{1P} = (\mathfrak{o}_P, \dots, \mathfrak{o}_P)(\alpha_{ij}) = (1 \times n\mathfrak{o}_P)(\alpha_{ij}).$$

In the same way M_{2P} becomes simply $1 \times n_{\mathfrak{o}_P}$. Thus

$$\rho_P = \dim_F(1 \times n_{\mathfrak{o}_P})(\alpha_{ij}) / (1 \times n_{\mathfrak{o}_P}).$$

In order to calculate ρ_P , we represent (α_{ij}) according to (2.2) as $(\alpha_{ij}) = u(\delta_{ij} \tau^{e_i})v$, where u and v are unitary $n \times n$ matrices over K_P and $\nu_P(\tau) = 1$. Now since $(1 \times n_{\mathfrak{o}_P})u = (1 \times n_{\mathfrak{o}_P})$, our above factor-space is $(1 \times n_{\mathfrak{o}_P})(\delta_{ij} \tau^{e_i})v / (1 \times n_{\mathfrak{o}_P})$, which is isomorphic over F to $(1 \times n_{\mathfrak{o}_P})$.

$$(\delta_{ij} \tau^{e_i}) / (1 \times n_{\mathfrak{o}_P}) = (\mathfrak{p}^{e_1}, \dots, \mathfrak{p}^{e_n}) / (\mathfrak{o}_P, \dots, \mathfrak{o}_P) \cong \mathfrak{K}_P \oplus \dots \oplus \mathfrak{K}_P$$

with $-(e_1 + \dots + e_n)$ summands (the e_i being all nonpositive because of the assumption that $M_1 \supset M_2$). Therefore the desired dimension ρ_P is $-n_P(e_1 + \dots + e_n)$. And this in turn may be written

$$\rho_P = n_P \nu_P(\det(\alpha_{ij})^{-1}).$$

To find the relation between $\det(\alpha_{ij})$ and the norms of a and b , we use the structure theorem [2, p. 46] quoted in the proof of Lemma 3.1. Here it is easy to see that the matrix (β_{ij}) for $a \in A$ arising out of $av_i = \sum \beta_{ij} v_j$, with $\beta_{ij} \in K$, $\{v_j\}$ a basis of V/K , is the r_1 -fold repetition of the matrix obtained when one replaces each S_0 -entry of a with its matrix in the regular representation of S_0/K . (The positive integer r_1 is the number of columns in the isomorph of V given by the structure theorem.) Since the matrix of a in the regular representation of A over K is the r -fold repetition of the same matrix, it follows immediately that $\det(\beta_{ij}) = N(a)^{r_1/r}$. When we pass to the local situation, both r_1 and r are multiplied by μ_P , leaving the exponent unchanged.

Similarly, the analogous matrix (γ_{ij}) for $b \in B$ satisfies $\det(\gamma_{ij}) = N'(b)^{r_2/r'}$ for some positive integer r_2 (the number of rows in the appropriate isomorph of V , when B is isomorphic to $r' \times r' S'_0$, S'_0 a normal skew-field over K). N' denotes the norm of the regular representation of B/K . It can be extended uniquely to \tilde{B}/R .

Returning now to the provocation for all this, we see that there exist rational numbers $\rho_1 = r_1/r$ and $\rho_2 = r_2/r'$ depending only on the module structure of (A, V, B) such that

$$\det(\alpha_{ij})^{-1} = N_P(a_P)^{\rho_1} N_P(b_P)^{-\rho_2}.$$

Therefore $\rho_P = n_P(\rho_1 \nu_P N_P(a_P) - \rho_2 \nu_P N_P(b_P))$. And now we can assert

LEMMA 3.3. *If M_0 is an open, linearly compact \mathfrak{o} -module contained in \tilde{V} , and if $M = a^{-1}M_0 b$ contains M_0 , for regular $a \in \tilde{A}$, $b \in \tilde{B}$, then there exist positive rational numbers ρ_1 and ρ_2 depending only on the module structure of (A, V, B) such that*

$$\nu(M, M_0) = \dim_F(M/M_0) = n(N(a)^{\rho_1} N'(b)^{-\rho_2}),$$

where $n(c)$ denotes the degree of the regular element c in R .

Proof. We need only recall that $\dim_F M/M_0 = \sum \rho_P$ and that the degree of a regular element c of R is $\sum n_P \nu_P(c_P)$.

Now we need to consider how to compute $\nu(M, M_0)$ in the general case, when M may not contain M_0 . We still assume that $M = a^{-1}M_0 b$ for regular $a \in \tilde{A}$, $b \in \tilde{B}$, however, and that M_0 is an open, linearly compact \mathfrak{o} -module. We simply define $\nu(M, M_0) = n(N(a)^{\rho_1} N'(b)^{-\rho_2})$; the verification that property (i) of (3.2) holds for this ν -function is routine, and we have just proved that (ii) holds. Therefore we have proved

THEOREM 3.3. *Let A and B act faithfully on V , and let the subspace M_0 of \tilde{V} be an open, linearly compact \mathfrak{o} -module. Then for all subspaces of the form $M = a^{-1}M_0 b$, with a regular in \tilde{A} , b regular in \tilde{B} , the ν -function (3.2) satisfies*

$$\nu(M, M_0) = n(N(a)^{\rho_1} N(b)^{-\rho_2})$$

for certain positive rational numbers ρ_1 and ρ_2 depending only on the structure of the module (A, V, B) and not on M_0 or M .

Under the notations of Theorem 3.3, let us define the *degree* of M with respect to M_0 as

$$(3.5) \quad n(M) = n(N(a)^{\rho_1} N'(b)^{-\rho_2}).$$

These subspaces M will play the role of divisors in our generalization of the Riemann-Roch theorem to the module V .

Let the annihilator of \mathfrak{o} in R with respect to χ be $d^{-1}\mathfrak{o}$ for a regular $d \in R$. For a given $P \in \mathfrak{M}$, let $M_{0P} = \mathfrak{o}_P w_1 + \cdots + \mathfrak{o}_P w_n$ in accordance with Lemma 3.2. Then the P -component of the annihilator of M_0 is $M'_{0P} = d_P^{-1} \mathfrak{o}_P w'_1 + \cdots + d_P^{-1} \mathfrak{o}_P w'_n$, where w'_1, \dots, w'_n is the dual basis to w_1, \dots, w_n . And that for M is $M'_P = d_P^{-1} \mathfrak{o}_P (b_P^{-1} w'_1 a_P) + \cdots + d_P^{-1} \mathfrak{o}_P (b_P^{-1} w'_n a_P)$. Thus Lemma 3.2 and Theorem 3.3 allow us to state Theorem 3.2 in a more explicit form, which we call our generalization of the Riemann-Roch Theorem to V :

THEOREM 3.4. *Under the hypotheses and notations of Theorem 3.3, we have*

$$l(M) = l(M') + n(M) - (l(M'_0) - l(M_0)),$$

where $n(M)$ is the degree of M with respect to M_0 as defined in (3.5). Here the quantity $l(M'_0) - l(M_0)$ depends only on M_0 , not on the module structure.

Remark. The functions l and n appearing here are “class-functions”; that is, if a and b are regular elements of A and B , respectively, then $l(aMb) = l(M)$ and $n(aMb) = n(M)$, for any open, linearly compact \mathfrak{o} -module M .

This theorem contains the classical Riemann-Roch theorem: We take $A = V = B = K$, $M_0 = \mathfrak{o}$, $M = a^{-1}\mathfrak{o}$ for a regular element a of R ; then $l(\mathfrak{o}) = 1$, $l(\mathfrak{o}') = g$, the genus of K , and the degree of $M = a^{-1}\mathfrak{o}$ with respect to $M_0 = \mathfrak{o}$ is $n(a^{-1}\mathfrak{o}) = n(a)$ in our definition. For the classical theorem we define $l^*(a) = l(a^{-1}\mathfrak{o})$ and obtain from our theorem the classical form of the Riemann-Roch theorem, namely,

$$l^*(a) = l^*(a') + n(a) - g + 1,$$

where by a' we understand any regular $b \in R$ such that $(a^{-1}a) = b$; it is well known that $b = a^{-1}d$, when $a' = d^{-1}a$.

In the classical case, divisors are defined as the set of all $a\mathfrak{o}$, a regular in R ; they can be characterized as the set of all open, linearly compact \mathfrak{o} -modules. For the module V considered in this paper we have taken for divisors the set of all subspaces of \tilde{V} which are open, linearly compact \mathfrak{o} -modules. In the general Theorem 3.2 the algebras A and B play no role, nor is the assumption that the subspaces be \mathfrak{o} -modules needed there. The use of the algebras A and B and the assumption of closure under \mathfrak{o} -multiplication is that they enable us to find a nice formula for the ν -function, provided one of the two divisors can be obtained from the other via multiplication by regular elements of \tilde{A} and \tilde{B} . As noted above, this relation holds between any two divisors in the classical case; it does not hold in general for our module V , however. But in one example where this relation fails to be universal, V is not irreducible as a double module; in another such example, B is not normal as a simple algebra over K ; but in these examples divisors are further restricted to be modules with respect to the actions of maximal open linearly compact subrings of \tilde{A} and \tilde{B} . Whether the reasonable assumptions of faithfulness, irreducibility as a double module, and normality imply that any (reasonably defined) divisor can be obtained from any other divisor via multiplication by regular elements of \tilde{A} and \tilde{B} is an open question. This relation between pairs of divisors is an equivalence relation, and Theorem 3.4 holds for divisors taken from any one class.

We now turn to a situation where, when the notion of divisor is suitably restricted, the relation in question holds between any two divisors.

4. Simple algebras over K

Let $A = V = B$ be a simple algebra over the center K , with the action being multiplication in A . Letting T denote the reduced trace from A to K , we pair A to itself by setting $\langle c, c' \rangle_0 = T(cc')$, for $c, c' \in A$. Then $\langle acb, c' \rangle_0 = \langle c, bc'a \rangle_0$ for all $a, b \in A$. Our dual pairing of \tilde{A} to itself becomes

$$(4.1) \quad [c, c'] = \chi T(cc'), \quad c, c' \in \tilde{A}.$$

In order to determine the numbers ρ_1 and ρ_2 appearing in the formula (3.5), we need only recall that if A is isomorphic to $r \times rS_0$, S_0 being a skew-field with center K , then $\rho_1 = r_1/r$, where r_1 is the number of columns of $r \times r_1S_0$, the isomorph of V . Thus $r_1 = r$ and $\rho_1 = 1$. Similarly $\rho_2 = 1$. Therefore, if M_0 is a divisor of \tilde{A} and if $M = a^{-1}M_0 b$, for regular elements $a, b \in \tilde{A}$, then

$$(4.2) \quad n(M) = \nu(M, M_0) = n(N(ab^{-1})),$$

where N denotes the norm (of the regular representation) from \tilde{A} to R . (N is the "direct product" of the local norms from \tilde{A}_P to K_P .)

Divisors. For convenience we shall denote the set of all maximal open linearly compact subrings of \tilde{A} as $\mathcal{L}(\tilde{A}) = \mathcal{L}$. In the present situation we

restrict our divisors to be open, linearly compact subspaces M of A such that there exist $H, J \in \mathcal{L}$ for which $HMJ = M$. For this divisor we shall occasionally denote H by M_l and J by M_r .

We can easily prove that all divisors are equivalent in the sense discussed at the end of §3 by using the isomorphism of §2 between \tilde{A} and the appropriate space of matrices \tilde{S} : The members of $\mathcal{L}(\tilde{S})$ are of the form $C^{-1}IC$, where C is a regular element of \tilde{S} and I is the subring of "integral" matrices defined near the end of §2. If $C_1^{-1}IC_1$ and $C_2^{-1}IC_2$ are two such subrings equalling M_{1l} and M_{1r} for a divisor M_1 , then $C_1 M_1 C_2^{-1} = M_2$ is a two-sided I -module; it is easy to prove that M_2 must then be of the form cI , where c is a regular element of \tilde{S} of the form

$$(4.3) \quad c_P = (\delta_{ij} a_P), \quad a_P \in S_P,$$

for each $P \in \mathfrak{M}$. Thus $M_1 = C_1^{-1}cIC_2$. Conversely, if C_1 and C_2 are regular elements of \tilde{S} , then $C_1^{-1}IC_2$ is a divisor of \tilde{S} . If we transfer these results back to A by means of our isomorphism, we can now assert

LEMMA 4.1. *Each divisor of \tilde{A} is of the form $a^{-1}Hb$ for regular $a, b \in \tilde{A}$ and for a fixed subring $H \in \mathcal{L}$. Conversely, every such subspace of \tilde{A} is a divisor of \tilde{A} .*

For later use, we shall now discuss the element c mentioned above. First we state a criterion for equality between divisors, the proof of which follows rapidly from the decomposition (2.2):

LEMMA 4.2. *The divisors $C^{-1}IC_0$ and $C'^{-1}IC'_0$ of \tilde{S} are equal if and only if there is an element $a \in \tilde{S}$ locally of the form (4.2) such that both $aC'C^{-1}$ and $aC'_0C_0^{-1}$ are unitary.*

In our proof of Lemma 4.1 we saw that any divisor M_2 of \tilde{S} which is a two-sided I -module has the form $M_2 = cI$, where each P -component of c is in S_P , i.e., is a diagonal matrix. The above lemma implies that c is uniquely determined up to a unitary factor. Furthermore, $cI = Ic$; and c belongs to \tilde{S}_0 , the image of \tilde{S}_0 in \tilde{S} . If $H \in \mathcal{L}$, let us define an H -unit as a regular element b of \tilde{A} such that $b \in H$ and $b^{-1} \in H$.

Then we have proved

LEMMA 4.3. *If the divisor M of \tilde{A} is a two-sided H -module, for $H \in \mathcal{L}$, then M is of the form $cH = Hc$, where c is a regular element of \tilde{S}_0 uniquely determined up to an H -unit factor.*

This lemma assumes that one selects a particular $S_0 \subset A$.

The degree of a given divisor M satisfies, when $H \in \mathcal{L}$,

$$\nu(M, H) = \nu(M, a^{-1}Ha)$$

for all regular $a \in \tilde{A}$; or, in other words, since all $H \in \mathcal{L}$ are conjugate to each other, the degree of a divisor is invariant with respect to the members of this class \mathcal{L} . From now on in this section we restrict our definition of the degree

(3.5) of a divisor by requiring that M_0 belong to \mathcal{L} . (It is true that the degree of a divisor is invariant with respect to the members of any conjugacy-class of divisors, but \mathcal{L} is a naturally distinguished such class.)

Let H_0 and H be any two members of \mathcal{L} . As divisors, these have degree 0, so that if we apply Theorem 3.2 to H and H_0 , we find that $l(H') - l(H) = l(H'_0) - l(H_0)$, which proves that this quantity is an invariant of A . We denote it by

$$(4.4) \quad \xi(A) = l(H') - l(H), \quad H \in \mathcal{L}.$$

If A is isomorphic to $r \times rS_0$, as before, then we can prove

PROPOSITION 4.1. $\xi(A) = r^2\xi(S_0)$.

Proof. We use the isomorphism of \tilde{A} with \tilde{S} : Since $I \in \mathcal{L}(\tilde{S})$, it suffices to consider $l(I') - l(I)$; now $I = r \times r\theta$, and $\theta \in \mathcal{L}(\tilde{S}_0)$; $I' = r \times r\theta'$; therefore $\xi(A) = r^2\xi(S_0) = r^2(l(\theta') - l(\theta))$. We shall discuss some questions related to this invariant farther on.

Canonical divisors. In the classical case $A = K$, the canonical divisor corresponding to a given admissible character χ is defined as the inverse of the annihilator of \mathfrak{o} with respect to the dual pairing $[c, b] = \chi(cb)$, $c, b \in R$. That is, the annihilator \mathfrak{o}' equals $d^{-1}\mathfrak{o}$ for some regular $d \in R$; and $d\mathfrak{o}$ is the corresponding canonical divisor. As a runs through the nonzero elements of K , all admissible characters of R are obtained as χ_a , where $\chi_a(\) = \chi(a(\))$; the corresponding canonical divisor is $ad\mathfrak{o}$. Here the divisors form an abelian group and the principal divisors (namely, $a\mathfrak{o}$, $0 \neq a \in K$) a subgroup Π . Thus, modulo Π , the set of all canonical divisors is precisely a coset. Analogous conditions hold in the general case.

Let $M = a^{-1}Hb$ be a divisor of \tilde{A} . By the *inverse* of M we simply mean the divisor $M^{-1} = b^{-1}Ha$. The relations $MM^{-1} = M_l$ and $M^{-1}M = M_r$ hold.

In the present case, "the" ring of integers in \tilde{A} is determined only up to inner automorphism. Each $H \in \mathcal{L}$ will have a collection of canonical divisors; those of $a^{-1}Ha$ will be the conjugates under a of those of H .

Let $H \in \mathcal{L}$, and consider the annihilator H' of H with respect to (4.1). H' is an open, linearly compact, two-sided H -module; in other words H' is a divisor of \tilde{A} . We call H'^{-1} the canonical divisor for H corresponding to χ . By Lemma 4.3, H' is of the form $\mathfrak{d}^{-1}H$, for some regular $\mathfrak{d} \in S_0$ such that $\mathfrak{d}H = H\mathfrak{d}$; and \mathfrak{d} is uniquely determined up to an H -unit factor. If a is a regular element of \tilde{A} , then the canonical divisor for $a^{-1}Ha$ with respect to χ is $a^{-1}\mathfrak{d}Ha$, or $a^{-1}\mathfrak{d}a \cdot a^{-1}Ha$. Therefore we need only determine the canonical divisors for H .

By Theorem 3.1, the annihilator of A is A itself; therefore we obtain all characters of \tilde{A} which vanish on A as $\chi_a = [a, \]$, $a \in A$. Among these, the ones which give rise to dual pairings of \tilde{A} with itself are those with a regular. For such a , the pairing is $[c_1, c_2]_a = \chi T(ac_1 c_2)$. When $a \notin K$, this pairing is not symmetric, so we must speak of left- and right-hand annihilators and

canonical divisors. For example, the left-hand annihilator $A_l(H)$ of H is the set of all c_1 such that $[c_1, H]_a = 0$; or $A_l(H) = a^{-1}H' = a^{-1}\mathfrak{d}^{-1}H$. (We have now $A_r(A_l(H)) = H$, but $A_l(A_l(H)) = a^{-1}Ha$.) The corresponding canonical divisor is $\mathfrak{d}Ha$, which we shall call the *right-hand* canonical divisor.

We now define, by analogy with the case $A = K$, equivalence relations \sim_l, \sim_r on the set of all divisors of \tilde{A} . If M_1 and M_2 are divisors of \tilde{A} , we say

$M_1 \sim_l M_2$ ($M_1 \sim_r M_2$) if and only if there exists a regular $a \in A$ such that $M_1 = aM_2$ ($M_1 = M_2 a$).

We see that the set of left-hand canonical divisors for H is precisely the equivalence-class containing $\mathfrak{d}H$ under \sim_l , and correspondingly for the right-hand ones. If a and c are regular elements of A and \tilde{A} , respectively, then the right-hand canonical divisor for $c^{-1}Hc$ corresponding to $[\ , \]_a$, is $c^{-1}\mathfrak{d}Hca$.

If $M = a^{-1}Hb, H \in \mathcal{L}$, is an arbitrary divisor of \tilde{A} , then $M' = b^{-1}H'a = b^{-1}\mathfrak{d}^{-1}Ha$. If we (inadequately) denote $b^{-1}\mathfrak{d}b$ by \mathfrak{d}_M , then $M' = \mathfrak{d}_M^{-1}M^{-1}$. We can also say that $M' = (b^{-1}\mathfrak{d}^{-1}Hb)M^{-1}$, the first factor being the inverse of the canonical divisor for $b^{-1}Hb$. The left-annihilator of M with respect to $[\ , \]_c, c$ regular in A , is $c^{-1}b^{-1}\mathfrak{d}^{-1}Ha$.

We can now assert our generalization of the Riemann-Roch theorem for A :

THEOREM 4.1. *If M is any divisor of \tilde{A} , then*

$$l(M) = l(\mathfrak{d}_M^{-1}M^{-1}) + n(M) - r^2\xi(S_0).$$

COROLLARY 4.1. *All canonical divisors have degree*

$$-2r^2\xi(S_0) = n(N(\mathfrak{d})^{-1}) = -n(H'), \quad H' \in \mathcal{L}.$$

Proof. That they all have the same degree $n(N(\mathfrak{d})^{-1})$ follows from the construction of them in the preceding paragraphs and the fact that K -elements have degree 0 in R . We obtain the corollary by putting $M = H', H \in \mathcal{L}$, in the theorem.

We can also derive as a corollary the generalization of Riemann's theorem in the special case $A = S_0$.

COROLLARY 4.2. *If M is a divisor of \tilde{S}_0 with degree $n(M) > 2\xi(S_0)$, then*

$$l(M) = n(M) - \xi(S_0).$$

Proof. We first notice that for any divisor $M, c \in M \cap A$ implies $n(Nc) \geq -n(M)$. Therefore, $n(M) < 0$ implies $l(M) = 0$. Now if our given M is of the form $a^{-1}Hb$, then we see, from $M' = b^{-1}\mathfrak{d}^{-1}Ha$, that $n(M') = n(N\mathfrak{d}) - n(M) < 0$. Therefore, $l(M') = 0$.

Remark 4.1. Theorem 4.1 is usually stated in terms of the functions l^* and n^* , where $l^*(M) = l(M^{-1})$ and $n^*(M) = n(M^{-1})$ for divisors M of \tilde{A} .

The theorem then reads

$$(4.5) \quad l^*(M) = l^*(\mathfrak{d}_M M^{-1}) + n^*(M) - r^2\xi(S_0).$$

Of course, we could have simply reasserted Theorem 3.4 for $V = A$, but the advantages of restricting our divisors are important: The invariant $\xi(A) = r^2\xi(S_0)$ arises, and the existence of inverse and canonical divisors allows a nice expression for the annihilator.

Before comparing this theorem with the Riemann-Roch theorem of Witt [16], we shall need to discuss the different, which will lead to some other points of interest. Accordingly we shall defer the comparison to the next section, where we shall also state a generalization of the theorem of Weil [15].

The different. Define the subspace M of \tilde{S} as

$$(4.6) \quad M = \{a; a \in \tilde{S}, T(aI) \subset \mathfrak{o}\},$$

where T is the reduced trace from \tilde{S} to R obtained by extending that from $r \times rS_0$ to K . M is obviously an open two-sided I -module and is contained in $b^{-1}I'$ for a regular $b \in R$ satisfying $b\mathfrak{o} \subset \text{kernel } \chi$; therefore M is linearly compact. By the proof of Lemma 4.1, M has the form $M = D^{-1}I$ for some regular element D of \tilde{S} of the form (4.3); by Lemma 1.2, each P -component of D in the form (4.3) has $a_P \in \mathfrak{O}_P$. The divisor DI is called the *different of I/K* . If $C^{-1}IC$ is any maximal open linearly compact subring of \tilde{S} , then its different (over K) is defined analogously and turns out to be $C^{-1}DIC$. The different D_x of $K/F(x)$ is defined¹⁰ similarly by the relation

$$\{a; a \in R, T_{K/F(x)}(a\mathfrak{o}) \subset \mathfrak{o}_0\} = D_x^{-1}\mathfrak{o},$$

where \mathfrak{o}_0 is the ring of integers of R_0 . The different D^* of $I/F(x)$ is defined similarly, and the result that $D^*I = DD_x I$ follows immediately from the factorability of the reduced trace.

Now let χ be any admissible character of R , and let $d\mathfrak{o}$ and $\mathfrak{d}I$ be the corresponding canonical divisors of R and I , respectively. We shall prove

LEMMA 4.4. $\mathfrak{d}I = DdI$.

Proof. Taking M as in (4.6), we have $(dD)^{-1}I = d^{-1}M$ and $\chi T(d^{-1}MI) = \chi(d^{-1}T(MI)) = \chi(d^{-1}\mathfrak{o}) = \mathfrak{0}$. Therefore $\mathfrak{d}I \subset dDI$. Since T is open, $T(D^{-1}I)$ is a divisor of R , which must then be \mathfrak{o} . Therefore $T(d^{-1}D^{-1}I) = \mathfrak{o}'$. Now $\chi T(\mathfrak{d}^{-1}I) = \mathfrak{0}$ implies $T(\mathfrak{d}^{-1}I) \subset \mathfrak{o}'$, or $T(d\mathfrak{d}^{-1}I) \subset \mathfrak{o}$. Thus $d\mathfrak{d}^{-1}I \subset D^{-1}I$, or $\mathfrak{d}I \supset dDI$, Q.E.D.

We can apply this result to the separable extension $K/F(x)$, achieving the result that $d\mathfrak{o} = D_x d_0 \mathfrak{o}$, where $d_0 \mathfrak{o}_0$ is the canonical divisor of $F(x)$ corresponding to the admissible character χ_0 of R_0 , and $d\mathfrak{o}$ is the canonical divisor of R arising from $\chi = \chi_0 T_0$, T_0 being the reduced trace from K to $F(x)$. Furthermore, we can easily construct a χ_0 such that $d_0 = u^{-2}$, where u is the denominator of x . (To carry out this construction, one needs the facts that $R_0 =$

¹⁰ Here we need to assume, with Witt, that $K/F(x)$ is separable.

$F(x) + u\bar{0}_0$, a topological direct sum, and that $\bar{0}'_0 \cap F(x)$ has F -dimension equal to the genus of $F(x)$, which is 0, [9, 10].) Thus we have proved rather simply the well-known result [6, p. 374] that $d = D_x/u^2$, i.e., that $(D_x/u^2)\bar{0}$ is a canonical divisor of R . From this result it follows that $(D^*/u^2)I$ is a canonical divisor for I .

Thus there is an admissible character of R such that if $M = C^{-1}IC_0$ is a divisor of \bar{S} , then the annihilator of M is the space $C_0^{-1}(D^*/u^2)^{-1}IC = M'$. We have proved

LEMMA 4.5. *There exists an admissible character χ_1 of R such that if M is a divisor of \bar{A} with $M_l = H$, then the annihilator M' corresponding to χ_1 is that divisor satisfying*

$$(4.7) \quad (MM')^{-1} = u^{-2}\delta(H),$$

where $\delta(H)$ is the different of $H/F(x)$.

Since the various differentials of \bar{A}/K are determined up to conjugation, and multiplication by units, and since $D_P \in S_P$ for each P , the integer $\delta_P = v_P(D_P)$ is an invariant of \bar{A}_P ; in fact, δ_P depends only on S_0 , so that we may as well take $A = S_0$ when investigating this differential exponent δ_P .

We do so now; our first result will be a relation between the reduced traces T_P and T_{1P} of S_P/K_P and $\mathfrak{S}_P/\mathfrak{K}_P$, respectively. Let $[S_P:K_P] = m_P'^2 = e_P f_P$; thus if $[S:K] = m^2$, then $m^2 = m_P'^2 \mu_P^2$. For each $a \in \mathfrak{O}_P$ let a^* denote the residue class of a modulo \mathfrak{F}_P .

LEMMA 4.6. *For each $P \in \mathfrak{M}$, the reduced traces satisfy*

$$T_P(a)^* = \alpha_P T_{1P}(a^*), \quad a \in \mathfrak{O}_P,$$

where $\alpha_P = e_P m_P/m_P'$ is a positive rational integer.

Proof. The matrix of the regular representation of a generic element of S_P (with respect to the integral basis of Lemma 1.2), on reduction modulo \mathfrak{F}_P breaks naturally into submatrices of size $f_P \times f_P$; below the diagonal block these matrices are zero; the diagonal block is an e_P -fold repetition of the matrix of the regular representation of a generic element of $\mathfrak{S}_P/\mathfrak{K}_P$. Therefore the characteristic polynomial $c(X)$ of S_P/K_P is related to that, $c_1(X^*)$, of $\mathfrak{S}_P/\mathfrak{K}_P$ by the formula

$$(4.8) \quad c(X)^* = c_1(X^*)^{e_P}.$$

Let $f(X)$ be the minimal polynomial of S_P/K_P and $f_1(X^*)$ that of $\mathfrak{S}_P/\mathfrak{K}_P$. We know that in general [1, p. 17] the characteristic polynomial of a skew-field is a power of the minimal polynomial, and that, when the center is separable over the base field, this power is the index of the skew-field [1, p. 123]. Therefore (4.8) becomes

$$(4.9) \quad f(X)^{*m_P'} = f_1(X^*)^{m_P e_P},$$

where $m_P \geq 1$ is the index of \mathfrak{S}_P whenever the center of \mathfrak{S}_P is separable over \mathfrak{R}_P . But $f_1(X^*)$ is irreducible over $\mathfrak{R}_P(\xi_i)$ (the ξ_i being indeterminates used to make the generic element); therefore f^* is a power of f_1 : There is a rational integer α_P such that $f(X)^* = f_1(X^*)^{\alpha_P}$, which gives our desired formula. It follows from (4.9) that $\alpha_P = e_P m_P / m'_P$.

Using Lemma 4.6, the formula of which is analogous to the one for fields, in which e_P replaces our α_P , one proves easily, exactly as in [17, p. 70],

PROPOSITION 4.2. *The differential exponent δ_P is at least $e_P - 1$ for all $P \in \mathfrak{M}$, and $\delta_P = e_P - 1$ if and only if both (i) and (ii) hold:*

- (i) *The center of \mathfrak{S}_P is separable over \mathfrak{R}_P .*
- (ii) *The characteristic of F does not divide α_P .*

As we shall see in a moment, the condition (i) implies condition (ii) in the noncommutative case, whereas (ii) is necessary for field extensions of K . But the relative simplicity of the proof here and the interesting corollaries which obtain at this point may justify the redundancy.

COROLLARY 4.3. *$e_P = 1$ for almost all $P \in \mathfrak{M}$.*

Proof. $\delta_P = 0$ for almost all P , and $\delta_P \geq e_P - 1 \geq 0$.

COROLLARY 4.4 *If the constant field F has characteristic zero or is finite, then $\delta_P = e_P - 1$ for all $P \in \mathfrak{M}$. When F is finite, then $e_P = f_P = m'_P$, and $\alpha_P = 1$, both for all $P \in \mathfrak{M}$, so that K_P splits S_0 for almost all P .*

Proof. The result in characteristic zero is immediate. When F is finite, then S_P is a finite skew-field and is therefore a field, by a famous theorem of Wedderburn. Then $m_P = 1$ for all P , so that $\alpha_P = e_P / m'_P$. But $e_P \mid m'_P$ in general, by Lemma 1.3; therefore $e_P = m'_P$, or $\alpha_P = 1$ for all P . From $e_P f_P = m_P'^2$ follows now $e_P = f_P = m'_P$.

We now prove that the assumption on α_P in the proposition is unnecessary. The proof is taken essentially from [12, p. 148].

THEOREM 4.2. *The center of the residue-class skew-field \mathfrak{S}_P is separable over \mathfrak{R}_P if and only if the differential exponent δ_P is $e_P - 1$.*

Proof. We need only prove that separability implies $\delta_P = e_P - 1$. It suffices to prove the existence of some $b \in \mathfrak{O}_P$ such that $T_P(b)$ is a unit in K_P . To this end let K_1 be a separable, unramified, maximal subfield of S_P/K_P with separable residue-class field \mathfrak{R}_1 over \mathfrak{R}_P [18, p. 12], [12, p. 148]. Then our formula of Lemma 4.6 for the unramified field extension K_1/K_P becomes $T_2(a)^* = T_{21}(a^*)$, $a \in \mathfrak{O}_P \cap K_1$, where T_2 is the trace of K_1/K_P and T_{21} that of $\mathfrak{R}_1/\mathfrak{R}_P$. The separability of the last named extension implies that for some $b \in \mathfrak{O}_P \cap K_1$, $T_2(b)$ is a unit of K_P . But T_P , when restricted to the maximal subfield K_1 , equals T_2 , Q.E.D.

Note. The existence of K_1 can be proved directly as follows: Let L_1 be a separable maximal subfield of \mathfrak{S}_P over the center C_P of \mathfrak{S}_P [1, p. 57].

Then $L_1 = \mathfrak{R}_P(a^*)$ for some $a \in \mathfrak{O}_P$, by the separability of C_P/\mathfrak{R}_P . Consider now $K_P(a)$, which has L_1 as residue-class field. Let

$$f(X) = X^q + a_1 X^{q-1} + \cdots + a_q$$

be a polynomial over \mathfrak{O}_P such that $f(X)^*$ is the (irreducible) minimal polynomial of a^* over \mathfrak{R}_P . Then $f(X)$ is irreducible over K_P . By Hensel's lemma, $f(X)$ has a zero b in $K_P(a) \cap \mathfrak{O}_P$ such that $b^* = a^*$. Therefore $K_P(b)$ has $\mathfrak{R}_P(a^*)$ as residue-class field, which implies that $K_P(b)/K_P$ is unramified, being of degree equal to that of $\mathfrak{R}_P(a^*)/\mathfrak{R}_P$. Now we prove that $K_P(b)$ is a maximal subfield of S_P and therefore that $K_P(a) = K_P(b)$. If $K_P(b)$ were not maximal, then its commutator algebra K' in S_P would not be a field [1, p. 53]. Then we would have $f(K'/K_P(b)) > 1$, by Lemma 1.3. This would imply the existence of a proper field extension of L_1 , in contradiction to the maximality of L_1 .

The Riemann-Hurwitz formula. We shall give the analogue of the Riemann-Hurwitz (? or Zeuthen-Halphen) formula relating, in our case, $\xi(S_0)$ to the genus g of K . If $\mathfrak{d}\mathfrak{O}$ is a canonical divisor of \tilde{S}_0 , we know that $n(N(\mathfrak{d})) = 2\xi(S_0) = n(N(D)) + n(N(d))$, the latter from Lemma 4.4. Since $d \in R$, $N(d) = d^{m^2}$, where $[S_0:K] = m^2$. If $D_P = (\delta_{ij} a_P)$, $a_P \in S_P$, the matrix being of size $\mu_P \times \mu_P$, then, at P , $N(D) = N_{S_P/K_P}(a_P)^{\mu_P^2}$. Thus $v_P N(D) = \mu_P^2 f_P \delta_P$, where δ_P is the differential exponent. Our above equation now becomes

$$2\xi(S_0) = m^2(2g - 2) + \sum_{P \in \mathfrak{M}} \mu_P^2 f_P n_P \delta_P.$$

Since $m^2 = \mu_P^2 e_P f_P$, we can put this as

THEOREM 4.3. *Let S_0 be a skew-field with finite rank m^2 over the center K . Then the invariants $\xi(S_0)$ and $\xi(K) = g - 1$ are related by the formula*

$$2\xi(S_0) = m^2(2g - 2 + \sum_{P \in \mathfrak{M}} n_P \delta_P / e_P),$$

where δ_P is the differential exponent at P , discussed in the preceding section.

The invariant $\xi(S_0)$. An interesting question concerning $\xi(S_0)$ is whether the two terms defining it are themselves invariants. That is, does $l(H_1)$ equal $l(H_2)$ for all $H_1, H_2 \in \mathfrak{L}(\tilde{S}_0)$? The equivalent question, of course, is whether the same holds with H'_1, H'_2 in place of H_1, H_2 . Some partial results in the affirmative are contained in the following two lemmas. They are phrased in the matrix terminology.

LEMMA 4.7. *Let S_0 be a skew-field extension of K with no "constant part"; that is, assume that F is (relatively) algebraically closed in S_0 . Then $l(b^{-1}\mathfrak{O}b) = 1$ for all regular $b \in \tilde{S}_0$.*

Proof. Let $a \in S_0$ and $a \in b^{-1}\mathfrak{O}b$. We wish to prove $a \in F$. The characteristic polynomial $c(X; u)$ of S_0/K is the same as that of $K_P \otimes_K S_0/K_P$. When specialized to the element a , this polynomial has coefficients in K . As an element of $b_P^{-1}(\mu_P \times \mu_P \mathfrak{O}_P)b_P$, a has the same characteristic polynomial

as $b_P ab_P^{-1} \in \mu_P \times \mu_P \Theta_P$ has; this one has coefficients in \mathfrak{o}_P , however, since, with respect to the usual integral basis $\{w_i t^j \cdot (\text{matrix units})\}$, $b_P ab_P^{-1}$ has coordinates in \mathfrak{o}_P . Therefore, the coefficients of $c(X; a)$ are in $K \cap \mathfrak{o} = F$. By assumption, $a \in F$, Q.E.D.

COROLLARY (of the proof). *If u_1, \dots, u_n is a basis of S_0/K and $u = x_1 u_1 + \dots + x_n u_n$ a generic element of S_0 , then the characteristic polynomial of S_0/K has coefficients in $F[x_1, \dots, x_n]$.*

Our next result shows that in some skew-field extensions obtained entirely by extensions of the constant field, the quantities in question are also invariants.

LEMMA 4.8. *Let K be a function field of genus 0, and let S_0 be a normal skew-field of finite rank m^2 over K . If the different $D\Theta$ of \tilde{S}_0 satisfies $n(N(D)) < 2m^2$, then $l(a^{-1}\Theta'a) = 0$ for all regular $a \in \tilde{S}_0$.*

Proof. The relation $y \in S_0 \cap a^{-1}\Theta'a$ implies $N(y) \in N(\mathfrak{d}^{-1})\mathfrak{o}$, where $\Theta' = \mathfrak{d}^{-1}\Theta$. Using Lemma 4.4, we find that $N(\mathfrak{d}^{-1}) = d^{-m^2}N(D^{-1})$. Now $n(N(\mathfrak{d}^{-1})) = 2m^2 - n(N(D)) > 0$ under our assumptions. Therefore $y = 0$.

This condition holds, for example, in the case $K = F(x)$, F the field of real numbers, $S_0 = K(i, j, k)$, where $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, and $ki = j$. Here all $\delta_P = 0$. It may be of interest to observe that when P has degree $n_P = 1$, then $f_P = 4$, $e_P = 1$ (hence $\delta_P = 0$), and $S_P = K_P(i, j, k)$. And when $n_P = 2$, then $e_P = f_P = 1$ (again $\delta_P = 0$), and $S_P = K_P$. Thus when F is infinite, it can happen that splitting occurs at infinitely many P , and nonsplitting occurs at infinitely many P .

5. The theorems of Witt and Weil

In comparing Theorem 4.1 with the Riemann-Roch theorem of Witt [16, p. 22] we shall first show that Witt's class of divisors is the same as ours. Witt defines divisors as follows: For a separating element x of K , first consider an ideal M_0 in A with respect to $F[x]$. A finite prime divisor P being one for which $\nu_P(x) \geq 0$, consider the closure M_P of M_0 in \tilde{A}_P for finite P . (M_P is shown to be the P -component of one of our divisors in Theorem 2.4.) At the (finite number of) nonfinite $P \in \mathfrak{M}$, introduce "components" formally in any possible way. These "components" and the M_P define a Witt-divisor. Although Witt does not explicitly define these "components", they can only be normal ideals (i.e., those belonging to maximal orders) in \tilde{A}_P with respect to \mathfrak{o}_P , P nonfinite; otherwise his Satz 3, which says that his class of divisors is independent of x , would be false. But our Lemmas 2.4 and 4.1 (local form), plus the obvious fact that a local ideal is open and linearly compact, show that such ideals are P -components of our divisors. Therefore, the set of P -components M_P , one for each $P \in \mathfrak{M}$, defining a Witt-divisor M , is precisely the set of P -components of one of our divisors, and conversely.

Witt defines the degree of a divisor M as the degree in R_0 of $N_0(M)$, where

N_0 is the norm from \tilde{A} to R_0 . Putting aside the question whether at P this norm maps local maximal orders onto \mathfrak{o}_Q , let us take the Witt-degree of M as the degree in R_0 of $N_0(M)\mathfrak{o}_0$. If a is a regular element of R , then the degree $n(a)$ of a in R is the degree $n_0(N_*(a))$ of the norm (from R to R_0) of a . Therefore, by our definition in §4 and our formula (4.2), the Witt-degree of M , which we shall denote as $n^*(M)$, is the negative of our degree $n(M)$.

Witt defines the quantity $\{M\}$, for a divisor M , as $l(M^{-1})$, or $l^*(M)$, in the notation of our Remark 4.1.

The ‘‘complementary’’ divisor M^* to the divisor M^{-1} is defined by Witt¹¹ as that satisfying $M^*M^{-1} = u^{-2}\delta(M_I)$, in the notation of (4.7). By Lemma 4.5, M^{*-1} is what we call M' .

Witt defines a genus G of A by the formula $2G - 2 = n^*(u^{-2}\delta(M_I))$. By Corollary 4.1, $n^*(u^{-2}\delta(M_I)) = 2r^2\xi(S_0)$.

Finally, Witt states his Riemann-Roch theorem as

$$l^*(M) = l^*(M^*) + n^*(M) - G + 1,$$

which agrees with our (4.5) when we determine the \mathfrak{d}_M there by means of the admissible character χ_1 of Lemma 4.5.

We shall now sketch the proof of a theorem which includes that of Weil [15, Ch. I, 3] (with trivial signature). Let $V = r \times r'S_0$ be the space of all matrices of r rows and r' columns over S_0 , a skew-field of finite rank over the center K . As A and B we take $r \times rS_0$ and $r' \times r'S_0$, the actions being the usual matrix multiplication. Let T denote the reduced trace from S_0 to K and Tr the ordinary matrix trace. Then for V' we take $r' \times rS_0$, and we set $\langle v, v' \rangle_0 = T \text{Tr}(vv')$, $v \in V, v' \in V'$. Our dual pairing of \tilde{V} and \tilde{V}' to F is then $[\tilde{v}, \tilde{v}'] = \chi T \text{Tr}(\tilde{v}\tilde{v}')$, for $\tilde{v} \in \tilde{V}, \tilde{v}' \in \tilde{V}'$.

The numbers ρ_1 and ρ_2 of Lemma 3.3 are r'/r and r/r' , respectively.

Letting H denote a member of $\mathfrak{L}(S_0)$, we take for V -divisors subspaces of \tilde{V} of the form $M = a^{-1}(r \times r'H)b$, a regular in \tilde{A} , b regular in \tilde{B} (V' -divisors have the form $b^{-1}(r' \times rH)a$). Our annihilator M' is $b^{-1}(r' \times r\tilde{b}^{-1}H)a$. The degree (3.5) of a divisor M is invariant with respect to all divisors of the form $c^{-1}(r \times r'H)c$, c regular in \tilde{S}_0 . We define the degree of M as

$$\nu(M, r \times r'H) = n(N(a)^{r'/r}N'(b)^{r/r'}),$$

where N is the norm from \tilde{A} to R and N' that from \tilde{B} to R .

The quantity $l(c^{-1}(r \times r'H)c) - l(c^{-1}(r \times r'H)c)$ is the same for all regular $c \in \tilde{S}_0$; it equals $rr'\xi(S_0)$.

Our generalization of the Riemann-Roch theorem to V is

THEOREM 5.1. *If M is a V -divisor, then*

$$l(M) = l(M') + n(M) - rr'\xi(S_0).$$

¹¹ The different appearing in Witt's definition is misprinted as that of $K/F(x)$ instead of $M_i/F(x)$.

This theorem agrees with that of Weil when his signature is identically 1 if we take S_0 to be K and F the field of complex numbers. To verify this agreement, one uses the one-one correspondence between canonical divisors and differentials of K (see [9]).

We could derive Theorem 4.1 from Theorem 5.1 if we used the isomorphism of Theorem 2.3.

BIBLIOGRAPHY

1. A. A. ALBERT, *Structure of algebras*, Amer. Math. Soc. Colloquium Publications, vol. 24, New York, 1939.
2. E. ARTIN, C. J. NESBITT, AND R. M. THRALL, *Rings with minimum condition*, University of Michigan Publications in Mathematics, no. 1, Ann Arbor, 1944.
3. C. CHEVALLEY AND A. WEIL, *Über das Verhalten der Integrale 1. Gattung bei Automorphismen des Funktionenkörpers*, Abh. Math. Sem. Univ. Hamburg, vol. 10 (1934), pp. 358-361.
4. M. DEURING, *Algebren*, Berlin, J. Springer, 1935.
5. H. HASSE, *Über \mathcal{Q} -adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlensysteme*, Math. Ann., vol. 104 (1931), pp. 495-534.
6. ———, *Zahlentheorie*, Berlin, Akademie-Verlag, 1949.
7. E. HECKE, *Über ein Fundamentalproblem aus der Theorie der elliptischen Modulfunktionen*, Abh. Math. Sem. Univ. Hamburg, vol. 6 (1928), pp. 235-257.
8. ———, *Über das Verhalten der Integrale 1. Gattung bei Abbildung, insbesondere in der Theorie der elliptischen Modulfunktionen*, Abh. Math. Sem. Univ. Hamburg, vol. 8 (1931), pp. 271-281.
9. K. IWASAWA, *Algebraic functions*, (mimeographed notes for M67, Fall Term, 1953-1954, M. I. T., Technology Store, Cambridge 39, Mass., February, 1954).
10. ———, *On the rings of valuation vectors*, Ann. of Math. (2), vol. 57 (1953), pp. 331-356.
11. S. LEFSCHETZ, *Algebraic topology*, Amer. Math. Soc. Colloquium Publications, vol. 27, New York, 1942.
12. O. F. G. SCHILLING, *The theory of valuations*, Amer. Math. Soc. Mathematical Surveys, no. 4, New York, 1950.
13. B. L. VAN DER WAERDEN, *Modern algebra, vol. II*, New York, F. Ungar Pub. Co., 1950.
14. A. WEIL, *Über Matrizenringe auf Riemannschen Flächen und den Riemann-Rochschen Satz*, Abh. Math. Sem. Univ. Hamburg, vol. 11 (1936), pp. 110-115.
15. ———, *Généralisation des fonctions abéliennes*, J. Math. Pures Appl. (9), vol. 17 (1938), pp. 47-87.
16. E. WITT, *Riemann-Rochscher Satz und Z -Funktion im Hyperkomplexen*, Math. Ann., vol. 110 (1935), pp. 12-28.
17. C. CHEVALLEY, *Introduction to the theory of algebraic functions of one variable*, Amer. Math. Soc. Mathematical Surveys, no. 6, New York, 1951.
18. T. NAKAYAMA, *Divisionalgebren über diskret bewerteten perfekten Körpern*, J. Reine Angew. Math., vol. 178 (1938), pp. 11-13.

SYLVANIA APPLIED RESEARCH LABORATORY
WALTHAM, MASSACHUSETTS