On the Theorem of Riemann-Roch.

By Tsuneo TAMAGAWA.

A. Weil [1] has discovered that there exists an intimate relation between the topological structure of the idèle ring $\tilde{k}$ of the function field k and the Riemann-Roch theorem. He has given a completely new proof of this theorem, defining the differential as a continuous linear function defined on the module $\tilde{k}/k$. This shows an example of the beautiful harmony which reigns over the arithmetic and the theory of the algebraic function field. As is well known, the notions of idèles and additive idèles have turned out to be the most important in the present day arithmetic, and the standard way of expressing these matters by means of these notions seems to have been now established. The object of the present paper is first to give a proof of the Riemann-Roch theorem in this style, and then to generalize it to "vector spaces", so that it may be applied more conveniently to various cases. In § 4, we give an application of this result to semi-simple algebras, and obtain a theorem of E. Witt [1] and a formula of Hurwitz [1] in a generalized form. It is also not difficult to explain the method of F.K. Schmidt [1] from our standpoint, but this topic will be reserved to another occasion.

The author wishes to express his hearty thanks to Professor K. Iwasawa who has proposed him the problem and given him many useful hints, and to Mr. M. Kuga who has helped him to simplify the proof in § 2.

1. Additive and multiplicative idèles.

Let k be a finite extension of a field $\sum$ with the dimension 1, in which $\sum$ is supposed to be algebraically closed. We shall then call k an *algebraic function field* over $\sum$. A *valuation* of k over $\sum$ is a homomorphism of the multiplicative group k^* of the non-zero elments of k into the additive group of real numbers, satisfying the following conditions.

1. $\nu(a+b) \geqq \text{Min.}\,(\nu(a),\ \nu(b)) \quad (a+b \neq 0)$
2. $\nu(a) = 0 \quad \text{for} \quad a \in \sum$
3. $\nu(k^*) \neq \{0\}$

Put further $\nu(0) = +\infty$, so that ν is defined for all elements of k, and that the condition 1. is satisfied in general. Two valuations ν, ν'

are called *equivalent*: $\nu \sim \nu'$, when there exists a positive number λ such that $\nu'(a) = \lambda\nu(a)$ for all $a \in k^*$. A class of valuations according to this equivalence relation is called a *prime divisor*. We shall denote the prime divisors with the letters like P, Q. To each prime divisor P belongs a *normalized valuation* ν_P, such that $\nu_P(k^*)$ coincides with the set of all rational integers. Put $\mathfrak{o} = \{a\,;\ a \in k,\ \nu_P(a) \geq 0\}$, $\mathfrak{p} = \{a\,;\ a \in k,\ \nu_P(a) > 0\}$. $\mathfrak{o}$ is an integrity domain determined by P, and $\mathfrak{p}$ is a prime ideal in $\mathfrak{o}$. $\mathfrak{o}/\mathfrak{p}$ is an algebraic extension of $\sum$ with a finite degree $n(P)$. Let $\mathfrak{M}$ be the set of all prime divisors of k. A *divisor* of k is an element of the free abelian group D generated by $\mathfrak{M}$. We shall write E for the neutral element of D.

Put $\nu_P(A) = \sum_{P=P_i} e_i$ and $n(A) = \sum_P n(P)\nu_P(A)$ for $A = P_1^{e_1} P_2^{e_2} \ldots P_h^{e_h}$. If $a \in k^*$, there are but finite number of prime divisors P with $\nu_P(a) \neq 0$. The divisor $\Pi_P P^{\nu_P(a)}$ is denoted by (a) and called a *principal divisor*. The mapping $k^* \ni a \rightarrow (a)$ is a homomorphism of k^* into D. The map of k^* by this homomorphism, i.e. the group of all principal divisors is denoted by D_0. Since $\sum_P n(P)\nu_P(a) = 0$ for $a \in k^*$ by the "product formula" we have $n(A) = 0$ for $A \in D_0$. The elements of D/D_0 are called *divisor classes*. $n(A)$ depends clearly only on the class to which A belongs. We shall write $A > B$ for two divisors A, B with $\nu_P(A) \geq \nu_P(B)$ for all $P \in \mathfrak{M}$, and call the *integral divisors* the divisors A such as $A > E$.

Let K be an extension of k with a finite degree, and $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ the extensions in K of a prime divisor P of k. Let p be an element of k with $\nu_P(p) = 1$. Put $e_i = \nu_{\mathfrak{P}_i}(p)$ and $f_i = n(\mathfrak{P}_i)/n(P)$. Then we have $\sum e_i f_i = [K:k]$. An isomorphism of D into D_K (the divisor group of K) is obtained by $P \rightarrow \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_g^{e_g}$. In identifying P with $\mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_g^{e_g}$, D is enbedded in D_K: $D \subset D_K$.

Let k_P be the completion of k with repect to the valuation ν_P, then ν_P is extended to k_P.

The elements (a_P) of the direct sum $\sum_P k_P$ will be called vectors, and denoted by $\tilde{a}$, $\tilde{b}$, ..., a_P, b_P, ... are called the *p-components* of $\tilde{a}$, $\tilde{b}$, ... They are added and multiplicated as follows.

$$\tilde{a} \pm \tilde{b} = (a_P \pm b_P)$$
$$\tilde{a}.\tilde{b} = (a_P . b_P)$$

We shall write $\nu_P(\tilde{a})$ for $\nu_P(a_P)$. An additive idèle $\tilde{a}$ is a vector satisfying the condition:

$\nu_P(\tilde{a}) \geq 0$ for all but a finite number of P.

If $\tilde{a}$ and $\tilde{b}$ are additive idèles, $\tilde{a} \pm \tilde{b}$ and $\tilde{a}.\tilde{b}$ are clearly also additive idèles, and the set of all additive idèles forms a commutative ring $\tilde{k}$. We can associate to an element a of k an additive idèle whose P-component is a for each P. If we identify a with this additive idèle, k becomes a sub-field of $\tilde{k}$, and the unit element of k is also the unit element of k_P. Similarly, we can associate to $a_P \in k_P$ an additive idèle whose P-component is a_P and P'-component is 0 for $P' \neq P$, then k_P becomes also a subring of $\tilde{k}$. We shall denote the unit element of k_P by 1_P. An addilive idèle having an inverse in $\tilde{k}$, will be called an *idèle* of k, and denoted by a small german letter. The set of all idèles forms a multiplicative group J_k in which k^* forms a subgroup. If $\mathfrak{a} = (a_P)$ is an idèle, then $a_P \neq 0$ for all P and $\nu_P(a_P) = 0$ for all but a finite number of P, so that we can associate to each idele $\mathfrak{a}$ a divisor $(\mathfrak{a}) = \Pi P^{\nu_P(\mathfrak{a})}$. $\mathfrak{a} \rightarrow (\mathfrak{a})$ is clearly a homomorphism of J_k *onto* D. Let $\mathfrak{a}$ be an idèle and $\tilde{a}$ an additive idèle, then the product $\mathfrak{a}\,\tilde{a}$ is defined in $\tilde{k}$, so that J_k forms a group of operators on $\tilde{k}$ as a $\sum$-module.

Let K be an algebraic extension of k with a degree n, $w_1, \ldots w_n$, a basis of K/k, and $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ the extensions in K of a prime divisor P of k. If we consider K as a commutative algebra over k, the scalar extension K_P/k_P of K/k is isomorphic with $K_{\mathfrak{P}_1} + \ldots\ldots + K_{\mathfrak{P}_1}$. For each $\tilde{k} \ni \tilde{a} = (a_P)$ we associate an additive idèle $\tilde{a}_K \in K$ whose $\mathfrak{P}$-component is equal to a_P for each $\mathfrak{P}|P$. Identifying $\tilde{a}_K$ with $\tilde{a}$, we can regard $\tilde{k}$ as a subring of K and J_K as a subgroup of J_K. It is easily proved by above remark that $\tilde{K} = \tilde{k}w_1 + \ldots\ldots + \tilde{k}w_n$.

2. Parallelotopes. Theorem of Riemann-Roch.

Put $\mathfrak{o}_P = \{a_P;\ a_P \in k_P,\ \nu_P(a_P) \geq 0\}$ and $\mathfrak{o} = \sum_P \mathfrak{o}_P$. Elements of $\mathfrak{o}$ will be called (additie) *integral idèles*.

Let $\mathfrak{a}$ be an idèle of k. The sub-module $\mathfrak{a}^{-1}\mathfrak{o}$ of $\tilde{k}$ depends clearly only on the divisor $A = (\mathfrak{a})$. We call this module *parallelotope* of the size A, and denote with $\tilde{L}(A)$. If we take the set of all $\tilde{L}(A)$ as a system of neighbourhoods of 0 of $\tilde{k}$, $\tilde{k}$ becomes a topological ring. The necessary and sufficient condition for $\mathfrak{b} \in \tilde{L}((\mathfrak{a}))$, is $\mathfrak{a} \cdot \mathfrak{b} \in \mathfrak{o}$. So if $n(A) < 0$, $\tilde{L}(A)$ contains only one element 0 of k by the product formula, hence k is a discrete set of $\tilde{k}$. Put $L(A) = \tilde{L}(A) \frown k$, then $L(A)$ is a $\sum$-module. We have clearly $\tilde{L}(\mathfrak{b})A) = \mathfrak{b}^{-1}\tilde{L}(A)$, and $L(A(x)) = x^{-1}L(A)$ $x \in k^*$. Hence the rank $l(A)$ of $L(A)$ over $\sum$ depends only on the divisor class of A.

Put $\mathfrak{p}_P = \{a_P;\ a_P \epsilon_P,\ \nu_P(a_P) \geq 1\}$. Then $\mathfrak{p}_P$ is a prime ideal of $\mathfrak{o}_P$ and $\mathfrak{o}_P/\mathfrak{p}_P$ is an algebraic extension of $\sum$ with the degree $n(P)$. Let $w_1^P \ldots\ldots w_{n(P)}^P$ be elements of k_P, whose residue classes mod. $\mathfrak{p}_P$ are linearly independent over $\sum$, and p_P an element of k with $\nu_P(p_P) = 1$. We shall call a system of elements $\{w_1^P, \ldots\ldots, w_n^P;\ p_P\}$ a *uniformizing* *system* at P, an p_P a prime element of P. Each element a_P of k_P has a unique expansion of the following form with respect to a uniformizing system $\{w_1^P, \ldots\ldots, w_n^P; P_P\}$:

$$a_P = \sum_{j > \nu_P(a_P)}^{\infty} \sum_{i=1}^{n(P)} a_{ij} w_i^P p_P^j = \sum_{i,j} f_{ij}^P(a_P) w_i^P p_P^j$$

From now on, we shall consider a uniformizing system associated to each P as fixed once for all. Then we have functions f_{ij}^P for all P and $1 \leq j \leq n(P)$, $-\infty < i < +\infty$. If $\tilde{a} = (a_P)$ is an additive idele, we shall write $f_{ij}^P(\tilde{a})$ instead of $f_{ij}^P(a_P)$. f_{ij}^P is then a linear function mapping $\tilde{k}$ as a $\sum$-module into $\sum$, and if we introduce the discrete topology in $\sum$, f_{ij}^P is a continuous function. It is easily proved that the set $\{f_{ij}^P\}$ is a strong base in the sense of Chevalley of the space of all continuous linear functions of $\tilde{k}$ in $\sum$. Now we can prove the following lemmas and propositions.

Lemma 1. If $A \succ B$, then $\tilde{L}(A) / \tilde{L}(B)$ is a $\sum$-module with the rank $n(A)-n(B)$.

Proof. Let A be a divisor of k. Then $\tilde{a}$ is in $\tilde{L}(A)$ if and only if $f_{ij}^P(\tilde{a}) = 0$ for $i < -\nu_P(A)$. Therefore if $A \succ B$ and $P_1, \ldots\ldots, P_h$ are all the prime divisors such that $\nu_P(A) > \nu_P(B)$, then $\tilde{L}(A) \ni \tilde{a}$ is in $\tilde{L}(B)$ if and only if $f_{ij}^{P_l}(\tilde{a}) = 0$ for $n(A)-n(B)$ functions $f_{ij}^{P_l}$, $1 \leq l \leq h$, $-\nu_{P_l}(A) \leq i < -\nu_{P_l}(B)$, $1 \leq j \leq n(P_l)$. Hence $\tilde{L}(A) / \tilde{L}(B)$ has a rank $n(A) - n(B)$ as a $\sum$-module.

Proposition 1. $l(A)$ is finite for all $A \in D$.
Proof. Let A_1 be a divisor such that $A \succ A_1$, $n(A_1) < 0$. Then we have $L(A_1) = \{0\}$ and $L(B) = L(A) \frown \tilde{L}(B)$ for $A \succ B$, so that

$$L(A) \simeq L(A) \smile \tilde{L}(A_1) / \tilde{L}(A_1) \subseteqq \tilde{L}(A) / \tilde{L}(A_1)$$

Hence $l(A) \leq n(A) - n(A_1) < \infty$.

We shall call l(A) the dimension of the divisor A.

Proposition 2. If k is a purely transcendental extension $\sum(x)$ of $\sum$, then $\mathfrak{o} \smile k = \tilde{k}$.

Proof. There is only one prime divisor P_∞ of k with $\nu_{P_\infty}(x) < 0$. We shall denote other prime divisor with P, Q, ... To each prime divisor $P (\neq P_\infty)$ we associate uniquely an irreducible polynomial $F_P(x) \in \sum[x]$ with highest coefficient 1 such that $\nu_P(F_P(x)) = 1$. Then obviously $\nu_{P'}(F_P(x)) = 0$ for $P' \neq P$, and $\nu_{P_\infty}(F_P(x)) = -n(P)$. We can take the set $\{1, x, \ldots\ldots, x^{n(P)-1}; F_P(x)\}$ as a uniformizing system at P. If a_P is an element of k_P with $\nu_P(a_P) = \mu < 0$, we put

$$H_P(x) = \sum_{i=-\mu}^{-1} \sum_{j=1}^{n(P)} f_{ij}^{P}(a_P) x^{j-1} (F_P(x))^{\mu+i}$$

then $\nu_P(a_P - H_P(x) / (F_P(x))^{\mu}) \geq 0$ and $\nu_{P'}(H_P(x) / F_P(x)^{\mu}) \geq 0$ for $P' \neq P$. As to P_∞, $\nu_{P\infty}(H_P(x) / F_P(x)^{\nu}) = \mu n(P) - \deg H_P(x) > 0$, hence $a_P - H_P(x) / (F_P(x))^{\mu} \epsilon \mathfrak{o}$ On the other hand, $1/x$ is a prime element of P_∞ and $n(P_\infty) = 1$, so $\{1 : 1/x\}$ is a uniformizing system at P_∞. If $a_{P\infty}$ is an element of $k_{P\infty}$ with $-\mu = \nu_{P\infty}(a_{P\infty}) < 0$, we put

$$H_\infty = \sum_{i=-1}^{-\mu} f_{i1}^{P\infty}(a_{P\infty}) x^{-i}$$

then it is easily proved as above that $a_{P\infty} - H_{P\infty}(x) \epsilon \mathfrak{o}$.

Let $\tilde{a} = (a_P)$ be a non integral idèle, and $P_1, \ldots\ldots P_h$ all the prime divisors such that $\nu_{P_l}(\tilde{a}) < 0$. To each a_{P_l} we associate a polynomial $H_{P_l}(x)$ as above and put

$$z = \sum_l H_{P_l}(x) / F_{P_l}(x)^{-\nu_{P_l}(\tilde{a})} + H_{P\infty}(x)$$

(The last term appears only when one of P_l is P_∞.) Then $\tilde{a} - z$ is ocviously an element of $\mathfrak{o}$, hence it follows that $\tilde{a} \epsilon \mathfrak{o} \smile k$. Our assertion is thereby proved.

Proposition 3. Let A be an arbitrary divisor of k, then

$$\tilde{k} / \tilde{L}(A) \smile k$$

is a $\sum$-module with a finite rank. If $r(A)$ is its rank, $n(A) - l(A) + r(A)$ is a constant depending only on k, and not on A.

Proof. Let $x \epsilon k$ be a transcendental element over $\sum$. Put $k_0 = \sum(x)$, k is then an algebraic extension of k_0. Set $n = [k : k_0]$. Let $w_1, \ldots, w_n$ be a relative basis of k over k_0. We can take an integral divisor A_0 such that $A_0 \succ (w_i)^{-1}$ for $1 \leq i \leq n$, then clearly $L(A_0) \ni w_1, \ldots\ldots, w_n$. So we have by Proposition 2: $\tilde{L}(A_0) \smile k_0 \supset \tilde{k}_0$. Hence $\tilde{L}(A_0) \smile k \supseteq \tilde{k}_0 w_1 + \ldots\ldots + \tilde{k}_0 w_n = \tilde{k}$. Take a divisor A_1 such that $A_1 \succ A_0$, $A_1 \succ A$. Then we have obviously $\tilde{L}(A_1) \smile k = \tilde{k}$, and

$$\begin{aligned} \tilde{k} / \tilde{L}(A) \smile k &= \tilde{L}(A_1) \smile k / \tilde{L}(A) \smile k \\ &\simeq \tilde{L}(A_1) / \tilde{L}(A_1) \frown (\tilde{L}(A) \smile k) = \tilde{L}(A_1) / \tilde{L}(A) \smile L(A_1), \\ \tilde{L}(A) \smile L(A_1) / \tilde{L}(A) &\simeq L(A_1) / \tilde{L}(A) \frown L(A_1) = L(A_1) / L(A). \end{aligned}$$

Hence $\qquad r(A) = n(A_1) - n(A) - (l(A_1) - l(A)) < \infty$

If in particular $\tilde{L}(A) \smile k = \tilde{k}$, we have $n(A_1) - l(A_1) = n(A) - l(A)$.

So if $\tilde{L}(A_1) \smile k = \tilde{k}$, $\tilde{L}(A_2) \smile k = \tilde{k}$, and $A_3 \succ A_1$, $A_3 \succ A_2$,

$$n(A_1) - l(A_1) = n(A_3) - l(A_3) = n(A_2) - l(A_2).$$

Therefore $n(A_1) - l(A_1)$ is constant for all A_1 satisfying $\tilde{L}(A_1) \smile k = \tilde{k}$.

So $r(A)+n(A)-l(A)$ does not depend on A as

$$r(A)+n(A)-l(A)=n(A_0)-l(A_0)$$

Remark: From Proposition 3, we see that $r(A)$ depends only on divisor class of A.

The constant value of $r(A)+n(A)-l(A)+1$ is called the genus of k, and denoted by g. Putting $A=E$, we see $g\geq 0$. Moreover if k is rational function field over $\sum$, i.e. the purely transcendental extension of $\sum$, the genus of k is equal to 0 by Proposition 2. We have clearly $r(A)\geq 0$. Further, $r(A)\leq r(B)$ for $A\succ B$. A divisor A with $r(A)=0$ is called *non special*. As shown in the proof of the Proposition 3, there exists at least one non special divisor A_0.

Proposition 4. There is a constant m, such that all A with $n(A)\geq m$ are non special.

Proof. Let A_0 be a non special prime divisor. Put $m=n(A_0)+g$. If $n(A)\geq m$, we have $l(A/A_0)\geq n(A/A_0)-g+1\geq 1$. Hence there is an element $x\neq 0$ in $L(A/A_0)$. Put $B=(x)$. A/A_0. So we have obviously $B\succ E$ and $r(A_0B)=0$. as $A_0B\succ B$. Hence

$$r(A)=r(A(x))=r(A_0B)=0.$$

Now a mapping f of $\tilde{k}$ into $\sum$ satisfying the following three conditions will be called a *differential* of k.

1. f is linear, i.e. $\sum\ni\alpha,\beta$ and $\tilde{k}\ni\tilde{a},\tilde{b}$, implies

$$f(\alpha\tilde{a}+\beta\tilde{b})=\alpha f(\tilde{a})+\beta f(\tilde{b})$$

2. f is continuous, i.e. there exists a divisor A such that

$$\tilde{L}(A)\ni\tilde{a} \text{ implies } f(\tilde{a})=0.$$

3. f maps k to 0.

Let A be a given divisor. Then the set of all differentials mapping all elements of $\tilde{L}(A)$ to 0 forms a $\sum$-module, whose rank is obviously equal to the rank $\tilde{k}/\tilde{L}(A)\cup k=r(A)$. If we denote this $\sum$-module with $\mathfrak{L}_A$, the Proposition 3 may be expressed as follows.

$$l(A)=n(A)-g+1+\text{rank }\mathfrak{L}_A.$$

Now the set D of the divisors of k forms obviously a distributive lattice with the order relation $A\succ B$. We have clearly $\tilde{L}(A\cup B)=\tilde{L}(A)\cup\tilde{L}(B)$, $L(A\cap B)=\tilde{L}(A)\cap\tilde{L}(B)$. If f is a differential $\neq 0$, $D_f=\{A\,;\,A\in D,\ \mathfrak{L}_A\ni f\}$ forms a sublattice of D. There is the maximal value of $n(A)$ for $A \epsilon \mathfrak{L}_A$, as $f \epsilon \mathfrak{L}_A$ for $n(A) \geq m$ by Prop. 4. Let $n(C)$, $C_y \epsilon D_f$ be this maximal value. As we have clearly $n(A) > n(B)$ for $A \succ B$, $A \neq B$, $D_f \ni A$ implies $C \succ A$. Since this divisor is determined by the differential $f \neq 0$, we shall write $C = (f)$.

Let $\mathfrak{L}$ be the module of all differentials. For $f \epsilon L$ we define a differential $x \cdot f$ by

$$xf(\bar{a}) = f(x\bar{a})$$

so that $\mathfrak{L}$ becomes a k-module. Clearly $(x.f) = (x). (f)$.

Proposition 5. $\mathfrak{L}$ is a 1-dimensional k-module.

Proof. Suppose f_1, f_2 be two linearly indepent differentials over k. Let ν be a natural number, and P an arbitrary prime divisor. We have

$$\dim\ (P^{\nu}(f_1)) = r \geq \nu n(P) + n((f_1)) - g + 1$$

$$\dim\ (P^{\nu}(f_2)) = s \geq \nu n(P) + n((f_2)) - g + 1.$$

Let $x_1, \ldots, x_r \epsilon L(P^{\nu}(f_1))$ and $y_1, \ldots, y_s \epsilon L(P^{\nu}(\mathrm{f}_2))$ be linearly independent over $\sum$, then $x_1 f_1, \ldots, x_r f_1, y_1 f_2, \ldots, y_s f_2$, are linearly independent over $\sum$, and $P^{-\nu} \prec (x_i f_1)$ as $x_i \epsilon L(P^{\nu}(f_1))$, $P^{-\nu} \prec (y_j f_2)$ as $y_j \epsilon (P^{\nu}(f_2))$, so that

$$r(P^{-\nu}) = \nu n(P) + g - 1 \geq r + s.$$

Hence

$$\nu.n(P) + g - 1 \geq 2\nu.n(P) + n((f_1)) + n((f_2)) - 2g + 2.$$

This leads to a contradiction, when $\nu \to \infty$, therefore $\mathfrak{L}$ is l-dimensional over k.

By the above proposition and the remark $(xf) = (x)(f)$, the set of divisors (f) $(f \epsilon L, f \neq 0)$ forms a divisor class, which be called the *canonical class* of k.

Theorem 1. (Theorem of Riemann-Roch). Let A be a divisor and f_0 a diffenrential $\neq 0$. Then it follows

$$l(A) = n(A) - g + 1 + l((f_0)A^{-1}).$$

Proof. We have only to show $\dim L_A = l((f_0)A^{-1})$. $\mathfrak{L}_A \ni f$ means $(f) \succ A$. We may write $f = x.f$ according to Proposition 4. This is equivalent with $(x) \succ A(f_0)^{-1}$. The number of such linearly independent x's are clearly $l((f_0)A^{-1})$.

C rollary. $l((f_0)) = g$, $n((f_0)) = 2g - 2$.

§ 3. Vector spaces.

Let M be an n-dimensional vector space over k, and $\mathbf{e}_1, \ldots, \mathbf{e}_n$ a basis of M over k. Then the "completion" $\tilde{M} = \tilde{k}\mathbf{e}_1 + \ldots. + \tilde{k}\mathbf{e}_n$ of M is determined by M, independently of the basis $\mathbf{e}_1, \ldots., \mathbf{e}_n$. $\tilde{M}$ is a $k-\sum-$ module, containing M and $M_P = k_P\mathbf{e}_1 + \ldots. + k_P\mathbf{e}_n$, as submodules.

Now take for each prime divisor P of k a submodule Π_P of M_P satisfying the following conditions.

i) Π_P is a finite $\mathfrak{o}_P$-module, containning a k_P-basis of M_P.

2) $\Pi_P = \mathfrak{o}_P\mathbf{e}_1 + \ldots. + \mathfrak{o}_P\mathbf{e}_n$, except for a finite number of P.

Then a submodule Π of M of the form $\Pi = \sum_P \Pi_P$ is called a *parallelotope*. In this definition a basis $\mathbf{e}_1, \ldots., \mathbf{e}_n$ of M over k is used, but obviously it is independent of the choice of basis whether a submodule Π of M is or is not a parallelotope. The paralleletope may be also defined as follows:

A submodule Π of M is a parallelotope, when it satisfies the following conditions.

1′) Π is an $\mathfrak{o}$-module.

2′) A, $A_{\prime}$ being certain divisors, $\tilde{L}(A)\,\mathbf{e}_1 + \ldots. + (A)\mathbf{e}_n < \Pi < \tilde{L}(A')\,\mathbf{e}_1 + \ldots. + \tilde{L}(A')\,\mathbf{e}_n$.

It is clear that these two definitions of the parallelotopes are equivalent. A module of the form $\tilde{L}(A)\,\mathbf{e}_1 + \ldots. + \tilde{L}(A)\,\mathbf{e}_n$ satisfies 1), 2), then this module is a parallelotope. Π_P is called the *P-component* of a parallelotope $\Pi = \sum \Pi_P$. When Π', Π'' are parallelotopes, so are also $\Pi' \smile \Pi''$, $\Pi' \frown \Pi''$.

Let $\Pi = \sum_P \Pi_P$ be a parallelotope. Let $\mathbf{a}_P^1, \ldots., \mathbf{a}_n^P$ be an $\mathfrak{o}_P$-basis of Π_P and put $\mathbf{a}_i^P = \sum a_{ij}^P \mathbf{e}_j$, $a_{ji}^P \epsilon k_P$. Denote with $\mathfrak{a} = (a_P)$ the idèle with the compodent $a_P = |a_{ji}^P|$. The divisor $(\mathfrak{a})$ is determined by Π independently of the basis $\mathbf{a}_i^P$. The divisor $(\mathfrak{a})$ is called the *norm* of Π and denoted by $N(\Pi)$. Obviously $\Pi > \Pi'$ implieses $N(\Pi) \prec N(\Pi')$. If $\mathbf{e}'_1, \ldots., \mathbf{e}'_n$ is another basis of M over k, and $\mathbf{e}_i = \sum a_{ji}\mathbf{e}'_j$, the norm $N'(\Pi)$ of Π formed with the basis $\mathbf{e}_1', \ldots., \mathbf{e}'_n$ instead of $\mathbf{e}_1, \ldots, \mathbf{e}_n$ is obtained from $N(\Pi)$ by $N'(\Pi) = (a)\,N(\Pi)$ where $a = |a_{ji}|$. Then $V(\Pi) = n(N(\Pi)^{-1})$ is independent of the choice of basis. $V(\Pi)$ is called the *volume* of the parallelotope Π. Tne following lemma is proved the same way as the lemma 1 of § 3.

Lemma 2. If $\Pi > \Pi'$, the rank of the $\sum$-module Π/Π' is equal to $V(\Pi) - (\Pi')$.

In particular, we have $V(\tilde{L}(A)\,\mathbf{e}_1 + \ldots. + \tilde{L}(A)\,\mathbf{e}_n) = n \cdot n(A)$. Now we shall write $M/M(\Pi) = \Pi \smile M$. Then we have.

Proposition 6. $M(\Pi)$ and $M(\Pi) \smile M$ are finite $\sum$-modules.

If $\lambda(\Pi)$, $\rho(\Pi)$ are their ranks respectively, it holds

$$\lambda(\Pi) = V(\Pi) - n(g-1) + \rho(\Pi).$$

Proof. Take two divisors A_0, A_1 such that $\Pi_0 = \tilde{L}(A_0)\mathbf{e}_1 + \dots + \tilde{L}(A_0)\mathbf{e}_n \subset \Pi \subset \tilde{L}(A_1)\mathbf{e}_1 + \dots + \tilde{L}(A_1)\mathbf{e}_n = \Pi_1$. We may suppose also $r(A_1) = 0$ in virtue of Proposition 4. $M(\Pi_0)$ is a $\sum$-module of dimension $n \cdot l(A_0)$. Furthermore we have

$$M(\Pi)/M(\Pi_0) \simeq M(\Pi) \cup \Pi_0 / \Pi_0 \subset \Pi/\Pi_0$$

so that $M(\Pi)$ is a $\sum$-module whose dimension $nl(A) + V(\Pi) - n.n(A)$. As $r(A_1) = 0$, we have $L(A_1) \cup k = \tilde{k}$, $\Pi_1 \cup M = M$, so that

$$M/\Pi \cup k = \Pi_1 \cup k/\Pi \cup k \cong \Pi_1/\Pi_1 \cap (\Pi \cup k) = \Pi_1/\Pi \cup M(\Pi_1).$$

hence

$$\rho(\Pi) = V(\Pi_1) - V(\Pi) - (\lambda(\Pi_1) - \lambda(\Pi))$$

so that

$$l(\Pi) = V(\Pi) - n(g-1) + \rho(\Pi)$$

A mapping of $\tilde{M}$ into $\sum$ is called a *differential* of M, when it satisfies the following conditions.

1) $\tilde{M} \ni \tilde{\mathbf{a}}, \tilde{\mathbf{b}}$ and $\sum \ni \alpha, \beta$ implies $\Phi(\alpha \cdot \tilde{\mathbf{a}} + \beta\tilde{\mathbf{b}}) = \alpha\Phi(\tilde{\mathbf{a}}) + \beta\Phi(\tilde{\mathbf{b}})$

2) There is a certain parallelotope Π so that $\Phi(\tilde{\mathbf{a}}) = 0$ for all $\tilde{\mathbf{a}} \in \Pi$.

3) $\Phi(\mathbf{a}) = 0$ for all $\mathbf{a} \in M$.

Now, let Π be a fixed Parallelotope, the set of differentials Φ, such that $\Phi(\tilde{\mathbf{a}}) = 0$ for all $\tilde{\mathbf{a}} \in \Pi$, a $\sum$-module, which will be deneted by L_Π. We have by Proposition 5; dim $\mathfrak{L}_\Pi = \rho(\Pi)$.

A differential Φ of M determines n differentials $f_1, \dots, f_n$ of k, by $f_i(\tilde{\alpha}) = \Phi(\tilde{\alpha}\mathbf{e}_i)$ for $\tilde{\alpha} \in \tilde{k}$. Conversely n differentials $f_1, \dots, f_n$ of k determine a differential Φ of M by $\Phi(\sum \tilde{\alpha}_i \mathbf{e}_i) = \sum f_i(\tilde{\alpha}_i)$. If a basis $\mathbf{e}_1, \dots, \mathbf{e}_n$ of M over k is fixed, this correspondence between Φ and $\{f_1, \dots, f_n\}$ is obviously one-to-one. Hence the set of all differentials forms an n-dimensional k-module.

Now, we shall define the inner product $(\mathbf{a}, \mathbf{b})$ for $\mathbf{a}, \mathbf{b} \in M$. It is a k-valued function of $\mathbf{a}, \mathbf{b} \in M$ satisfying the following conditions.

1. $(\mathbf{a}, \mathbf{b}) = (\mathbf{b}, \mathbf{a})$
2. $(\alpha\mathbf{a} + \alpha'\mathbf{a}', \mathbf{b}) = \alpha(\mathbf{a}, \mathbf{b}) + \alpha'(\mathbf{a}', \mathbf{b})$ for $\alpha, \alpha' \in k$.
3. If $\mathbf{a} \neq 0$, there exists $\mathbf{b} \in M$ such that $(\mathbf{a}, \mathbf{b}) \neq 0$.

Then we can take for a given basis $\mathbf{e}_1, \dots, \mathbf{e}_n$ of M over k, the "dual basis" $\mathbf{e}_1^*, \dots, \mathbf{e}_n^*$ such that $(\mathbf{e}_i, \mathbf{e}_j^*) = \delta_{ij}$. The domain of definition of the inner product can be extended te $\tilde{M}$ by

$$(\sum_i \tilde{a}_i \mathbf{e}_i\,,\ \sum_i \tilde{b}_i \mathbf{e}_i^*) = \sum_i \tilde{a}_i \tilde{b}_i$$

Let H be a parallelotope. We shall define the *dual parallelotope* H^* of H by

$$H^* = \{\tilde{\mathbf{a}}\,;\ \tilde{\mathbf{a}} \epsilon \tilde{M}\ (\tilde{\mathbf{a}},\ \tilde{\mathbf{b}}) \epsilon\, \mathfrak{o} \text{ for all } \tilde{\mathbf{b}} \epsilon H\}.$$

It can be proved without difficulty that H^* is a parallelotope satisfying

1. $(H^*)^* = H$
2. $V(H^*) = -V(H)$

Let f be a differential of k and $\mathbf{a} \epsilon M$. We shall define a differential $\mathbf{a}\cdot f$ of M by

$$\mathbf{a}\cdot f(\tilde{\mathbf{b}}) = f((\mathbf{a},\ \tilde{\mathbf{b}}))\,.$$

Suppose $f_0 \neq 0$, let Φ be an arbitrary differential of M, $f_1, \ldots\ldots, f_n$ the differentials of k corresponding to Φ as defined above. We can write $f_i = \tilde{a}_i f_0$ in vertue of Proposition 4. Then

$$\Phi(\sum \tilde{\mathbf{b}}_i \cdot \mathbf{e}_i) = f_0(\sum a_i b_i) = [\sum a_i \mathbf{e}_i^*] f_0(\sum \tilde{\mathbf{b}}_i \mathbf{e}_i)$$

so that every differential of M is expressible in the form $\mathbf{a}\cdot f_0$. It is easily shown that $\Phi = \mathbf{a} f_0 \epsilon\, \mathfrak{L}_H$, H being a given parallelotope, if and only if $(\mathbf{a},\ \mathbf{b}) \epsilon \tilde{L}((f_0))$. for all $\tilde{\mathbf{b}} \epsilon H$. On the other hand, let $\mathfrak{d}_0$ be an idele of k such that $(f_0) = \mathfrak{d}_0)$. Then we have $(\mathbf{a},\ \mathbf{b}) \epsilon L(\mathfrak{g}_0)$ if and only if $\mathbf{a} \epsilon M\ (\mathfrak{d}_0^{-1} H^*)$. From all this follows the following "Theorem of Riemann-Roch for vector spaces".

Theorem 2. $\lambda(H) = V(H) - n(g-1) + \lambda(\mathfrak{d}^{-1} H^*)$.

4. Separable semi-simple algebras.

k being a function field as before, let S be a separable semi-simple algebra over k with a rank n. If $S \ni \omega_1, \ldots\ldots, \omega_n$ are linearly independent over k, the structure of $\tilde{S}$ is determined by n^3 "constants of structure" $c_{ij}^l \epsilon k$:

$$\omega_i \cdot \omega_j = \sum_l c_{ij}^l \omega_l \qquad *$$

Considering S as a vector space over k, we shall use the same notations as in § 3.

Put $\tilde{S} = \tilde{k}\omega_1 \ldots\ldots + \tilde{k}\omega_n$. Extending the relations (*) to $\tilde{S}$, we can regard $\tilde{S}$ as a ring, which is generally non commutative. An element of S will be called an *additive idèle* of S, an element of S with an inverse in $\tilde{S}$ an *idèle* of S, and the multiplicative group of all idèles, idèle group J of S.

We can naturally regard S, S_p k, k_p, $\tilde{k}$ and J_k as subsets of S. If

$J_S \ni \mathfrak{A}$, then $\mathfrak{A}\cdot\omega_j = \sum \tilde{a}_{ij}\omega_i$ with $\tilde{a}_{ij} \in \tilde{k}$, and

$$\mathfrak{A} = |\tilde{a}_{ij}|$$

is in J_k. We shall call $\mathfrak{a}$ the *norm* of $\mathfrak{a}$ and denote by

$$N_{S/k}(\mathfrak{A}) = \mathfrak{a}$$

Proposition 7. $\mathfrak{o}_P\omega_1 + , \dots + \mathfrak{o}_P\omega_n$ is a maximal domain of integrity of S_P except for a finite number of P.

Proof. We have $\nu_P(c^l_{ij}) \geq 0$, $1 \leq i, j, \leq n$ for all but a finite number of P. So $\mathfrak{o}_P\omega_1 + \dots + \mathfrak{o}_P\omega_n$ is a domain of integrity of S_P. Let $T\cdot\zeta$ be principal trace of $\zeta \in S$, i.e. the sum of the traces of matrices corresponding to ζ in all inequivalent absolutely irreducible representations of S. So

$$D(\omega) = |T\cdot\omega_i\omega_j| \neq 0$$

because S is separable over k. $\nu_P(D(\omega))$ is 0 for all but a finite number of P. If $\nu_P(c^l_{ij}) \geq 0$, $1 \leq i, j, l \leq n$, and $\nu_P(D(\omega)) = 0$, $\mathfrak{o}_P\omega_1 + \dots + \mathfrak{o}_P\omega_n$ is clearly a maiximal domain of integrity of S_P.

If every P-component O_P of parallelotope O of S are maximal domain of integrity, we shall call O a *principal parallelotope*. In the following, we shall consider a fixed principal parallelotope. Every principal parallelotope O' of S can be then expressed in the following form with a suitable idèle $\mathfrak{A}$.

$$O' = \mathfrak{A}^{-1}O\mathfrak{A}$$

To each P, we determine a minimal basis $\eta_1^P, \dots, \eta_n^P$ of O_P over $\mathfrak{o}_P$ and set

$$d_P = D(\eta^P) = |T\eta_i^P\cdot\eta_j^P|$$

Then the vector $\mathfrak{d}$ of k whose P-component is d_P for each P is clearly an idèle of k, and the divisor $(\mathfrak{d})$ depends only on S and not on the choice of O. We shall call $D = (\mathfrak{d})$ the *discriminant* of S.

Proposition 8. Let $d = n((\mathfrak{d}))$, then the volume of every principal parallelotope is $-\frac{1}{2}d$.

Proof. Let $\eta_j^P = \sum_i c_{jj}^P \quad c_{ij}^P \in k_P$.
then

$$D(\eta^P) = |c_{ij}^P|^2 D(\omega)$$
$$d = n(D) = 2\textstyle\sum_P n(P)\nu_P(|c_{ij}^P|) = -2V(O).$$

Put $(\xi, \eta) = T\xi\cdot\eta$ for $\xi, \eta \in S$, then (ξ, η) satisfies the conditions for the inner product in §3, and can be regarded as such.

Put

$$\Delta_p = \{\xi_p ;\ \xi_p \epsilon S,\ (\xi_p,\ \zeta_p) \epsilon \mathfrak{o}_p \text{ for all all } \zeta_p \epsilon \mathfrak{o}_p\}$$

Δ_p^{-1} is then "Differente" of O_p, and $\sum'_p \Delta_p = O^*$ is a parallelotope of S which is dual to O with respect to the above defined inner product. Put $\Delta_p = \delta_p O_p$. The idèle $\mathfrak{D} = (\delta_p)$ will be called the *Diffarente idele* of O. It is obvious that $O^* = \mathfrak{D}^{-1} O = O\mathfrak{D}^{-1}$, and the discriminant of S coincides with $(N_{S/k}\mathfrak{D})$.

Let $\mathfrak{A}$ be an arbitrary idele of S, then the volume of the parallelotope $\mathfrak{A}\cdot O$ is obviously $-n((N_{S/k}\mathfrak{A})) + V(O)$, and the dual of $\mathfrak{A}\cdot O$ is $O^*\mathfrak{A}^{-1} = O\mathfrak{D}^{-1}\mathfrak{A}^{-1}$

Put

$$\lambda(\mathfrak{A}^{-1} O) = l(\mathfrak{A}),\ \lambda(O \cdot \mathfrak{A}^{-1}) = \mathfrak{l}(\mathfrak{A})$$

$$n(N_{S/k}(\mathfrak{A})) = n(\mathfrak{A})$$

Let f_0 be a differential $\neq 0$ of k and $\mathfrak{d}_0$ an idèle of k with $(\mathfrak{d}_0) = (f_0)$. Then applying the Theorem 2, we obtain the following theorem.

Theorem 3. (Theorem of Riemann-Roch for S)

$$l(\mathfrak{A}) = n(\mathfrak{A}) - n(g-1) - \frac{1}{2}d + \mathfrak{l}(\mathfrak{A}^{-1}\Delta\vartheta_0)$$

Each differential Φ of S is defined by f_0, $\xi \epsilon S$ as follows.

$$\Phi(\eta) = \xi \cdot f_0(\eta) = f_0(T\xi \cdot \eta),\ \xi \epsilon S,\ \eta \epsilon \check{S}.$$

If S coincides in particular with an algebraic extension K of k, then Theorem 3 coincides with R-R- Theorem on K, and genus G of K can be expressed by g as follows.

$$2G - 2 = n(2g-2) + d$$

This is the well known formula of Hurwitz.

References

A. Hurwitz. [1] Über algebraische Gebilde mit eindeutigen Transformationen in sich. Math. Ann. 41 (1893).

F. K. Schmidt. [1] Zur algebraischen Theorie der algebraischen Funktionen I. Math. Zeit. 41 (1936).

A. Weil. [1] Zur algebraischen Theorie der algebraischen Funktionen. Journ. rein. angew. Math. 179 (1938).

E. Witt. [1] Riemann-Rochscher S tz und Z-Funktion im Hyperkomplexen. Math. Ann. 110 (1935).