Inventiones math. 9, 318–344 (1970)

Algebraic K-Theory and Quadratic Forms

JOHN MILNOR (Cambridge, Massachusetts)

The first section of this paper defines and studies a graded ring K_*F associated to any field F. By definition, K_nF is the target group of the universal n-linear function from $F^\bullet \times \cdots \times F^\bullet$ to an additive group, satisfying the condition that $a_1 \times \cdots \times a_n$ should map to zero whenever $a_i + a_{i+1} = 1$. Here $F^\bullet$ denotes the multiplicative group $F - 0$.

Section 2 constructs a homomorphism $\partial\colon K_nF \to K_{n-1}\bar{F}$ associated with a discrete valuation on F with residue class field $\bar{F}$. These homomorphisms ∂ are used to compute the ring $K_*F(t)$ of a rational function field, using a technique due to John Tate.

Section 3 relates K_*F to the theory of quadratic modules by defining certain "Stiefel-Whitney invariants" of a quadratic module over a field F of characteristic $\neq 2$. The definition is closely related to Delzant [5].

Let W be the Witt ring of anisotropic quadratic modules over F, and let $I \subset W$ be the maximal ideal, consisting of modules of even rank. Section 4 studies the conjecture that the associated graded ring

$$(W/I, I/I^2, I^2/I^3, \ldots)$$

is canonically isomorphic to $K_*F/2K_*F$. Section 5 computes the Witt ring of a field $F(t)$ of rational functions.

Section 6 describes the conjecture that $K_*F/2K_*F$ is canonically isomorphic to the cohomology ring $H^*(G_F; Z/2Z)$; where G_F denotes the Galois group of the separable closure of F. An appendix, due to Tate, computes $K_*F/2K_*F$ for a global field.

Throughout the exposition I have made free use of unpublished theorems and ideas due to Bass and Tate. I want particularly to thank Tate for his generous help.

§1. The Ring K_*F

To any field F we associate a graded ring

$$K_*F = (K_0F, K_1F, K_2F, \ldots)$$

as follows. By definition, K_1F is just the multiplicative group $F^\bullet$ written additively. To keep notation straight, we introduce the canonical isomorphism

$$l\colon F^\bullet \to K_1F,$$

where $l(a\,b)=l(a)+l(b)$. Then K_*F is defined to be the quotient of the tensor algebra

$$(Z,\ K_1F,\ K_1F\otimes K_1F,\ K_1F\otimes K_1F\otimes K_1F,\ldots)$$

by the ideal generated by all $l(a)\otimes l(1-a)$, with $a\neq 0, 1$. In other words each $K_nF, n\geqq 2$, is the quotient of the n-fold tensor product $K_1F\otimes\cdots\otimes K_1F$ by the subgroup generated by all $l(a_1)\otimes\cdots\otimes l(a_n)$ such that $a_i+a_{i+1}=1$ for some i.

In terms of generators and relations, K_*F can be described as the associative ring with unit which is generated by symbols $l(a)$, $a\in F^*$, subject only to the defining relations $l(a\,b)=l(a)+l(b)$ and $l(a)\,l(1-a)=0$.

Explanation. This definition of the group K_2F is motivated by work of R. Steinberg, C. Moore, and H. Matsumoto on algebraic groups; and has already been the object of much study. (Compare references [2–4, 7–9, 17].) For $n\geqq 3$, the definition is purely ad hoc. Quite different definition of K_n for $n\geqq 3$ have been proposed by Swan [18] and by Nobile and Villamayor [11]; but no relationship between the various definitions is known.

First let us describe some fundamental properties of the ring K_*F. (Examples will be given in §§ 1.5–1.8.)

Lemma 1.1. *For every $\xi\in K_mF$ and every $\eta\in K_nF$, the identity*

$$\eta\,\xi=(-1)^{mn}\,\xi\,\eta$$

is valid in $K_{m+n}F$.

Proof (following Steinberg). Clearly it suffices to consider the case $m=n=1$. Since $-a=(1-a)/(1-a^{-1})$ for $a\neq 1$, we have

$$\begin{aligned} l(a)\,l(-a)&=l(a)\,l(1-a)-l(a)\,l(1-a^{-1})\\ &=l(a)\,l(1-a)+l(a^{-1})\,l(1-a^{-1})=0. \end{aligned}$$

Hence the sum $l(a)\,l(b)+l(b)\,l(a)$ is equal to

$$\begin{aligned} &l(a)\,l(-a)+l(a)\,l(b)+l(b)\,l(a)+l(b)\,l(-b)\\ &\quad=l(a)\,l(-a\,b)+l(b)\,l(-a\,b)\\ &\quad=l(a\,b)\,l(-a\,b)=0; \end{aligned}$$

which completes the proof.

Here are two further consequences of this argument:

Lemma 1.2. *The identity $l(a)^2=l(a)\,l(-1)$ is valid for every $l(a)\in K_1F$.*

For the equation $l(a)\,l(-a)=0$ implies that $l(a)^2=l(a)\,(l(-1)+l(-a))$ must be equal to $l(a)\,l(-1)$.

Lemma 1.3. *If the sum $a_1+\cdots+a_n$ of non-zero field elements is equal to either 0 or 1, then $l(a_1)\ldots l(a_n)=0$.*

Proof by Induction on n. The statement is certainly true for $n=1, 2$; so we may assume that $n\geqq 3$. If $a_1+a_2=0$, then the product $l(a_1)\,l(a_2)$ is already zero. But if $a_1+a_2\neq 0$, then the equation

$$a_1/(a_1+a_2)+a_2/(a_1+a_2)=1$$

implies that

$$\big(l(a_1)-l(a_1+a_2)\big)\big(l(a_2)-l(a_1+a_2)\big)=0.$$

Multiplying by $l(a_3)\ldots l(a_n)$, and using 1.1 and the inductive hypothesis that

$$l(a_1+a_2)\,l(a_3)\ldots l(a_n)=0,$$

the conclusion follows.

Here is an application.

Theorem 1.4. *The element -1 is a sum of squares in F if and only if every positive dimensional element of K_*F is nilpotent.*

Proof. If -1 is not a sum of squares, then F can be embedded in a real closed field, and hence can be ordered. Choosing some fixed ordering, define an n-linear mapping from $K_1F\times\cdots\times K_1F$ to the integers modulo 2 by the correspondence

$$l(a_1)\times\cdots\times l(a_n)\mapsto \frac{1-\operatorname{sgn}(a_1)}{2}\cdots\frac{1-\operatorname{sgn}(a_n)}{2}.$$

Evidently the right hand side is zero whenever $a_i+a_{i+1}=1$. Hence this correspondence induces a homomorphism

$$K_nF\to Z/2Z;$$

which carries $l(-1)^n$ to 1. This proves that the element $l(-1)$ is not nilpotent.

Conversely, if say $-1=a_1^2+\cdots+a_r^2$, then it follows from 1.3 that

$$l(-a_1^2)\ldots l(-a_r^2)=0;$$

hence

$$l(-1)^r\equiv 0 \bmod 2K_rF.$$

Since $2l(-1)=0$, it follows immediately that $l(-1)^{r+1}=0$.

For any generator $\gamma=l(a_1)\ldots l(a_n)$ of the group K_nF, it follows from 1.2 that γ^s is equal to a multiple of $l(-1)^{n(s-1)}$. Hence $\gamma^s=0$ whenever $n(s-1)>r$. Similarly, for any sum $\gamma_1+\cdots+\gamma_k$ of generators, the power $(\gamma_1+\cdots+\gamma_k)^s$ can be expressed as a linear combination of monomials $\gamma_1^{i_1}\ldots\gamma_k^{i_k}$ with $i_1+\cdots+i_k=s$. Choosing $s>k$, note that each such monomial is a multiple of $l(-1)^{n(s-k)}$. If $s>k+r/n$, it follows that $(\gamma_1+\cdots+\gamma_k)^s=0$; which completes the proof.

To conclude this section, the ring K_*F will be described in four interesting special cases.

Example 1.5 (Steinberg). If the field is finite, then $K_2F=0$. In fact K_1F is cyclic, say of order $q-1$; so §1.1 implies that K_2F is either trivial or of order $\leqq 2$, according as q is even or odd. But, if q is odd, then an easy counting argument shows that 1 is the sum of two quadratic non-residues in F; from which it follows that $K_2F=0$. This implies, of course, that $K_nF=0$ for $n>2$ also.

Example 1.6. Let R be the field of real numbers. Then every K_nR, $n\geqq 1$, splits as the direct sum of a cyclic group of order 2 generated by $l(-1)^n$, and a divisible group generated by all products $l(a_1)\dots l(a_n)$ with $a_1, \dots, a_n>0$. This is easily proved by induction on n, using the argument of §1.4 to show that $l(-1)^n$ is not divisible.

Example 1.7. Let F be a *local field* (i.e. complete under a discrete valuation with finite residue class field), and let m be the number of roots of unity in F. Calvin Moore [10] proves that K_2F is the direct sum of a cyclic group of order m and a divisible group.

We will show that K_nF is divisible for $n\geqq 3$. Consider the algebra K_*F/pK_*F over Z/pZ; where p is a fixed prime. If p does not divide m, then Moore's theorem clearly implies that $K_2F/pK_2F=0$. Suppose that p does divide m. We claim then that:

(1) the vector space K_1F/pK_1F has dimension $\geqq 2$ over Z/pZ;

(2) the vector space K_2F/pK_2F has dimension 1; and

(3) for each $\alpha\neq 0$ in K_1F/pK_1F there exists β in K_1F/pK_1F so that $\alpha\beta\neq 0$.

In fact (1) is clear; (2) follows from Moore's theorem; and (3) is an immediate consequence of the classical theorem which asserts that, for each $a\in F^\bullet$ which is not a p-th power, there exists b so that the p-th power norm residue symbol $(a, b)_F$ is non-trivial. (See for example [20, p. 260].) The correspondence

$$l(a)\,l(b)\mapsto (a, b)_F$$

clearly extends to a homomorphism from K_2F to the group of p-th roots of unity. So, taking $\alpha\equiv l(a)$, $\beta\equiv l(b)$, the conclusion (3) follows.

Proof that every generator $\alpha\beta\gamma$ of K_3F/pK_3F is zero. Given α, β, γ one can first choose $\beta'\neq 0$ so that $\alpha\beta'=0$ (using (1) and (2)), and then choose γ' so that $\beta'\gamma'=\beta\gamma$ (using (2) and (3)). The required equation

$$\alpha\beta\gamma=\alpha\beta'\gamma'=0$$

follows.

Thus $K_3F/pK_3F=0$ for every prime p; which proves that K_3F is divisible.

Example 1.8. Let F be a *global field* (that is a finite extension of the field Q of rational numbers, or of the field of rational functions in one indeterminate over a finite field). Let F_v range over all local or real completions of F. The complex completions (if any) can be ignored for our purposes. The inclusions $F \to F_v$ induce a homomorphism

$$K_2 F \to \oplus_v K_2 F_v/(\text{max. divis. subgr.}),$$

where each summand on the right is finite cyclic by 1.6 and 1.7. Bass and Tate [3] have shown that the kernel of this homomorphism is finitely generated, but the precise structure of the kernel is not known. Moore has shown that the cokernel is isomorphic to the group of roots of unity in F.

The structure of $K_n F$ is not known for $n \geqq 3$, but Tate has proved the following partial result: *The quotient $K_n F/2K_n F$ maps isomorphically to the direct sum, over all real completions F_v, of*

$$K_n F_v/2K_n F_v \cong Z/2Z.$$

Thus the dimension of $K_n F/2K_n F$ as a mod 2 vector space is equal to the number of real completions. Tate's proof of this result is presented in the Appendix.

It may be conjectured that the subgroup $2K_n F$ is actually zero for $n \geqq 3$, so that $K_n F$ itself is a vector space over $Z/2Z$. As an example, for the field Q of rational numbers the isomorphism

$$K_n Q \cong Z/2Z$$

for $n \geqq 3$ can be established by methods similar to those of §2.3.

§ 2. Discrete Valuations and the Computation of $K_* F(t)$

Suppose that a field F has a discrete valuation v with residue class field $\bar{F}$ $(=\bar{F}_v)$. The group of *units* (elements u with $\text{ord}_v u = 0$) will be denoted by U, and the natural homomorphism $U \to \bar{F}^\bullet$ by $u \mapsto \bar{u}$. An element π of $F^\bullet$ is *prime* if $\text{ord}_v \pi = 1$.

Lemma 2.1. *There exists one and only one homomorphism $\partial = \partial_v$ from $K_n F$ to $K_{n-1}\bar{F}$ which carries the product $l(\pi)\, l(u_2) \ldots l(u_n)$ to $l(\bar{u}_2) \ldots l(\bar{u}_n)$ for every prime element π and for all units $u_2, \ldots, u_n$. This homomorphism ∂ annihilates every product of the form $l(u_1) \ldots l(u_n)$.*

(For $n = 1$ the defining property is to be that $\partial l(\pi) = 1$.)

Remarks. Evidently ∂ is always surjective. For $n = 1$ the homomorphism ∂ can essentially be identified with the homomorphism

$$\text{ord}_v \colon F^\bullet \to Z;$$

and for $n=2$ it is closely related to the classical "tame symbol"

$$\pi^i u_1, \pi^j u_2 \mapsto (\overline{-1})^{ij} \bar{u}_2^i / \bar{u}_1^j$$

which is utilized for example in [3].

To begin the proof, note that any unit u_1 can be expressed as the quotient $\pi u_1/\pi$ of two prime elements. So the property

$$\partial(l(u_1)\dots l(u_n))=0$$

follows immediately from the defining equation.

Proof of Uniqueness. Choose a prime element π. Since F^* is generated by π and U, it follows that $K_n F$ is generated by products of the form $l(\pi)^r l(u_{r+1})\dots l(u_n)$. If $r=1$, then the image of any such product under ∂ has been specified; and if $r>1$ then using the identity $l(\pi)^r = l(\pi)\, l(-1)^{r-1}$ it is also specified. But if $r=0$, then any such product maps to zero. This proves that ∂ is unique, if it exists.

Proof of Existence[1]. It will be convenient to introduce an indeterminate symbol x which is to anticommute with all elements of $K_1 \bar{F}$. Given any n-tuple of elements

$$l(\pi^{i_1} u_1), \dots, l(\pi^{i_n} u_n) \in K_1 F,$$

construct a sequence of elements $\varphi_j \in K_j \bar{F}$ by the formula

$$(x\, i_1 + l(\bar{u}_1))\dots(x\, i_n + l(\bar{u}_n)) = x^n \varphi_0 + x^{n-1} \varphi_1 + \dots + \varphi_n.$$

Evidently each φ_j is n-linear as a function of $l(\pi^{i_1} u_1), \dots, l(\pi^{i_n} u_n)$. Now consider the linear combination

$$\varphi = l(\overline{-1})^{n-1} \varphi_0 + l(\overline{-1})^{n-2} \varphi_1 + \dots + \varphi_{n-1}.$$

Thus $\varphi \in K_{n-1} \bar{F}$, and evidently φ is also linear as a function of each $l(\pi^{i_j} u_j)$.

If two successive $\pi^{i_j} u_j$ add up to 1, we will prove that $\varphi=0$. This will show that the correspondence

$$l(\pi^{i_1} u_1)\dots l(\pi^{i_n} u_n) \mapsto \varphi$$

---

1 *Added in Proof.* A much better construction of the homomorphism ∂ has been suggested by Serre. Adjoin to the ring $K_* \bar{F}$ a new symbol ξ of degree 1 which is to anticommute with the elements of $K_1 \bar{F}$, and to satisfy the identity $\xi^2 = \xi\, l(\overline{-1})$, but is to satisfy no other relations. Thus the enlarged ring $(K_* \bar{F})[\xi]$ is free over $K_* \bar{F}$ with basis $\{1, \xi\}$. It is not difficult to show that the correspondence

$$l(\pi^i u) \mapsto i\,\xi + l(\bar{u})$$

extends uniquely to a ring homomorphism θ_π from $K_* F$ to this enlarged ring. Now, setting

$$\theta_\pi(\alpha) = \psi(\alpha) + \xi\, \partial(\alpha)$$

with $\psi(\alpha)$ and $\partial(\alpha)$ in $K_* \bar{F}$, we obtain the required homomorphism ∂.

is well defined and extends to a homomorphism

$$K_n F \to K_{n-1} \bar{F}.$$

Since it is clear that $l(\pi u)\, l(u_2) \ldots l(u_n)$ maps to $l(\bar{u}_2) \ldots l(\bar{u}_n)$, this will complete the proof.

To avoid complicated notation, we will carry out details only for the case

$$\pi^{i_1} u_1 + \pi^{i_2} u_2 = 1.$$

There are four possibilities to consider.

If $i_1 > 0$, then it follows easily that

$$i_2 = 0, \quad \bar{u}_2 = 1.$$

Hence the factor $x\, i_2 + l(\bar{u}_2)$ is zero and it certainly follows that $\varphi = 0$.

The case $i_1 = 0$, $i_2 > 0$ is disposed of similarly.

If $i_1 = i_2 = 0$, then $\bar{u}_1 + \bar{u}_2 = \bar{1}$, hence

$$\big(x\, i_1 + l(\bar{u}_1)\big)\big(x\, i_2 + l(\bar{u}_2)\big) = 0,$$

so again $\varphi = 0$.

Finally suppose that $i_1 < 0$. Then clearly $i_1 = i_2$ and $\bar{u}_2 = -\bar{u}_1$. In this case the product $\big(x\, i_1 + l(\bar{u}_1)\big)\big(x\, i_2 + l(\bar{u}_2)\big)$ evidently simplifies to

$$x^2\, i_1^2 + x\, i_1\, l(\overline{-1}) + 0.$$

Hence the expression $\sum x^{n-j} \varphi_j$ can be written as

$$x\big(x\, i_1^2 + i_1\, l(\overline{-1})\big)\big(x\, i_3 + l(\bar{u}_3)\big) \ldots \big(x\, i_n + l(\bar{u}_n)\big).$$

Cancelling the initial x, and then substituting $l(\overline{-1})$ for the remaining x's, we evidently obtain an expression for φ. But this substitution carries $x\, i_1^2 + i_1\, l(\overline{-1})$ to $l(\overline{-1})\, i_1^2 + i_1\, l(\overline{-1}) = 0$. So $\varphi = 0$ in this case also; which completes the proof of 2.1.

A similar argument proves the following.

Lemma 2.2. *Choosing some fixed prime element π, there is one and only one ring homomorphism*

$$\psi\colon\ K_* F \to K_* \bar{F}$$

which carries $l(\pi^i u)$ to $l(\bar{u})$ for every unit u.

In fact ψ is defined by the rule

$$l(\pi^{i_1} u_1) \ldots l(\pi^{i_n} u_n) \mapsto l(\bar{u}_1) \ldots l(\bar{u}_n).$$

Details will be left to the reader. Evidently this homomorphism ψ is less natural than ∂, since it depends on a particular choice of π.

Now let F be an arbitrary field. We will use 2.1 and 2.2 to study the field $F(t)$ of rational functions in one indeterminate over F.

Each monic irreducible polynomial $\pi \in F[t]$ gives rise to a (π)-adic valuation on $F(t)$ with residue class field $F[t]/(\pi)$. Here (π) denotes the prime ideal spanned by π. Hence there is an associated surjection

$$\partial_\pi \colon K_n F(t) \to K_{n-1} F[t]/(\pi).$$

Theorem 2.3. *These homomorphisms ∂_π give rise to a split exact sequence*

$$0 \to K_n F \to K_n F(t) \to \oplus K_{n-1} F[t]/(\pi) \to 0,$$

where the direct sum extends over all non-zero prime ideals (π).

This theorem is essentially due to Tate. In fact the proof below is an immediate generalization of Tate's proof for the special case $n=2$.

Proof. Keeping n fixed, let $L_d \subset K_n F(t)$ be the subgroup generated by those products $l(f_1) \dots l(f_n)$ such that $f_1, \dots, f_n \in F[t]$ are polynomials of degree $\leqq d$. Thus

$$L_0 \subset L_1 \subset L_2 \subset \cdots$$

with union $K_n F(t)$. Using the homomorphism

$$\psi_\pi \colon K_n F(t) \to K_n F$$

of 2.2, where π is any monic (irreducible) polynomial of degree 1, we see easily that L_0 is a direct summand of $K_n F(t)$, naturally isomorphic to $K_n F$.

Let π be a monic irreducible polynomial of degree d. Then each element $\bar{g}$ of the quotient $F[t]/(\pi)$ is represented by a unique polynomial $g \in F[t]$ of degree $< d$.

Lemma 2.4. *There exists one and only one homomorphism*

$$h_\pi \colon K_{n-1} F[t]/(\pi) \to L_d/L_{d-1}$$

which carries each product $l(\bar{g}_2) \dots l(\bar{g}_n)$ to the residue class of $l(\pi)\, l(g_2) \dots l(g_n)$ modulo L_{d-1}.

Proof. First consider the correspondence

$$l(\bar{g}_2) \times \cdots \times l(\bar{g}_n) \mapsto l(\pi)\, l(g_2) \dots l(g_n) \bmod L_{d-1}$$

from $K_1 F[t]/(\pi) \times \cdots \times K_1 F[t]/(\pi)$ to L_d/L_{d-1}. We will show that this correspondence is linear, for example as a function of $\bar{g}_2$. Suppose that

$$g_2 \equiv g_2' g_2'' \bmod (\pi),$$

where g_2, g_2', g_2'' are polynomials of degree $< d$. Then

$$g_2 = \pi f + g_2' g_2''$$

where f is also a polynomial of degree $<d$. Hence, if $f \neq 0$,

$$1 = \pi f/g_2 + g_2' g_2''/g_2$$

and therefore

$$\big(l(\pi)+l(f)-l(g_2)\big)\big(l(g_2')+l(g_2'')-l(g_2)\big)=0.$$

Multiplying on the right by $l(g_3)\dots l(g_n)$, and then reducing modulo L_{d-1}, we obtain

$$l(\pi)\big(l(g_2')+l(g_2'')-l(g_2)\big)\, l(g_3)\dots l(g_n)\equiv 0.$$

Since the case $f=0$ is straight forward, this proves that our correspondence is $(n-1)$-linear.

To prove that this correspondence gives rise to a homomorphism

$$l(\bar{g}_2)\dots l(\bar{g}_n)\mapsto l(\pi)\, l(g_2)\dots l(g_n)$$

from $K_{n-1}\bar{F}$ to L_d/L_{d-1}, it is now only necessary to note that the image is zero whenever $\bar{g}_j+\bar{g}_{j+1}=\bar{1}$ and hence $g_j+g_{j+1}=1$. This proves 2.4.

Lemma 2.5. *The homomorphisms ∂_π give rise to an isomorphism between L_d/L_{d-1} and the direct sum of $K_{n-1}F[t]/(\pi)$ as π ranges over monic irreducible polynomials of degree d.*

Proof. Inspection shows that each ∂_π induces a homomorphism

$$L_d/L_{d-1}\to K_{n-1}F[t]/(\pi).$$

Furthermore it is clear that the composition

$$K_{n-1}F[t]/(\pi)\xrightarrow{h_\pi} L_d/L_{d-1}\xrightarrow{\partial_{\pi'}} K_{n-1}F[t]/(\pi')$$

is either the identity or zero, according as $\pi=\pi'$ or $\pi\neq\pi'$. So to complete the argument we need only to show that L_d/L_{d-1} is generated by the images of the h_π.

Consider any generator of L_d, expressed as a product $l(f_1)\dots l(f_s)\, l(g_{s+1})\dots l(g_n)$ where $f_1,\dots,f_s$ have degree d and $g_{s+1},\dots,g_n$ have degree $<d$. If $s\geqq 2$ then we can set

$$f_2=-af_1+g$$

with $a\in F^\bullet$ and degree $g<d$. If $g\neq 0$ it follows that

$$af_1/g+f_2/g=1$$

hence

$$\big(l(a)+l(f_1)-l(g)\big)\big(l(f_2)-l(g)\big)=0.$$

Thus the product $l(f_1)\, l(f_2)$ can be expressed as a sum of terms

$$l(f_1)\, l(g)+l(g)\, l(f_2)-l(a)\, l(f_2)+l(a)\, l(g)-l(g)^2,$$

each of which involves at most one polynomial of degree d. A similar situation obtains when $g=0$. It follows, by induction on s, that every element of L_d can be expressed, modulo L_{d-1}, in terms of products $l(f_1)\,l(g_2)\ldots l(g_n)$ where only f_1 has degree d. If f_1 is irreducible, then setting $f=a\,\pi$ this product evidently belongs to the image of h_π. But if f_1 is reducible then the product is congruent to zero modulo L_{d-1}. Thus L_d/L_{d-1} is generated by the images of the homomorphisms h_π, which completes the proof of 2.5.

An easy induction on d now shows that the homomorphisms ∂_π induce an isomorphism from L_d/L_0 to the direct sum of $K_{n-1}F[t]/(\pi)$, taken over all monic irreducible π of degree $\leqq d$. Passing to the direct limit as $d\to\infty$, this completes the proof of Theorem 2.3.

To conclude this section, let us record a similar, but easier statement.

Lemma 2.6. *Suppose that a field E is complete under a discrete valuation with residue class field $\bar{E}=F$. Then for any prime p distinct from the characteristic of $\bar{E}$ there is a natural split exact sequence*

$$0\to K_nF/pK_nF\to K_nE/pK_nE\xrightarrow{\partial}K_{n-1}F/pK_{n-1}F\to 0.$$

Proof. If a unit of E maps to 1 in F, then it has a p-th root. Hence the correspondence $l(\bar{u})\mapsto l(u) \bmod pK_1E$ is well defined. This correspondence extends to a ring homomorphism

$$K_*F\to K_*E/pK_*E.$$

Further details will be left to the reader.

§ 3. The Stiefel-Whitney Invariants of a Quadratic Module

For the rest of this paper we will only be interested in the quotient of the ring K_*F by the ideal $2K_*F$. To simplify the notation, let us set

$$k_nF=K_nF/2K_nF.$$

Thus k_*F is a graded algebra over $Z/2Z$, with $k_1F\cong F^\bullet/F^{\bullet 2}$. *We will always assume that F has characteristic $\neq 2$.*

The symbol $k_\Pi F$ will stand for the algebra consisting of all formal series $\xi_0+\xi_1+\xi_2+\cdots$ with $\xi_i\in k_iF$. Thus $k_\Pi F$ is additively isomorphic to the cartesian product $k_0F\times k_1F\times k_2F\times\cdots$.

Let M be a *quadratic module* over F. That is M is a finite dimensional vector space with a non-degenerate symmetric bilinear inner product. Then M is isomorphic to an orthogonal direct sum $\langle a_1\rangle\oplus\cdots\oplus\langle a_r\rangle$ of one dimensional modules. Here $\langle a\rangle$ denotes the one dimensional quadratic module such that the inner product of a suitable basis vector with itself is a.

Define the *Stiefel-Whitney invariant*

$$w(M) \in k_{II} F$$

of a quadratic module $M \cong \langle a_1 \rangle \oplus \cdots \oplus \langle a_r \rangle$ by the formula

$$w(M) = (1 + l(a_1))(1 + l(a_2)) \ldots (1 + l(a_r)).$$

Thus $w(M)$ can be written as

$$1 + w_1(M) + \cdots + w_r(M)$$

where $w_i(M)$, the i-th *Stiefel-Whitney invariant*, is equal to the i-th elementary symmetric function of $l(a_1), \ldots, l(a_r)$ considered as an element of $k_i F$.

Evidently w_1 is just the classical "discriminant" of M, and w_2 is closely related to the classical Hasse-Witt invariant.

Remark. This definition is very similar to the definition proposed by Delzant [5]. However Delzant's Stiefel-Whitney classes belong to the cohomology $H^*(G_F; Z/2Z)$ of the maximal Galois extension of F. They are precisely the images of our w_i under a canonical homomorphism

$$k_* F \to H^*(G_F; Z/2Z)$$

which is described in § 6.

Lemma 3.1. *The invariant $w(M)$ is a well defined unit in the ring $k_{II} F$ and satisfies the Whitney sum formula*

$$w(M \oplus N) = w(M)\, w(N).$$

Proof. Just as in the classical proof that the Hasse-Witt invariant is well defined, it suffices to consider the rank 2 case. (Compare O'Meara [12, p. 150].) Suppose then that

$$\langle a \rangle \oplus \langle b \rangle \cong \langle \alpha \rangle \oplus \langle \beta \rangle.$$

Then the discriminant ab must be equal to $\alpha\beta$ multiplied by a square; or in other words

$$l(a) + l(b) \equiv l(\alpha) + l(\beta) \mod 2K_1 F. \tag{4}$$

Furthermore, the equation $\alpha = a x^2 + b y^2$ must have a solution $x, y \in F$. Since the case $x = 0$ or $y = 0$ is easily disposed of, we may assume that $x \neq 0$, $y \neq 0$. Then the equation

$$1 = a x^2/\alpha + b y^2/\alpha$$

implies that

$$\begin{aligned} 0 &= (l(a) + 2l(x) - l(\alpha))(l(b) + 2l(y) - l(\alpha)) \\ &\equiv (l(a) - l(\alpha))(l(b) - l(\alpha)) \mod 2K_2 F. \end{aligned}$$

Rearranging terms, and then substituting (4) this implies that

$$\begin{aligned} l(a)\,l(b) &\equiv l(\alpha)\,(l(a)+l(b)-l(\alpha)) \\ &\equiv l(\alpha)\,l(\beta) \quad \mod 2K_2F; \end{aligned}$$

which completes the proof.

Remark. Delzant shows that a quadratic module over a number field is determined up to isomorphism by its rank and Stiefel-Whitney cohomology classes. But Scharlau points out that the corresponding statement for an arbitrary field is false. The same statements, proofs, and examples apply to our Stiefel-Whitney invariants.

Now let us introduce the *Witt-Grothendieck ring* $\hat{W}F$, consisting of all formal differences $M-N$ of quadratic modules over F; where $M-N$ equals $M'-N'$ if and only if the orthogonal direct sum $M\oplus N'$ is isomorphic to $M'\oplus N$. (Compare [5, 14].) The product operation in $\hat{W}F$ is characterized by the identity

$$\langle a\rangle\langle b\rangle=\langle ab\rangle.$$

The *augmentation ideal*, consisting of all $M-N$ in $\hat{W}F$ with $\operatorname{rank}M=\operatorname{rank}N$, will be denoted by $\hat{I}F$, and its n-th power by $\hat{I}^nF$.

Evidently the function w extends uniquely to a homomorphism from the additive group of $\hat{W}F$ to the multiplicative group of units in $k_\Pi F$; where

$$w(M-N)=w(M)/w(N)$$

by definition.

Next consider a generator

$$\xi=(\langle a_1\rangle-\langle 1\rangle)(\langle a_2\rangle-\langle 1\rangle)\dots(\langle a_n\rangle-\langle 1\rangle) \tag{5}$$

of the ideal $\hat{I}^nF$. Let $t=2^{n-1}$.

Lemma 3.2. *The Stiefel-Whitney invariant w of such a product ξ is equal to either*

$$1+l(a_1)\dots l(a_n)\,l(-1)^{t-n}$$

or

$$(1+l(a_1)\dots l(a_n)\,l(-1)^{t-n})^{-1}$$

according as n is odd or even.

Proof. Multiplying out the formula (5), we obtain

$$\xi=\sum\pm\langle a_1^{\varepsilon_1}\dots a_n^{\varepsilon_n}\rangle,$$

to be summed as $\varepsilon_1,\dots,\varepsilon_n$ range over 0 and 1. Here and subsequently, $\pm$ stands for the sign $(-1)^{\varepsilon_1+\cdots+\varepsilon_n+n}$. Therefore

$$w(\xi)=\prod(1+\varepsilon_1\,l(a_1)+\cdots+\varepsilon_n\,l(a_n))^{\pm 1}.$$

Consider the corresponding product

$$\prod (1+\varepsilon_1 x_1+\cdots+\varepsilon_n x_n)^{\pm 1} \tag{6}$$

in the ring of formal power series with mod 2 coefficients in n indeterminates. If we substitute 0 for some x_i, then evidently this product becomes 1. Hence the product (6) must be equal to

$$1+x_1 \ldots x_n f(x_1, \ldots, x_n)$$

for some formal power series f. Therefore

$$\begin{aligned} w(\xi) &= 1+l(a_1)\ldots l(a_n) f\big(l(a_1), \ldots, l(a_n)\big) \\ &= 1+l(a_1)\ldots l(a_n) f\big(l(-1), \ldots, l(-1)\big); \end{aligned}$$

using § 1.2.

To compute the power series $f\big(l(-1), \ldots, l(-1)\big)$ it suffices to substitute $x_1=\cdots=x_n=x$ in (6), so as to compute $f(x, \ldots, x)$. Evidently the product reduces to either $(1+x)^t$ or $(1+x)^{-t}$ according as n is odd or even; where $t=2^{n-1}$. For n odd it follows that

$$1+x^n f(x, \ldots, x)=(1+x)^t=1+x^t,$$

so that

$$f(x, \ldots, x)=x^{t-n};$$

and a similar computation can be carried out for n even. This completes the proof.

Corollary 3.3 *If $t=2^{n-1}$, then the invariants $w_1, \ldots w_{t-1}$ annihilate the ideal $\hat{I}^n F$, while w_t induces a homomorphism*

$$w_t\colon \hat{I}^n F/\hat{I}^{n+1} F \to k_t F$$

which carries the product

$$(\langle a_1\rangle-\langle 1\rangle)\ldots(\langle a_n\rangle-\langle 1\rangle)$$

to $l(a_1)\ldots l(a_n)\, l(-1)^{t-n}$.

Proof. Since the elements $\langle a\rangle-\langle 1\rangle$ form an additive set of generators for $\hat{I}F$, it is clear that the n-fold products of such elements generate $\hat{I}^n F$. The conclusion now follows immediately.

Remark 3.4. These formulas suggest that the Stiefel-Whitney invariants are not independent of each other. In fact the following is true: *If n is not a power of 2, then $w_n(M)$ can be expressed as a product $w_r(M)\, w_{n-r}(M)$ where r is the highest power of 2 dividing n.*

(Compare also [14, § 2.2.2].) The proof can be outlined as follows. Interpreting w_s as an elementary symmetric function, and using § 1.2,

it is not difficult to show that

$$w_r w_s = \sum (i, r-i, s-i)\, w_{r+s-i}\, l(-1)^i,$$

to be summed over $0 \leqq i \leqq \mathrm{Min}\{r, s\}$. Here (i, j, k) stands for the trinomial coefficient $(i+j+k)!/i!\,j!\,k!$. But if r is a power of 2, and if

$$s \equiv 0 \bmod 2r,$$

then this identity takes the simple form

$$w_r w_s = w_{r+s}$$

which completes the outlined proof.

§ 4. The Surjection $K_n/2K_n \to I^n/I^{n+1}$

Let F be a field of characteristic $\neq 2$. The Witt ring $W = WF$ can be defined as the quotient $\hat{W}/H$, where $\hat{W}$ is the Witt-Grothendieck ring of § 3, and H is the free cyclic additive group spanned by $\langle 1\rangle \oplus \langle -1\rangle$. Clearly H is an ideal, so that W is a ring. Note that the augmentation ideal $\hat{I}$ in $\hat{W}$ maps bijectively to a maximal ideal in W. This image ideal will be denoted by $I = IF$.

(Remark. The utility of working with W, rather than $\hat{W}$, will become apparent only in § 5.)

As in § 3, we set $k_n F = K_n F/2K_n F$. This will sometimes be abbreviated as $k_n = K_n/2K_n$.

Theorem 4.1. *There is one and only one homomorphism*

$$s_n\colon\ k_n F \to I^n F/I^{n+1} F$$

which carries each product $l(a_1)\ldots l(a_n)$ in $k_n F$ to the product

$$(\langle a_1\rangle - \langle 1\rangle)\ldots(\langle a_n\rangle - \langle 1\rangle)$$

modulo $I^{n+1}F$. The homomorphisms s_1 and s_2 are bijective (compare [13]*); and every s_n is surjective.*

Proof. The correspondence

$$l(a_1) \times \cdots \times l(a_n) \mapsto \prod (\langle a_i\rangle - \langle 1\rangle) \mod I^{n+1}$$

from $K_1 \times \cdots \times K_1$ to I^n/I^{n+1} is n-linear since

$$\langle a\rangle - \langle 1\rangle + \langle b\rangle - \langle 1\rangle \equiv \langle a\,b\rangle - \langle 1\rangle \mod I^2.$$

Furthermore, if $a_i + a_{i+1} = 1$ then an easy computation shows that

$$(\langle a_i\rangle - \langle 1\rangle)(\langle a_{i+1}\rangle - \langle 1\rangle) = 0,$$

so the image is zero. Thus this correspondence gives rise to a homomorphism $K_n \to I^n/I^{n+1}$. This homomorphism annihilates $2K_n$ since

$$2l(a_1)\dots l(a_n) = l(a_1^2)\,l(a_2)\dots l(a_n)$$

with

$$\langle a_1^2\rangle - \langle 1\rangle = 0.$$

Thus we have shown that the homomorphism

$$s_n\colon\ K_n/2K_n \to I^n/I^{n+1}$$

exists and is well defined. This homomorphism is clearly surjective, since the elements $\langle a\rangle - \langle 1\rangle$ form an additive set of generators for the ideal I.

Now let $t = 2^{n-1}$, and consider the homomorphism

$$w_t\colon\ I^n/I^{n+1} \cong \hat{I}^n/\hat{I}^{n+1} \to k_t$$

of § 3.3. Evidently the composition $w_t \circ s_n$ is just multiplication by $l(-1)^{t-n}$.

But if n equal 1 or 2, then $t = n$, and the appropriate statement is that $w_n \circ s_n$ is the identity. This shows that s_1 and s_2 are bijective; which completes the proof of 4.1.

Remark 4.2. For $n > 2$, this argument proves the following: *If multiplication by* $l(-1)^{t-n}$ *carries* k_nF *injectively into* k_tF, *then the homomorphism*

$$s_n\colon\ k_nF \to I^n/I^{n+1}$$

is necessarily bijective.

Evidently there are two key questions in relating k_* to the Witt ring W. Let F be any field of characteristic $\neq 2$.

Question 4.3. *Is the homomorphism* $s_n\colon\ k_nF \to I^n/I^{n+1}$ *bijective for all values of* n?

Question 4.4. *Is the intersection of the ideals* I^n *equal to zero?* (Compare [13, 14].)

This section will conclude by proving two preliminary results. (See also §§ 5.2 and 5.8.)

Lemma 4.5. *If* F *is a global field, or a direct limit of global fields, then both questions have affirmative answers.*

Proof. Using Tate's explicit computation of k_*F for a global field (§ 1.8 or the Appendix), we see that multiplication by $l(-1)$ induces isomorphisms

$$k_3F \to k_4F \to k_5F \to \cdots.$$

Together with § 4.2, this proves that s_n is bijective in the case of a global field. The corresponding statement for a direct limit follows immediately.

As to the intersection of the ideals I^n, first note that each embedding of F in the real field gives rise to a ring homomorphism

$$WF \to WR \cong Z$$

called the *signature*. Note that an element of $I^3 F$ is zero if and only if its signature at every embedding $F \to R$ is zero. In the case of a global field, this statement follows immediately from the Hasse-Minkowski theorem; and for the direct limit of a sequence

$$F_1 \subset F_2 \subset F_3 \subset \cdots$$

of global fields it follows easily using the isomorphisms

$$W \varinjlim F_\alpha = \varinjlim WF_\alpha$$

and

$$\mathrm{Emb}(\varinjlim F_\alpha, R) = \varprojlim \mathrm{Emb}(F_\alpha, R).$$

But each such signature carries the ideal IF to $2Z$, and hence carries the intersection of the ideals $I^n F$ to $\bigcap 2^n Z = 0$. This completes the proof.

Lemma 4.6. *Now suppose that F is a field such that $k_2 F$ has at most two distinct elements. Then again the s_n are bijective and $\bigcap I^n = 0$.*

Notice that this includes the case of a finite, or local, or real closed, or quadratically closed field; as well as any direct limit of such fields.

Proof. If k_1, modulo the null-space of the pairing $k_1 \otimes k_1 \to k_2$, has dimension $\neq 1$, then Kaplansky and Shaker [6] show that a quadratic module is completely determined by its rank, discriminant, and Hasse-Witt invariant. It follows that $I^3 = 0$. But just as in §1.7 one sees that $k_3 = 0$. Since s_1 and s_2 are already known to be bijective, it certainly follows that every s_n is bijective.

On the other hand if k_1 modulo this null-space has dimension 1, then it is easy to define the "signature" of a quadratic module, and to show that the rank, discriminant, and signature form a complete invariant. (Compare [6, Lemma 1].) Since the signature of an element in I^n is divisible by 2^n, it follows that $\bigcap I^n = 0$. Futhermore, techniques similar to those of §1.4 show that k_n is cyclic of order 2, generated by $l(-1)^n$, for every $n \geqq 2$; hence §4.2 implies that every s_n is bijective. This completes the proof.

§5. The Witt Ring of a Rational Function Field

This section will study the Witt ring, using constructions very similar to those of §2.

First consider a field E which is complete under a discrete valuation v, with residue class field $\bar{E}$ of characteristic $\neq 2$. Let π be a prime element.

Theorem of Springer. *The Witt ring WE contains a subring W_0 canonically isomorphic to $W\bar{E}$. Furthermore WE, splits additively as the direct sum of W_0 and $\langle\pi\rangle W_0$.*

In fact W_0 can be defined as the subring generated by $\langle u\rangle$ as u ranges over units of E, and the isomorphism $W_0 \to W\bar{E}$ is defined by the correspondence $\langle u\rangle \mapsto \langle\bar{u}\rangle$.

For the proof, see T.A. Springer [16]. Since $\langle\pi\rangle^2 = \langle 1\rangle$, it follows that the ring WE is completely determined by $W\bar{E}$.

Corollary 5.1. *There is a split exact sequence*

$$0 \to W\bar{E} \to WE \xrightarrow{\partial} W\bar{E} \to 0,$$

where the first homomorphism carries $\langle\bar{u}\rangle$ to $\langle u\rangle$, and where ∂ is defined by the conditions

$$\partial\langle u\rangle = 0, \quad \partial\langle\pi u\rangle = \langle\bar{u}\rangle.$$

Note however that ∂ depends on the particular choice of the prime element π.

The proof is straightforward.

Corollary 5.2. *If the questions* 4.3 *and* 4.4 *have affirmative answers for the residue class field $\bar{E}$, then they also have affirmative answers for E.*

Proof. It will be convenient to identify $W\bar{E}$ with the sub-ring $W_0 \subset WE$. Note that the ideal IE then splits as a direct sum

$$IE = I\bar{E} \oplus (\langle\pi\rangle - \langle 1\rangle)\, W\bar{E}.$$

It follows inductively that

$$I^n E = I^n \bar{E} \oplus (\langle\pi\rangle - \langle 1\rangle)\, I^{n-1}\bar{E}.$$

Hence the sequence 5.1 gives rise to a split exact sequence

$$(7_n) \qquad 0 \to I^n\bar{E} \to I^n E \to I^{n-1}\bar{E} \to 0.$$

Consider the diagram

$$\begin{array}{ccccc} k_n\bar{E} & \longrightarrow & k_n E & \longrightarrow & k_{n-1}\bar{E} \\ \downarrow & & \downarrow & & \downarrow \\ I^n\bar{E}/I^{n+1}\bar{E} & \to & I^n E/I^{n+1}E & \to & I^{n-1}\bar{E}/I^n\bar{E}, \end{array}$$

where the top sequence comes from §2.6, the vertical arrows from §4.1, and the bottom sequence is the quotient of (7_n) by (7_{n+1}). Checking that this diagram is commutative, and then applying the Five Lemma, the conclusion follows.

Now consider a field $E=F(t)$ of rational functions. For each monic irreducible $\pi\in F[t]$ we can form the π-adic completion E_π, with residue class field

$$\bar{E}_\pi \cong F[t]/(\pi).$$

Let

$$\partial_\pi\colon\ WE \to W\bar{E}_\pi$$

denote the composition of the natural map $WE \to WE_\pi$ with the homomorphism ∂ of 5.1. Evidently $\partial_\pi\langle u\rangle = 0$ and $\partial_\pi\langle \pi u\rangle = \langle \bar{u}\rangle$.

Theorem 5.3. *These homomorphisms ∂_π give rise to a split exact sequence*

$$0 \to WF \to WE \to \oplus W\bar{E}_\pi \to 0,$$

where $E=F(t)$, and where the summation extends over all monic irreducible polynomials π in $F[t]$.

The proof will be based on the Tate technique already utilized in §2.3. Let $L_d \subset WE$ denote the subring generated by all $\langle f\rangle$ such that $f\in F[t]$ is a polynomial of degree $\leqq d$. Thus

$$L_0 \subset L_1 \subset L_2 \subset \cdots$$

with union WE. Additively, L_d is generated by all products $\langle f_1 \ldots f_s\rangle$ where the f_i are polynomials of degree $\leqq d$.

Note that L_0 is just the image of the natural homomorphism $WF \to WE$.

Lemma 5.4. *In fact WF maps bijectively to L_0. Furthermore L_0 is a retract of WE under a ring homomorphism*

$$\rho\colon\ WE \to WF \cong L_0.$$

Proof. Choose some monic polynomial π of degree 1, and define ρ by the conditions

$$\rho\langle u\rangle = \langle \bar{u}\rangle, \qquad \rho\langle \pi u\rangle = \langle \bar{u}\rangle.$$

Here u denotes any unit with respect to the (π)-adic valuation. It follows from Springer's theorem, applied to the (π)-adic completion, that ρ is a well defined ring homomorphism. Since the composition

$$WF \to WE \xrightarrow{\rho} WF$$

is the identity, this proves 5.4.

Now suppose that $d\geqq 1$.

Lemma 5.5. *The additive group L_d is generated, modulo L_{d-1}, by expressions $\langle \pi g_1 \ldots g_s\rangle$ where π is an irreducible polynomial of degree d, and $g_1, \ldots, g_s$ are polynomials of degree $<d$. Furthermore if f is the poly-*

nomial of degree $<d$ defined by

$$f \equiv g_1 \dots g_s \mod (\pi),$$

then

$$\langle \pi f \rangle \equiv \langle \pi g_1 \dots g_s \rangle \mod L_{d-1}.$$

Proof. First note that the identity

$$\langle a+b \rangle = \langle a \rangle + \langle b \rangle - \langle a\, b(a+b) \rangle \tag{8}$$

holds in the Witt ring of any field.

Consider a generator $\langle f_1 \dots f_r g_1 \dots g_s \rangle$ of L_d, where the polynomials $f_1, \dots, f_r$ are distinct, monic of degree d, and where $g_1, \dots, g_s$ have degree $<d$. If $r \geqq 2$, then defining a polynomial h of degree $<d$ by

$$f_1 = f_2 + h,$$

the identity (8) becomes

$$\langle f_1 \rangle = \langle f_2 \rangle + \langle h \rangle - \langle f_1 f_2 h \rangle.$$

Multiplying by $\langle f_2 \dots f_r g_1 \dots g_s \rangle$ and cancelling all squared factors, it follows that $\langle f_1 \dots f_r g_1 \dots g_s \rangle$ is equal to

$$\langle f_3 \dots g_s \rangle + \langle h f_2 \dots g_s \rangle - \langle f_1 h f_3 \dots g_s \rangle.$$

Since each of these terms has at most $r-1$ factors of degree d, it follows by induction on r that L_d is generated, modulo L_{d-1}, by expressions $\langle f g_1 \dots g_s \rangle$ where f is monic of degree d and the g_i have degree $<d$. We may clearly assume that f is irreducible.

Consider then such a generator $\langle \pi g_1 \dots g_s \rangle$ with π monic and irreducible. Setting

$$g_1 g_2 \equiv h \mod (\pi)$$

with degree $h<d$, we have

$$g_1 g_2 = h + \pi k$$

for some k of degree $<d$, hence

$$\langle g_1 g_2 \rangle = \langle h \rangle + \langle \pi k \rangle - \langle \pi k h g_1 g_2 \rangle.$$

Multiplying by $\langle \pi g_3 \dots g_s \rangle$, this shows that $\langle \pi g_1 \dots g_s \rangle$ is equal to

$$\langle \pi h g_3 \dots g_s \rangle + \langle k g_3 \dots g_s \rangle - \langle k h g_1 \dots g_s \rangle \equiv \langle \pi h g_3 \dots g_s \rangle \mod L_{d-1}.$$

An easy induction now completes the proof of 5.5.

Now consider the field $\bar{E}_\pi = F[t]/(\pi)$, where π is monic irreducible of degree d. For each residue class $\bar{f}$ modulo (π), let f denote the unique polynomial of degree $<d$ representing $\bar{f}$.

Lemma 5.6. *The correspondence*

$$\langle \bar{f} \rangle \mapsto \langle \pi f \rangle \mod L_{d-1}$$

gives rise to a homomorphism from $W\bar{E}_\pi$ *to* L_d/L_{d-1}.

Proof. For any field F of characteristic $\neq 2$ it is not difficult to show that the additive group of WF has a presentation in terms of generators $\langle a \rangle$, where a ranges over $F^\bullet$, subject only to the relations

$$\langle a b^2 \rangle = \langle a \rangle,$$
$$\langle a+b \rangle = \langle a \rangle + \langle b \rangle - \langle a\, b(a+b) \rangle,$$
$$\langle 1 \rangle + \langle -1 \rangle = 0,$$

and their consequences. But, substituting $\bar{E}_\pi$ for F, each such relation in $W\bar{E}_\pi$ maps to a valid relation in L_d/L_{d-1}. Thus if

$$f g(f+g) \equiv h \mod (\pi),$$

where f, g, h are non-zero polynomials of degree $< d$, then the relation

$$\langle \bar{f} + \bar{g} \rangle = \langle \bar{f} \rangle + \langle \bar{g} \rangle - \langle \bar{h} \rangle$$

in $W\bar{E}_\pi$ corresponds to the relation

$$\begin{aligned} \langle \pi(f+g) \rangle &= \langle \pi f \rangle + \langle \pi g \rangle - \langle \pi f g(f+g) \rangle \\ &\equiv \langle \pi f \rangle + \langle \pi g \rangle - \langle \pi h \rangle \mod L_{d-1}; \end{aligned}$$

making use of Lemma 5.5. Similarly, if $f g^2 \equiv k \bmod (\pi)$, then the relation $\langle \bar{f} \rangle = \langle \bar{k} \rangle$ corresponds to $\langle \pi f \rangle = \langle \pi f g^2 \rangle \equiv \langle \pi k \rangle$. Finally, the relation $\langle 1 \rangle + \langle -1 \rangle = 0$ corresponds to $\langle \pi \rangle + \langle -\pi \rangle = 0$. So it follows that the correspondence $\langle \bar{f} \rangle \mapsto \langle \pi f \rangle \bmod L_{d-1}$ does indeed define a homomorphism from $W\bar{E}_\pi$ to L_d/L_{d-1}. This proves 5.6.

Proof of Theorem 5.3. The argument is very similar to that in §2.5. First one checks that the composition

$$W\bar{E}_\pi \to L_d/L_{d-1} \xrightarrow{\partial_{\pi'}} W\bar{E}_{\pi'}$$

is either the identity or zero according as $\pi = \pi'$ or $\pi \neq \pi'$. Using 5.5, it follows that L_d/L_{d-1} splits canonically as the direct sum of those $W\bar{E}_\pi$ for which degree $\pi = d$.

Now induction on d shows that the homomorphisms ∂_π give rise to an isomorphism

$$L_d/L_0 \to \oplus_{\text{degree } \pi \leqq d} W\bar{E}_\pi.$$

Passing to the direct limit as $d \to \infty$, this completes the proof of 5.3.

Remark. More generally, suppose that E is a finite extension field of $F(t)$. Every valuation v of E which is trivial on F gives rise to a homomorphism

$$\partial_v\colon\ WE \to W\bar{E}_v,$$

well defined up to multiplication by a unit of the form $\langle \bar{e} \rangle$. It would be very interesting to know something about the kernel and cokernel of the associated homomorphism

$$WE \to \oplus\, W\bar{E}_v.$$

For the special case $E = F(t)$, both kernel and cokernel turn out to be isomorphic to WF.

Perhaps one may find some clue by applying the analogous construction to a global field. As an example, for the field Q of rationals, there is an additive isomorphism

$$WQ \to Z \oplus (Z/2Z) \oplus \oplus_{p\,\mathrm{odd}} W(Z/pZ),$$

using the signature and the correspondence

$$\langle q \rangle \mapsto \mathrm{ord}_2\, q \mod 2$$

to map to the first two summands, and using the homomorphisms ∂_p for the third.

Now let us bring the multiplicative structure of W into Theorem 5.3. Again let $E = F(t)$.

Lemma 5.7. *The sequence* 5.3 *gives rise to an exact sequence*

$$0 \to I^n F \to I^n E \to \oplus\, I^{n-1} \bar{E}_\pi \to 0$$

for any $n \geqq 1$.

Proof. The proof of 5.2 shows that each ∂_π maps $I^n E$ to $I^{n-1}\bar{E}_\pi$. Consider any generator

$$\eta = (\langle \bar{f}_2 \rangle - \langle \bar{1} \rangle) \ldots (\langle \bar{f}_n \rangle - \langle \bar{1} \rangle)$$

of $I^{n-1}\bar{E}_\pi$. Let degree $\pi = d$. Then the product

$$\xi = (\langle \pi \rangle - \langle 1 \rangle)(\langle f_2 \rangle - \langle 1 \rangle) \ldots (\langle f_n \rangle - \langle 1 \rangle)$$

in $I^n E$, where each representative f_i has degree $< d$, satisfies $\partial_\pi \xi = \eta$, and satisfies $\partial_{\pi'} \xi = 0$ for every $\pi' \neq \pi$ with degree $\pi' \geqq d$.

Now, given any element (η_π) of $\oplus\, I^{n-1}\bar{E}_\pi$, let

$$d_0 = \mathrm{Max}\,\{\mathrm{degree}\,\pi \mid \eta_\pi \neq 0\}.$$

Then it follows by induction on d_0 that (η_π) is the image of some element in $I^n E$.

To prove exactness in the middle of the sequence 5.7, consider any $\xi \in I^n E$ which maps to zero in $\oplus I^{n-1}\bar{E}_\pi$. According to 5.3, ξ comes from some element ζ of WF. Now apply the homomorphism ρ of §5.4. Evidently ρ maps $I^n E$ into $I^n F$, and evidently $\rho(\xi)=\zeta$. This proves that $\zeta \in I^n F$; which completes the proof of 5.7.

Corollary 5.8. *If the questions* 4.3 *and* 4.4 *have affirmative answers for every finite extension $\bar{E}_\pi$ of a field F, then they have affirmative answers for the field $E=F(t)$ of rational functions.*

The proof is completely analogous to that of 5.2.

§6. Relations with Galois Cohomology

The following construction is due to Bass and Tate. For any field F of characteristic $\neq 2$, let F_s be a separable closure, and let $G=G_F$ be the Galois group of F_s over F. Then the exact sequence

$$1 \to \{\pm 1\} \to F_s^\bullet \xrightarrow{2} F_s^\bullet \to 1,$$

upon which G operates, leads to an exact sequence

$$H^0(G; F_s^\bullet) \xrightarrow{2} H^0(G; F_s^\bullet) \to H^1(G; \{\pm 1\}) \to H^1(G; F_s^\bullet)$$

of cohomology groups; where the right hand group is zero. Identifying the first two groups with $F^\bullet$, and substituting $Z/2Z$ for $\{\pm 1\}$, this yields

$$F^\bullet \xrightarrow{2} F^\bullet \xrightarrow{\delta} H^1(G; Z/2Z) \to 0.$$

The quotient $F^\bullet/F^{\bullet 2}$ can of course be identified with $k_1 F$.

Lemma 6.1 (Bass, Tate). *The isomorphism $l(a) \mapsto \delta(a)$ from $k_1 F$ to $H^1(G; Z/2Z)$ extends uniquely to a ring homomorphism*

$$h_F\colon\ k_* F \to H^*(G; Z/2Z).$$

Proof. It is only necessary to verify that each of the defining relations $l(a)\, l(1-a)=0$ for the ring $k_* F$ maps to a valid relation

$$\delta(a)\, \delta(1-a)=0$$

in $H^2(G; Z/2Z)$. But in fact, if we identify $H^2(G; Z/2Z)$ with the set of elements of order 2 in the Brauer group $H^2(G; F_s^\bullet)$, then $\delta(a)\, \delta(b)$ corresponds to the quaternion algebra associated with a, b. (Compare Delzant [5].) Since the quaternion algebra associated with $a, 1-a$ splits, the relation $\delta(a)\, \delta(1-a)=0$ follows.

Remark. Bass and Tate [3] also consider the more general homomorphism associated with the sequence

$$1 \to \{m\text{-th roots of } 1\} \to F_s^\bullet \xrightarrow{m} F_s^\bullet \to 1,$$

but we will only be interested in the case $m=2$.

I do not know of any examples for which the homomorphism $h=h_F$ fails to be bijective. Here is a list of special cases.

Lemma 6.2. *If the field F is finite, or local, or global, or real closed, then the homomorphism*

$$h_F\colon k_* F \to H^*(G; Z/2Z)$$

is bijective. Furthermore if F is the direct limit of subfields F_α, and if each h_{F_α} is bijective, then h_F is bijective.

Proof. The finite, local, and real closed cases are straightforward. (Compare §1, together with Serre [15, II, pp. 10–20].) Suppose then that F is a global field. Bass and Tate [3] prove that the homomorphism

$$h_2\colon k_2 F \to H^2(G; Z/2Z)$$

is bijective. But for $n \geqq 3$ the group $H^n(G; Z/2Z)$ has been completely described by Tate [19, §3.1]. Comparing with Tate's computation of $k_n F$, as described in §1.8 or the Appendix, it follows that h_n is bijective also.

Finally, the statement for direct limits follows easily from [15, I, p. 9]. This completes the proof.

Here is one final partial result. Let $F((t))$ be the field of formal power series in one variable over F.

Theorem 6.3. *If h_F is bijective, then $h_{F((t))}$ is bijective.*

Proof. We will concentrate on the characteristic p case, leaving characteristic zero to the reader. Recall that $p \neq 2$.

Let V be the maximal tamely ramified extension of $F((t))$. (Compare Artin [1, pp. 70, 81].) Then V can be obtained from $F_s((t))$ by adjoining $t^{1/r}$ for every integer r prime to p. The Galois group G_V is a pro-p-group; and the quotient $G_{F_s((t))}/G_V$, which we denote briefly by $G_{V/F_s((t))}$, is isomorphic to $\varprojlim (Z/rZ)$, taking the inverse limit over integers r prime to p. Hence the mod 2 cohomology group

$$H^n G_{F_s((t))} \cong H^n G_{V/F_s((t))}$$

is cyclic of order 2 for $n=0, 1$, and is zero otherwise.

Clearly there is an exact sequence

$$1 \to G_{F_s((t))} \to G_{F((t))} \to G_F \to 1.$$

Dividing the first two groups by G_V, we obtain a sequence

$$1 \to G_{V/F_s((t))} \to G_{V/F((t))} \to G_F \to 1$$

which is actually split exact, since each automorphism of F_s over F lifts uniquely to an automorphism of V which keeps each $t^{1/r}$ fixed.

The associated cohomology spectral sequence now gives rise to a split exact sequence

$$0 \to H^n G_F \to H^n G_{V/F((t))} \to H^{n-1} G_F \to 0.$$

Note that the middle group is canonically isomorphic to $H^n G_{F((t))}$.

With a little work one can check that the homomorphism $H^n G_{F((t))} \to H^{n-1} G_F$ carries each product $\delta(t)\delta(u_2)\dots\delta(u_n)$ to $\delta(\bar{u}_2)\dots\delta(\bar{u}_n)$. Hence the following diagram is commutative:

$$\begin{array}{ccccc} k_n F & \longrightarrow & k_n F((t)) & \longrightarrow & k_{n-1} F \\ \downarrow & & \downarrow & & \downarrow \\ H^n G_F & \longrightarrow & H^n G_{F((t))} & \longrightarrow & H^{n-1} G_F. \end{array}$$

(Compare §2.6.) Applying the Five Lemma, the conclusion 6.3 follows.

Appendix: $K_*/2K_*$ for a Global Field

The arguments in this appendix are due to Tate.

Let F be a global field of characteristic $\neq 2$. We will again use the abbreviation $k_* F$ for the algebra $K_* F/2K_* F$.

The group $k_2 F$ has been computed by Bass and Tate as follows.

Lemma A.1. *There is an exact sequence*

$$0 \to k_2 F \to \oplus k_2 F_v \to Z/2Z \to 0,$$

where the summation extends over all completions F_v of F. Here the homomorphism $k_2 F \to k_2 F_v$ is induced by inclusion, and the homomorphism $k_2 F_v \to Z/2Z$ is injective.

In fact we recall from §1 that the group $k_2 F_v$ is cyclic of order 2, unless F_v is the complex field in which case $k_2 F_v$ is clearly zero. The composition

$$k_2 F \to k_2 F_v \subset Z/2Z$$

evidently carries each generator $l(a)\,l(b)$ of $k_2 F$ to either 0 or 1 according as the quadratic Hilbert symbol $(a, b)_v$ is trivial or not.

For the proof, we refer to Bass and Tate [3]. (Alternatively, this lemma can be proved by comparing the isomorphism $k_2 F \cong I^2/I^3$ of §4.1 with standard descriptions of the Witt ring of a global field.)

Theorem A.2 (Tate). *For $n \geqq 3$ the natural homomorphism*

$$k_n F \to \oplus k_n F_v$$

is an isomorphism.

Here the group $k_n F_v$ is cyclic of order 2 if F_v is the real field, and is zero otherwise. So it follows that the groups

$$k_3 F \cong k_4 F \cong k_5 F \cong \cdots$$

are finite, and in fact are zero unless F has a real completion.

To prove A.2, first consider any homomorphism Φ from $k_n F$ to the multiplicative group $\{\pm 1\}$. The image $\Phi(l(a_1) \ldots l(a_n))$ will be denoted briefly by $\varphi(a_1, \ldots, a_n)$. Thus φ is a symmetric function of n variables, multiplicative in each variable, and $\varphi(a_1, \ldots, a_n) = 1$ whenever $a_1 + a_2 = 1$.

If $n = 2$, then it follows from A.1 that any such function $\varphi(a, b)$ can be expressed in terms of the Hilbert symbols $(a, b)_v$ as a product

$$\varphi(a, b) = \prod_v (a, b)_v^{\varepsilon_v},$$

where each exponent ε_v is 0 or 1. These exponents are well defined except that we may simultaneously replace each ε_v by $1 - \varepsilon_v$.

Now suppose that $n = 3$. For fixed c the correspondence

$$a, b \mapsto \varphi(a, b, c)$$

can be described as above. Thus there exist exponents $\varepsilon_v(c)$ so that

$$\varphi(a, b, c) = \prod_v (a, b)_v^{\varepsilon_v(c)}.$$

Fixing b and c, consider the idele (d_v) whose v-th component is

$$d_v = b^{\varepsilon_v(c)} c^{\varepsilon_v(b)}.$$

Using the symmetry relation

$$\varphi(a, b, c) = \varphi(a, c, b)$$

it follows that

$$\prod_v (a, d_v)_v = 1. \tag{9}$$

We will need the following classical result.

Lemma A.3. *If an idele (d_v) satisfies the product formula* (9) *for every non-zero field element a, then (d_v) can be expressed as the product of a field element d and the square of an idele.*

This is proved for example in Weil [20, p. 262].

Thus, given field elements b and c, we can construct the idele (d_v), and hence the field element d, so that

$$d \in b^{\varepsilon_v(c)} c^{\varepsilon_v(b)} F_v^{\bullet 2} \tag{10}$$

for every v.

Consider the extension field $F(\sqrt{b}, \sqrt{c})$. Since d is a square in every completion of this field, it follows that d is a square in the field $F(\sqrt{b}, \sqrt{c})$ itself. By Kummer theory, this implies that d can be expressed as $b^i c^j$ times the square of an element of F. Here the exponents i and j are equal to 0 or 1. The assertion (10) now implies that

$$b^{\varepsilon_v(c)-i} c^{\varepsilon_v(b)-j} \in F_v^{\bullet 2} \tag{11}$$

for every v.

Lemma A.4. *If v and w are discrete valuations (i.e. corresponding to finite primes), then $\varepsilon_v(c) = \varepsilon_w(c)$ for all c.*

Proof. Note that the groups $F_v^\bullet / F_v^{\bullet 2}$ and $F_w^\bullet / F_w^{\bullet 2}$ both have order at least 4. So given c it is possible to choose b so that the image of b in $F_v^\bullet / F_v^{\bullet 2}$ is independent of c, and simultaneously so that the image of b in $F_w^\bullet / F_w^{\bullet 2}$ is independent of c. Thus (11) implies that

$$\varepsilon_v(c) - i = 0, \quad \varepsilon_w(c) - i = 0;$$

which proves A.4.

Proof of Theorem A.2. Replacing every $\varepsilon_v(c)$ by $1 - \varepsilon_v(c)$ if necessary, we may assume that $\varepsilon_v(c) = 0$ for every discrete valuation v. Hence in the formula

$$\varphi(a, b, c) = \prod\nolimits_v (a, b)_v^{\varepsilon_v(c)},$$

we need only take the product over real completions of F. It follows that $\varphi(a, b, c) = 1$ unless there exists a real completion at which both a and b are negative.

But this is true for every φ. So it follows that:

Lemma A.5. *The product $l(a)\, l(b)\, l(c) \in k_3 F$ is zero unless there exists a real completion at which both a and b are negative.*

The rest of the proof is easy. Let $v_1, \ldots, v_r$ be the real valuations, and let $e_1, \ldots, e_r$ be field elements such that e_j is negative in the v_j-th completion but positive in the other real completions. Then A.5 implies that a product $l(e_{i_1}) \ldots l(e_{i_n})$ with $n \geqq 3$ is zero unless $i_1 = \cdots = i_n$. On the other hand the powers $l(e_1)^n, \ldots, l(e_r)^n$ certainly are linearly independent, since they map into linearly independent elements of $\oplus_v k_n F_v$.

Since F^* is generated by $e_1, \ldots, e_r$ together with the totally positive elements, it follows immediately that these powers $l(e_1)^n, \ldots, l(e_r)^n$ actually form a basis for $k_n F$, $n \geqq 3$. This completes the proof.

References

1. Artin, E.: Algebraic numbers and algebraic functions. New York: Gordon and Breach 1967.
2. Bass, H.: K_2 and symbols, pp. 1 – 11 of Algebraic K-theory and its geometric applications. Lecture Notes in Mathematics, Vol. **108**. Berlin-Heidelberg-New York: Springer 1969.
3. – Tate, J.: K_2 of global fields (in preparation).
4. Birch, B. J.: K_2 of global fields (mimeographed proceedings of conference, S.U.N.Y. Stony Brook 1969).
5. Delzant, A.: Definition des classes de Stiefel-Whitney d'un module quadratique sur un corps de caractéristique différente de 2. C.R. Acad. Sci. Paris **255**, 1366 – 1368 (1962).
6. Kaplansky, I., Shaker, R. J.: Abstract quadratic forms. Canad. J. Math. **21**, 1218 – 1233 (1969).
7. Kervaire, M.: Multiplicateurs de Schur et K-théorie (to appear in de Rham Festschrift).
8. Matsumoto, H.: Sur les sous-groupes arithmétiques des groupes semi-simples deployés. Ann. Sci. Ec. Norm Sup. 4^e série **2**, 1 – 62 (1969).
9. Milnor, J.: Notes on algebraic K-theory (to appear).
10. Moore, C.: Group extensions of p-adic and adelic linear groups. Publ. Math. I.H.E.S. **35**, 5 – 74 (1969).
11. Nobile, A., Villamayor, O.: Sur la K-théorie algébrique. Ann. Sci. Ec. Norm. Sup. 4^e série **1**, 581 – 616 (1968).
12. O'Meara, O. T.: Introduction to quadratic forms. Berlin-Göttingen-Heidelberg: Springer 1963.
13. Pfister, A.: Quadratische Formen in beliebigen Körpern. Inventiones math. **1**, 116 – 132 (1966).
14. Scharlau, W.: Quadratische Formen und Galois-Cohomologie Inventiones math. **4**, 238 – 264 (1967).
15. Serre, J. P.: Cohomologie Galoisienne. Lecture Notes in Mathematics, Vol. **5**. Berlin-Heidelberg-New York: Springer 1964.
16. Springer, T. A.: Quadratic forms over a field with a discrete valuation. Indag. Math. **17**, 352 – 362 (1955).
17. Swan, R.: Algebraic K-theory. Lecture Notes in Mathematics, Vol. **76**. Berlin-Heidelberg-New York: Springer 1968.
18. – Non-abelian homological algebra and K-theory, (mimeographed) Univ. of Chicago, 1968.
19. Tate, J.: Duality theorems in Galois cohomology over number fields. Proc. Int. Congr. Math. Stockholm, 288 – 295 (1963).
20. Weil, A.: Basic number theory. Berlin-Heidelberg-New York: Springer 1967.

John Milnor
Mathematics Department
Massachusetts Institute of Technology
Cambridge, Mass. 02139 (USA)

(Received February 10, 1970)