K-Theory **27:** 245–252, 2002.

Milnor *K*-Groups and Finite Field Extensions

KARIM JOHANNES BECHER
Fachbereich Mathematik und Statistik, D204, Universität Konstanz, D-78457 Konstanz, Germany.
e-mail: becher@maths.ucd.ie

(Received: June 2002)

Abstract. Let E/F be a finite separable field extension and let m denote the integral part of $\log_2[E : F]$. David Leep recently showed that if $\mathrm{char}(F) \neq 2$, then for $n \geqslant m$ the nth power of the fundamental ideal in the Witt ring of E satisfies the equality $I^n E = I^{n-m} F \cdot I^m E$. The aim of this note is to prove the analogous equality for the Milnor K-groups, that is $K_n E = K_{n-m} F \cdot K_m E$ for $n \geqslant m$. In either of these equalities one may not replace m by $m - 1$, as examples of certain m-quadratic extensions indicate.

Mathematics Subject Classifications (2000): 11E81, 12F05, 19D45.

Key words: Milnor *K*-theory, higher *K*-groups, Witt ring, field extension.

1. Main Result and Consequences

Throughout this paper, let F denote a field. We recall the definition of the groups $K_n F (n \geqslant 1)$ of Milnor K-theory, introduced in [4]: for $n \geqslant 1$, let $K_n F$ be the Abelian group generated by elements $\{a_1, \dots, a_n\}$ $(a_1, \dots, a_n \in F^\times)$, called *symbols*, which are subject to the only relations that $\{a_1, \dots, a_n\}$ be zero whenever $a_i + a_{i+1} = 1$ in F and that $\{*, \dots, *\}$ viewed as a function $(F^\times)^n \to K_n F$ be multilinear. The group operation in $K_n F$ is written additively. As a consequence of the defining relations, one has, further, for $a_1, \dots, a_n \in F^\times$, that $\{a_1, \dots, a_n\} = 0$ if $a_i + a_{i+1} = 0$ for some $i < n$ and that $\{a_{\sigma(1)}, \dots, a_{\sigma(n)}\} = \mathrm{sgn}(\sigma)\{a_1, \dots, a_n\}$ for any permutation $\sigma \in \mathcal{S}_n$ with signature $\mathrm{sgn}(\sigma) \in \{+1, -1\}$ (cf. [4, Lemma 1.3 and Lemma 1.1]).

With the convention $K_0 F := \mathbb{Z}$, the group $K_* F := \coprod_{i \geqslant 0} K_i F$ has a natural structure as a graded $\mathbb{Z}$-algebra. Furthermore, if L/F is an arbitrary field extension, then the natural group homomorphisms $K_n F \to K_n L$ $(n \geqslant 0)$ and the induced ring homomorphism $K_* F \to K_* L$ turn $K_* L$ into a $K_* F$-algebra.

THEOREM 1.1. *Let E/F be a finite field extension such that $E = F(\theta)$ for some $\theta \in E$. The group $K_n E$ is generated by the symbols $\{f_1(\theta), \dots, f_n(\theta)\}$ where $f_1, \dots, f_n \in F[X]$ are such that $f_i(\theta) \neq 0$ for $1 \leqslant i \leqslant n$ and such that* $\deg(f_i) \leqslant \frac{1}{2}\deg(f_{i+1})$ *for* $1 \leqslant i < n$ *and* $\deg(f_n) \leqslant \frac{1}{2}[E : F]$.

The proof of this statement will be achieved at the end of Section 2. We first want to discuss its consequences. The following corollary can be considered as the main statement of this article:

COROLLARY 1.2. *Let E/F be a finite separable extension and let m denote the integral part of* $\log_2[E : F]$. *For $n \geqslant m$ one has $K_nE = K_{n-m}F \cdot K_mE$.*

The equality in the statement can be rephrased by saying that K_nE is generated by those symbols $\{a_1, \ldots, a_n\}$ $(a_1, \ldots, a_n \in E^\times)$ where $a_1, \ldots, a_{n-m}$ lie in F. This is actually what we are going to show.

Proof. By the 'primitive element theorem' there exists $\theta \in E$ such that $E = F(\theta)$. Theorem 1.1 then implies that K_nE is generated by the symbols $\{f_1(\theta), \ldots, f_n(\theta)\}$ where $f_1, \ldots, f_n \in F[X]$ are such that $f_i(\theta) \neq 0$ and $\deg(f_i) \leqslant 2^{i-n-1}[E : F]$ for $1 \leqslant i \leqslant n$; in particular for $i \leqslant n - m$, since $[E : F] < 2^{m+1}$, f_i must be constant, whence $f_i(\theta) \in F^\times$. □

In Section 3 we will see that, in general, the choice of the value for m in Corollary 1.2 is best possible.

At least when E/F has no nontrivial subextension (e.g. when $[E : F]$ is prime), the hypothesis in Corollary 1.2 that the extension E/F be separable is superfluous, since the existence of θ such that $E = F(\theta)$ then is evident. In particular one has $K_nE = K_{n-1}F \cdot K_1E$ whenever $[E : F] \leqslant 3$; this has already been observed by Merkurjev in [3, Lemma 2] (for the crucial case $n = 2$).

COROLLARY 1.3 (Merkurjev). *Let E/F be a field extension of degree* 2 *or* 3 *and let $l \in \mathbb{N}$. If $K_nF/l \cdot K_nF = 0$ then $K_{n+1}E/l \cdot K_{n+1}E = 0$.*

Proof. As just explained, we have $K_{n+1}E = K_nF \cdot K_1E$. Hence, if K_nF is divisible by l then so is $K_{n+1}E$. □

Examples of finite field extensions E/F where $K_nF/l \cdot K_nF = 0$ while $K_nE/l \cdot K_nE \neq 0$, for given $l, n \in \mathbb{N}$, are easy to obtain. One way of constructing such examples will be explained in the third section. By this fact together with the last corollary we are lead to

QUESTION 1.4. Let E/F be a finite field extension and $l, n \in \mathbb{N}$. Assume that $K_nF/l \cdot K_nF = 0$. Does it follow that $K_{n+1}E/l \cdot K_{n+1}E = 0$?

Note that the problem can be easily reduced to the case where l is prime.

In the rest of this section we compare the above corollaries with the results of Leep in [2] which inspired the present investigation.

We assume that $\mathrm{char}(F) \neq 2$. For $n \geqslant 0$ one denotes by $I^nF := (IF)^n$ the nth power of the fundamental ideal in the Witt ring of F, further by $\bar{I}^nF$ the quotient $I^nF/I^{n+1}F$. The natural homomorphism $K_nF \to \bar{I}^nF$ which sends any symbol

$\{x_1, \ldots, x_n\}$ to the class of the n-fold Pfister form $\langle 1, -x_1\rangle \otimes \cdots \otimes \langle 1, -x_n\rangle$ is clearly surjective. (By part of the Milnor conjecture its kernel is precisely $2K_nF$; in characteristic zero, a proof of this has recently been given in [5, Theorem 4.1].) Elman and Lam have shown by elementary arguments that $K_nF/2K_nF = 0$ if and only if $I^nF = 0$ [1, Corollary 3.3].

We consider again a finite extension E/F and denote by m the integral part of $\log_2[E : F]$. Leep showed in [2, Theorem 2.1] that

$$I^nE = I^{n-m}F \cdot I^mE. \tag{1}$$

As an immediate consequence we get

$$\bar{I}^nE = \bar{I}^{n-m}F \cdot \bar{I}^mE \tag{2}$$

in the graded Witt ring of E. On the other hand, the last equation can also be deduced from Corollary 1.2 using the natural homomorphism $K_nF \to \bar{I}^nF$. (Indeed, one applies Corollary 1.2 to E_0/F where E_0 is the separable closure of F in E and observes that $\bar{I}^nE_0 \to \bar{I}^nE$ is surjective, as explained in [2, Section 2].)

One can ask whether equalities (1) and (2) are equivalent. If so then Leep's result would follow from Corollary 1.2. At least under some additional assumption such as $I^eF = 0$ or (weaker) $I^eE = IF \cdot I^{e-1}E$ for some $e \in \mathbb{N}$, one can indeed prove that (2) implies (1), regardless of the value of $m \leqslant n$.

Furthermore, since $K_nF/2K_nF = 0$ if and only if $I^nF = 0$ [1, Corollary 3.3], it follows from [2, Corollary 3.4] that in the case where $l = 2$ and $\mathrm{char}(F) \neq 2$, the Question 1.4 has a positive answer at least if $[E : F] \leqslant 5$.

2. On K_n of a Rational Function Field

We will obtain Theorem 1.1 at the end of this section as a consequence of an observation which gives generators for certain subgroups L_d of $K_nF(X)$, where $F(X)$ is the rational function field in one variable over F (Proposition 2.3). To carry this information on $F(X)$ down to the finite extension $E = F(\theta)$ of F we use a surjection $K_nF(X) \to K_nE$, which has been considered by Milnor.

In order to shrink the set of generators for those groups, we will use a degree reduction argument which is based on the division algorithm for polynomials together with the following rule:

LEMMA 2.1. *Let $f, g, h, t \in F^\times$ be such that $g = fh + t$. In K_2F one has*

$$\{f, g\} = -\{-h, g\} + \{t, g\} - \{t, h\} - \{t, f\} = \left\{-h, \frac{1}{g}\right\} + \left\{t, \frac{g}{fh}\right\}.$$

Proof. By hypothesis we have

$$\frac{g}{fh} - \frac{t}{fh} = 1,$$

hence

$$\left\{-\frac{t}{fh}, \frac{g}{fh}\right\} = 0$$

in K_2F. Expanding the last equation yields

$$\begin{aligned} 0 &= \{t, g\} - \{t, fh\} - \{-fh, g\} + \{-fh, fh\} \\ &= \{t, g\} - \{t, f\} - \{t, h\} - \{f, g\} - \{-h, g\}. \end{aligned}$$

This shows the first equality of the statement, the second one is obvious. □

We define a partial order on the set $\mathbb{N}_0^n$ in the following way: for two n-tuples $d = (d_1, \dots, d_n)$ and $e = (e_1, \dots, e_n)$ where $d_1, \dots, d_n, e_1, \dots, e_n \in \mathbb{N}_0$, we write $d \leqslant e$ in case we have $d_i \leqslant e_i$ for $1 \leqslant i \leqslant n$. Obviously, any nonempty subset of $\mathbb{N}_0^n$ has a minimal element with respect to this partial order. In the sequel, we implicitly refer to this partial order on $\mathbb{N}_0^n$ when we say that an element of $\mathbb{N}_0^n$ is minimal with respect to a certain condition.

LEMMA 2.2. *Let L be a proper subgroup of $K_nF(X)$. Let $f_1, \dots, f_n$ be nonzero polynomials in $F[X]$ such that* $(\deg(f_1), \dots, \deg(f_n))$ *is minimal with respect to the condition that the symbol $\{f_1, \dots, f_n\}$ belong to $K_nF(X)\backslash L$. Then*

(a) *each of the polynomials $f_1, \dots, f_n$ is either a constant or irreducible*,
(b) *for any distinct positive $i, j \leqslant n$, if* $\deg(f_i) \leqslant \deg(f_j)$ *then one has actually* $\deg(f_i) \leqslant \frac{1}{2}\deg(f_j)$.

Proof. (a) Let $1 \leqslant i \leqslant n$. If $f_i = gh$ for some $g, h \in F[X]$ then the equality $\{f_1, \dots, f_i, \dots, f_n\} = \{f_1, \dots, g, \dots, f_n\} + \{f_1, \dots, h, \dots, f_n\}$ shows that at least one of the last two symbols does not belong to L; by minimality of $(\deg(f_1), \dots, \deg(f_n))$, one of g and h must be of the same degree as f_i. This means that f_i is irreducible.

(b) Observe that any change of the order of $f_1, \dots, f_n$ leaves the symbol $\{f_1, \dots, f_n\}$ unchanged up to a sign and therefore does not affect the hypotheses of the lemma. Hence, to prove (b) we may assume without loss of generality that $i = 1$ and $j = 2$.

Suppose now that $\deg(f_1) \leqslant \deg(f_2)$. Using the division algorithm, we may write $f_2 = f_1h + t$ with polynomials $h, t \in F[X]$ where either $t = 0$ or $\deg(t) < \deg(f_1)$. If $t = 0$ then $\{f_1, \dots, f_n\} = -\{-h, f_2, \dots, f_n\}$. On the other hand, if $t \neq 0$ then from Lemma 2.1 we obtain

$$\begin{aligned} \{f_1, \dots, f_n\} &= -\{-h, f_2, \dots, f_n\} + \{t, f_2, \dots, f_n\} - \\ &\quad - \{t, h, f_3, \dots, f_n\} - \{t, f_1, f_3, \dots, f_n\} \end{aligned}$$

and by the minimality of $(\deg(f_1), \dots, \deg(f_n))$, the last three symbols lie in L. In any case we conclude from $\{f_1, \dots, f_n\} \notin L$ that $\{-h, f_2, \dots, f_n\} \notin L$. By the minimality of $(d_1, \ldots, d_n)$ it follows that $\deg(h) \geqslant \deg(f_1)$ which leads to $\deg(f_2) = \deg(f_1) + \deg(h) \geqslant 2\deg(f_1)$. □

PROPOSITION 2.3. *For a given positive integer d, let L_d denote the subgroup of $K_nF(X)$ generated by the symbols $\{f_1, \ldots, f_n\}$ where $f_1, \ldots, f_n \in F[X]$ are nonzero polynomials of degree at most d. L_d is already generated by the symbols $\{g_1, \ldots, g_n\}$ where $g_1, \ldots, g_n \in F[X]$ are nonzero polynomials with $\deg(g_i) \leqslant \frac{1}{2}\deg(g_{i+1})$ for $1 \leqslant i < n$ and $\deg(g_n) \leqslant d$.*

Proof. Let L be the subgroup of L_d generated by the symbols $\{g_1, \ldots, g_n\}$ where $g_1, \ldots, g_n \in F[X]$ are nonzero and such that $\deg(g_i) \leqslant \frac{1}{2}\deg(g_{i+1})$ for $1 \leqslant i < n$ and $\deg(g_n) \leqslant d$. Assume that L is a proper subgroup of L_d. We may then choose nonzero polynomials $f_1, \ldots, f_n \in F[X]$ of degree less or equal to d such that $\{f_1, \ldots, f_n\}$ belongs to $K_nF(X)\backslash L$ and with $(\deg(f_1), \ldots, \deg(f_n))$ minimal with respect to this condition. Since the symbol $\{f_1, \ldots, f_n\}$ is invariant up to a sign under any change of order of $f_1, \ldots, f_n$, we may further assume that $\deg(f_1) \leqslant \cdots \leqslant \deg(f_n) \leqslant d$. By the last lemma it follows that $\deg(f_i) \leqslant \frac{1}{2}\deg(f_{i+1})$ for $1 \leqslant i < n$. But then $\{f_1, \ldots, f_n\}$ belongs to L, by definition of L. This contradicts the choice of $f_1, \ldots, f_n$. The conclusion is that L equals L_d, which gives the statement. □

COROLLARY 2.4. *The group $K_nF(X)$ is generated by the symbols $\{f_1, \ldots, f_n\}$ where $f_1, \ldots, f_n \in F[X]$ are nonzero with $\deg(f_i) \leqslant \frac{1}{2}\deg(f_{i+1})$ for $1 \leqslant i < n$.*

Proof. This is clear from the above proposition, since $K_nF(X)$ is the union of the groups L_d $(d \geqslant 1)$. □

The next lemma is [2, Corollary 2.7]. For the convenience of the reader, we include the proof.

LEMMA 2.5. *Let $E = F(\theta)$ be a finite field extension of F of degree l. Any nonzero element of E can be written as a quotient $f(\theta)/g(\theta)$ where f and g are nonzero polynomials of degree less or equal to* $[l/2]$.

Proof. Let V be an arbitrary F-subspace of E of dimension strictly greater than $l/2$. We claim that every nonzero element of E is a quotient of two nonzero elements of V. Indeed, for $x \in E\backslash\{0\}$ the F-subspaces V and Vx of E both have dimension greater than $l/2$, hence their intersection is not zero; in other words, there exist $v, w \in V\backslash\{0\}$ such that $v = wx$, i.e. $x = v/w$.

We apply this to the F-space V generated by $1, \theta, \theta^2, \ldots, \theta^{[\frac{l}{2}]}$. Since $V\backslash\{0\} = \{f(\theta) \in E \mid f \in F[X]\backslash\{0\}, \deg(f) \leqslant [\frac{l}{2}]\}$, the statement follows. □

We are now ready to prove Theorem 1.1. Using the identification of $E^\times$ with K_1E, the last lemma actually corresponds to the case in Theorem 1.1 where $n = 1$.

We continue to consider a finite extension E/F such that $E = F(\theta)$ for some $\theta \in E$. By the 'primitive element theorem', the last condition is satisfied whenever E/F is a separable extension. Let π be the minimal polynomial of θ over F. Any nonzero element of $F(X)$ can be written in the form $f/g \cdot \pi^z$ where $f, g \in F[X]$ are polynomials not divisible by π and $z \in \mathbb{Z}$. Associating to an element $f/g \cdot \pi^z \in F(X)^\times$ the element $f(\theta)/g(\theta) \in E$ defines a surjective map $F(X)^\times \longrightarrow E^\times$. This map induces a group homomorphism ψ_n: $K_nF(X) \longrightarrow K_nE$, uniquely determined by the rules that $\psi_n(\{f_1, \dots, f_n\}) = \{f_1(\theta), \dots, f_n(\theta)\}$ if $f_1, \dots, f_n \in F[X]$ are not divisible by π and that $\psi_n(\{\pi, *, \dots, *\}) = 0$. The homomorphism ψ_n depends on the choice of θ, its construction is due to J. Milnor [4, Lemma 2.2].

Let d denote the integral part of $\frac{1}{2}[E : F]$ and L_d the subgroup of $K_nF(X)$ generated by symbols $\{f_1, \dots, f_n\}$ where $f_1, \dots, f_n \in F[X]\backslash\{0\}$ are of degree less or equal to d. From the last lemma we conclude that $\psi_n(L_d) = K_nE$. Using this, Theorem 1.1 follows immediately from Proposition 2.3.

3. Two Examples

The following proposition is a variant of [2, Proposition 3.1]. It gives an example of a separable field extension E/F such that the equality $K_nE = K_{n-m}F \cdot K_mE$, which holds for $m = [\log_2[E : F]]$ by Corollary 1.2, would be wrong for any lower value for m.

PROPOSITION 3.1. *Let k be a field of characteristic different from 2 and let $m \leqslant n$. Let $E = k(X_1, \dots, X_n)$, the rational function field in n variables over k, and $F = k(X_1^2, \dots, X_m^2, X_{m+1}, \dots, X_n)$. Then*

(a) *E/F is a separable extension of degree 2^m, that is $m = \log_2[E : F]$,*
(b) *the class in the group $\bar{I}^nE$ represented by the n-fold Pfister form $\langle 1, -X_1\rangle \otimes \cdots \otimes \langle 1, -X_n\rangle$ is not contained in $\bar{I}^{n-m+1}F \cdot \bar{I}^{m-1}E$,*
(c) *$I^nE \neq I^{n-m+1}F \cdot I^{m-1}E$ and $K_nE \neq K_{n-m+1}F \cdot K_{m-1}E$.*

Proof. Part (a) should be clear. Let $\bar{k}$ denote an algebraic closure of k. It is clear that the n-fold Pfister form $\langle 1, -X_1\rangle \otimes \cdots \otimes \langle 1, -X_n\rangle$ stays anisotropic over $\bar{E} := \bar{k}((X_1))\dots((X_n))$ and thus represents a nontrivial class in $\bar{I}^n\bar{E}$. The field $\bar{E}$ contains the subfield $\bar{F} := \bar{k}((X_1^2))\dots((X_m^2))((X_{m+1}))\dots((X_n))$ which in turn contains F.

Consider an anisotropic $(n-m+1)$-fold Pfister form π defined over $\bar{F}$. Since $|\bar{F}^\times/\bar{F}^{\times 2}| = 2^n$ and $X_1^2, \dots, X_m^2$ lie in $\bar{E}^2$, it is clear that the image of $\bar{F}^\times/\bar{F}^{\times 2}$ in $\bar{E}^\times/\bar{E}^{\times 2}$ has cardinality 2^{n-m}. It follows that in any diagonalization of π over $\bar{E}$, at least two of the 2^{n-m+1} entries must lie in the same square class of $\bar{E}^\times$. Since $-1 \in \bar{E}^2$, it follows that π becomes hyperbolic over $\bar{E}$.

This argument shows that the image of $\bar{I}^{n-m+1}F \cdot \bar{I}^{m-1}E$ in $\bar{I}^n\bar{E}$ is zero, while we have seen that the image of $\bar{I}^nE$ in $\bar{I}^n\bar{E}$ contains the class of $\langle 1, -X_1\rangle \otimes \cdots \otimes \langle 1, -X_n\rangle$, which is nonzero as a consequence of the Arason–Pfister–Hauptsatz

[6, 4.5.6. Theorem]. This shows (*b*), while (*c*) is an immediate consequence of (*b*). □

Remark 3.2. It is not difficult to see that the statements of the proposition hold more generally when F is a subfield of $\bar{k}((X_1^2))\dots((X_m^2))((X_{m+1}))\dots((X_n))$ containing $k(X_1^2, \dots, X_m^2, X_{m+1}, \dots, X_n)$ and $E = F(X_1, \dots, X_n)$.

We finish with a counter-example to a variation of Question 1.4 which might look more natural to ask at first sight.

EXAMPLE 3.3. Let $n \geqslant 1$ and let p be a prime. Suppose that F_1 is a field containing a primitive p-root of unity (in particular, not of characteristic p), having no cyclic extension of order p but having a Galois extension L/F_1 whose degree is divisible by p. Hence, there exists an F_1-automorphism of L which is of order p. Let E_1 denote the subfield of L fixed by this automorphism. Then L/E_1 is a cyclic extension of degree p, in particular E_1 is not p-closed while F_1 is p-closed. For

$$F = F_1((X_1))\dots((X_{n-1})) \quad \text{and} \quad E = E_1((X_1))\dots((X_{n-1}))$$

we obtain

$$K_nF/p\cdot K_nF = 0, \qquad K_nE/p\cdot K_nE \neq 0$$

and

$$[E : F] = [E_1 : F_1] < \infty.$$

Note that a Galois extension E_1/F_1 with the desired properties can be constructed without difficulties. Take a field F_0 of characteristic different from p with a Galois extension E_0/F_0 having as Galois group the alternating group $\mathcal{A}_m$ for some $m \geqslant \max\,(5, p)$. Write $E_0 \cong F_0[X]/(f)$ with $f \in F_0[X]$. We choose F_1 as a maximal algebraic extension of F_0 such that f is irreducible over F_1 and put $E_1 = F_1[X]/(f)$. Then E_1/F_1 is a Galois extension with group $\mathcal{A}_m$. Since $\mathcal{A}_m$ is simple, this extension is linearily disjoint from any cyclic extension of F_1. Hence, by its choice the field F_1 is perfect and has no cyclic extensions and, in particular, it contains a pth root of unity.

Acknowledgements

The author wishes to express his gratitude to David Leep for his interest in this work and many valuable remarks. The author also thanks the referee, whose suggestions helped improve an earlier version of the manuscript.

This research was carried out while the author enjoyed the hospitality of the Institut de Mathématiques de Jussieu in Paris as a postdoctoral fellow, supported by the TMR network ‘Algebraic *K*-Theory, Linear Algebraic Groups and Related Structures’ (ERB FMRX CT-97-0107).

References

1. Elman, R. and Lam, T. Y.: Pfister forms and K-theory of fields, *J. Algebra* **23** (1972), 181–213.
2. Leep, D. B.: The Witt ring of quadratic forms under algebraic extensions, Preprint, 2001.
3. Merkurjev, A. S.: Brauer groups of fields, *Comm. Algebra* **11**(22) (1983), 2611–2624.
4. Milnor, J.: Algebraic K-theory and quadratic forms, *Invent. Math.* **9** (1969/1970), 318–344.
5. Orlov, D., Vishik, A. and Voevodsky, V.: An exact sequence for Milnor's K-theory with applications to quadratic forms, K-theory Preprint Archives, http://www.math.uiuc.edu/K-theory/0454/, 2000.
6. Scharlau, W.: *Quadratic and Hermitian Forms*, Springer-Verlag, Berlin, 1985.