International Electronic Journal of Algebra
Volume 2 (2007) 100-105

GALOIS MODULE STRUCTURE OF FIELD EXTENSIONS

Patrik Lundström

Received: 31 January 2007; Revised: 24 April 2007
Communicated by Derya Keskin Tütüncü

Abstract. We show, in two different ways, that every finite field extension has a basis with the property that the Galois group of the extension acts faithfully on it. We use this to prove a Galois correspondence theorem for general finite field extensions. We also show that if the characteristic of the base field is different from two and the field extension has a normal closure of odd degree, then the extension has a self-dual basis upon which the Galois group acts faithfully.

Mathematics Subject Classification (2000): 12F10, 12G05
Keywords: Galois theory, normal basis, self-dual basis

1. Introduction

If K/k is a finite field extension and G is a subgroup of the group $\mathrm{Aut}_k(K)$ of k-automorphisms of K, then the action of G on K induces a left $k[G]$-module structure on K in a natural way. If the order of G equals the degree $[K:k]$ of K as a vector space over k, then K/k is a Galois extension and the well known normal basis theorem (see e.g. Theorem 13.1 in [8]) implies that K is a free $k[G]$-module with one generator. This result can of course be formulated more concretely by saying that there is an element x in K such that the conjugates $g(x)$, $g \in G$, form a basis for K as a vector space over k. If the order of G is less than $[K:k]$, then K is still a free $k[G]$-module but not necessarily with one generator. In fact, if we let K^G denote the subfield of elements x in K with the property that $g(x) = x$ for all $g \in G$, then the following result holds.

Theorem 1. *If K/k is a finite field extension and G is a subgroup of $\mathrm{Aut}_k(K)$, then K is a free $k[G]$-module with $[K^G : k]$ generators.*

This result follows directly from the normal basis theorem. In fact, since the extension K/K^G is Galois, the field K is a free $K^G[G]$-module with one generator. If we pick such a generator x and a basis A for K^G as a vector space over k, then it is easy to check that the set of products ax, $a \in A$, freely generates K as a left

$k[G]$-module. In Section 2, we give two different *direct* proofs of Theorem 1, that is, proofs that do not use the normal basis theorem. Both of these proofs are based on descent, that is, the fact that a basis with the desired property exists for the extension $K \otimes_k L$ where L is a normal closure of K. The first proof is a variant of an idea of Noether and Deuring (see [10] and [6]) which involves the Krull-Schmidt theorem. The second proof is a generalization of a folkloristic idea using Hilbert's theorem 90. As a by product of Theorem 1, we obtain a Galois correspondence theorem for general finite field extensions (see Theorem 3). This correspondence is more or less well known but rarely stated in the literature.

Now suppose that K/k is separable and let S denote the set of embeddings of K into L. The trace map $\mathrm{tr}_{K/k} : K \to k$, defined by $\mathrm{tr}_{K/k}(x) = \sum_{s \in S} s(x)$, $x \in K$, induces a symmetric bilinear form $q_K : K \times K \to k$ by the relation $q_K(x, y) = \mathrm{tr}_{K/k}(xy)$, $x, y \in K$. The bilinear form q_K is also a G-form, that is, it is invariant under the action of G. The G-form structure of (K, q_K) has been extensively studied (see e.g. [2], [3], [4], [5], [7] and [9]). In [3] Bayer-Fluckiger and Lenstra show that if K/k is Galois, the characteristic of k is different from two and the order $|G|$ of the group G is odd, then (K, q_K) is isomorphic to the G-form $(k[G], q_0)$, where q_0 is the unit G-form, that is, the k-bilinear map $k[G] \times k[G] \to k$ defined by the relations $q_0(g, g) = 1$ and $q_0(g, g') = 0$ if $g \neq g'$ for all $g, g' \in G$. It is easy to see that such an isomorphism exists precisely when K/k has a normal basis which is self-dual with respect to the bilinear form q_K. Bayer-Fluckiger and Lenstra utilize a general result (see Theorem 2.1 in [3]) concerning hermitian modules and in a special case G-forms (see Theorem 4) to show the existence of self-dual normal bases. In Section 3, we use this idea to prove the following generalization of their result.

Theorem 2. *Let K/k be a finite separable field extension and suppose that G is a subgroup of $\mathrm{Aut}_k(K)$. If the characteristic of k is different from two and K/k has a normal closure L/k of odd degree, then (K, q_K) is isomorphic to the direct sum of $[K^G : k]$ copies of the unit G-form $(k[G], q_0)$.*

Bayer-Fluckiger [1] has shown that finite Galois extensions of odd degree have self-dual normal bases in the case when the characteristic of the base field is two also. It is not clear to the author if Theorem 2 can be extended to this case.

2. Galois module structure

In this section, we give two different proofs of Theorem 1. Then we use this result to obtain a Galois correspondence theorem for general finite field extensions (see Theorem 3). We will use the following two standard facts from field theory. Let F/F' be a field extension.

(F1) If H is a finite subgroup of $\mathrm{Aut}_{F'}(F)$, then $[F : F^H] = |H|$ and for any field K', with $F^H \subseteq K' \subseteq F$, F/K' is Galois.

(F2) If F/F' is finite and Galois, then $[F : F'] = |\mathrm{Aut}_{F'}(F)|$.

Now we show Theorem 1. We claim that it is enough to show the result for separable extensions. To show the claim we need some more notations and a lemma. Let K_1/k be the maximally separable subextension of K/k. Then K/K_1 is purely inseparable and since the restriction map from $\mathrm{Aut}_k(K)$ to $\mathrm{Aut}_k(K_1)$ is a bijection, we can, by abuse of notation, assume that G is a subset of both of these groups.

Lemma 1. *There is a basis B for K as a vector space over K_1 with the property that $s(b) = b$, $s \in S$, $b \in B$.*

Proof. By induction over the degree of K over K_1, we can assume that $K = K_1(b)$ for some purely inseparable $b \in K$ over K_1. By it's definition $B := \{1, b, b^2, \ldots, b^{p^m-1}\}$, where $[K : K_1] = p^m$, has the desired property. □

Now we show the claim. By Lemma 1, $K = \oplus_{b \in B} K_1 b$ where each b belongs to K^G. If we assume that K_1 is a free $k[G]$-module with $[K_1^G : k]$ generators, then, by (F1), K is a free $k[G]$-module with

$$[K : K_1][K_1^G : k] = \frac{[K : K^G][K^G : K_1^G][K_1^G : k]}{[K_1 : K_1^G]} = \frac{|G|[K^G : k]}{|G|} = [K^G : k]$$

generators and the claim follows. From now on we assume that K/k is separable.

First proof of Theorem 1. Recall that if X is a finite set, then $L[X]$ is defined to be the set of formal sums $\sum_{x \in X} l_x x$, where $l_x \in L$, $x \in X$. If G acts on X, then $L[X]$ is, in a natural way, a left $L[G]$-module. In the following lemma we let G act on $S^{-1} := \{s^{-1} \mid s \in S\}$ by composition from the left. The action of G on K induces a left $L[G]$-module structure on $K \otimes_k L$.

Lemma 2. *The left $L[G]$-modules $K \otimes_k L$ and $L[S^{-1}]$ are isomorphic.*

Proof. Define a map $\varphi : K \otimes_k L \to L[S^{-1}]$ by the relation $\varphi(a \otimes b) = \sum_{s \in S} s(a) b s^{-1}$, $a \in K$, $b \in L$. It is clear that φ is L-linear. Now we show that φ respects the action of G. Take $a \in K$, $b \in L$ and $g \in G$. Then $\varphi(g(a \otimes b)) = \varphi(g(a) \otimes b) = \sum_{s \in S} sg(a) b s^{-1}$. If we put $t := sg$, then $s^{-1} = gt^{-1}$ and hence $\varphi(g(a \otimes b)) = \sum_{t \in S} t(a) b g t^{-1} = g \sum_{t \in S} t(a) b t^{-1} = g\varphi(a \otimes b)$. By L-dimensionality, we only need to show that φ is injective to finish the proof. Suppose that $\varphi(x) = 0$

for some $x \in K \otimes_k L$. Take a basis a_t, $t \in S$, for K as a vector space over k. Then we can choose $l_t \in L$, $t \in S$, such that $x = \sum_{t \in S} a_t \otimes l_t$. Therefore $0 = \varphi(\sum_{t \in S} a_t \otimes l_t) = \sum_{s \in S} \sum_{t \in S} s(a_t) l_t s^{-1}$. This implies that $\sum_{t \in S} s(a_t) l_t = 0$, $s \in S$. However, by Dedekinds linear independence theorem (see e.g. Theorem 4.1 in [8]), the matrix $(s(a_t))_{s,t}$ is non-singular. Therefore $l_t = 0$, $t \in S$, which in turn implies that $x = 0$. □

To finish the first proof of Theorem 1 note that the isomorpism in Lemma 2 implies an isomorphism $K^{\oplus [L:k]} \cong k[S^{-1}]^{\oplus [L:k]}$ of $k[G]$-modules. Therefore, by the Krull-Schmidt theorem (see e.g. Theorem 7.5 in [8]), $K \cong k[S^{-1}]$ as $k[G]$-modules. Since the action of G on S^{-1} is faithful, $k[S^{-1}]$ decomposes into a direct sum of copies of $k[G]$, the number of these copies being equal to the number of orbits for the action of G on S^{-1}, which, in turn, by (F1), equals $|S|/|G| = [K : k]/[K : K^G] = [K^G : k]$. This ends the first proof.

Second proof of Theorem 1. This proof uses the language of Galois cohomology (for the details, see e.g. pp. 158-162 in [11]). Put $G' := \mathrm{Aut}_k(L)$ and $V := k[S^{-1}]$. Let E_V denote the set of all isomorphism classes of left $k[G]$-modules V' with the property that $V \otimes_k L$ and $V' \otimes_k L$ are isomorphic as left $L[G]$-modules. Now we show that E_V can be embedded in a pointed cohomology set. We can define an action of G' on the set of $L[G]$-module isomorphisms $f : V \otimes_k L \to V' \otimes_k L$ by $g(f) = g \circ f \circ g^{-1}$, $g \in G'$, where G' acts on the second factor in $V \otimes_k L$. It is easy to check that $G' \ni g \mapsto p_g := f^{-1} \circ g(f) \in \mathrm{Aut}_{L[G]}(V \otimes_k L)$ is a cocycle, that is, a map satisfying $p_{gh} = p_g g(p_h)$, $g, h \in G'$. Two cocycles p and p' are called cohomologous, denoted $p \sim p'$, if there exists $a \in \mathrm{Aut}_{L[G]}(V \otimes_k L)$ such that $p'_g = a^{-1} p_g g(a)$, $g \in G'$. Then $\sim$ is an equivalence relation on the set of cocycles and the corresponding quotient set, denoted $H^1(G', \mathrm{Aut}_{L[G]}(V \otimes_k L))$, is called the first cohomology set of G' in $\mathrm{Aut}_{L[G]}(V \otimes_k L)$. By making p correspond to $V' \otimes_k L$ we get a canonical map from E_V to $H^1(G', \mathrm{Aut}_{L[G]}(V \otimes_k L))$. Since $(V \otimes_k L)^{G'} = V$ it follows that this map is injective. However, by Hilbert's theorem 90 (see e.g. Exercise 2 on p. 160 in [11]), the cohomology set $H^1(G', \mathrm{Aut}_{L[G]}(V \otimes_k L))$ is trivial. Therefore K and $k[S^{-1}]$ are isomorphic $k[G]$-modules and we can end the second proof in the same way as in the first proof.

A Galois correspondence. Let $\mathbf{F}$ denote the set of fields between K and k and let $\mathbf{G}$ denote the set of subgroups of $G := \mathrm{Aut}_k(K)$. Define functions $\alpha : \mathbf{G} \to \mathbf{F}$ and $\beta : \mathbf{F} \to \mathbf{G}$ by $\alpha(G') = K^{G'}$, $G' \in \mathbf{G}$ and $\beta(K') = \mathrm{Aut}_{K'}(K)$, $K' \in \mathbf{F}$. Also, let β' denote the restriction of β to $\mathbf{F}' := \{K' \in \mathbf{F} \mid K' \supseteq K^G\}$.

Theorem 3. *With the above notations, α and β are inclusion reversing maps satisfying $\beta\alpha = \mathrm{id}_{\mathbf{G}}$ and $\alpha\beta(K') \supseteq K'$, $K' \in \mathbf{F}$, with equality if and only if $K' \in \mathbf{F}'$. In particular, $\beta'\alpha = \mathrm{id}_{\mathbf{G}}$ and $\alpha\beta' = \mathrm{id}_{\mathbf{F}'}$.*

Proof. First we show that $\beta\alpha = \mathrm{id}_{\mathbf{G}}$. Take $G' \in \mathbf{G}$. It is clear that $H := \beta\alpha(G') = \mathrm{Aut}_{K^{G'}}(K) \supseteq G'$. To show the reversed inclusion we first note that, by Theorem 1, the elements in $K^{G'}$ correspond to elements $x = (\sum_{g\in G} k_{g,i} g)_{i=1}^{[K^G:k]}$ in $k[G]^{\oplus[K^G:k]}$ satisfying $g'x = x$, $g' \in G'$. This is equivalent to the conditions $k_{g'g,i} = k_{g,i}$, $g' \in G'$, $g \in G$, $1 \le i \le [K^G : k]$. In particular, this implies that $y := (\sum_{g'\in G'} g')_{i=1}^{[K^G:k]}$ belongs to $\left(k[G]^{\oplus[K^G:k]}\right)^{G'}$. Therefore $hy = y$, $h \in H$, which implies that $H \subseteq G'$.

For the second part of the proof take $K' \in \mathbf{F}$. The inclusion $K'' := \alpha\beta(K') = K^{\mathrm{Aut}_{K'}(K)} \supseteq K'$ is obvious. If equality holds, then $K' \supseteq K^G$. On the other hand, suppose that $K' \supseteq K^G$. Then K/K' is Galois, which, by (F1) and (F2), implies that $[K : K''] = |\mathrm{Aut}_{K'}(K)| = [K : K']$. Therefore $[K'' : K'] = 1$ and hence $K'' = K'$. The last part is clear. □

3. The trace form

The trace form q_K on K induces in a natural way an L-bilinear G-form q_L on $K \otimes_k L$. Also, define a G-form r on $L[S^{-1}]$ by the relation $r(s_1^{-1}, s_1^{-1}) = 1$ and $r(s_1^{-1}, s_2^{-1}) = 0$ if $s_1 \neq s_2$ for all $s_1, s_2 \in S$.

Lemma 3. *The G-forms $(K \otimes_k L, q_L)$ and $(L[S^{-1}], r)$ are isomorphic.*

Proof. Define $\varphi : K \otimes_k L \to L[S^{-1}]$ as in the proof of Lemma 2. All we need to show is that φ respects the bilinear forms. Take $a, a' \in K$ and $b, b' \in L$. Then $q_L(a \otimes b, a' \otimes b') = q_K(a, a')bb' = \mathrm{tr}_{K/k}(aa')bb' = \sum_{s\in S} s(aa')bb' = \sum_{s\in S} s(a)s(a')bb' = \sum_{s_1,s_2\in S} s_1(a)bs_2(a')b'r(s_1^{-1}, s_2^{-1}) = r(\sum_{s_1\in S} s_1(a)bs_1^{-1}, \sum_{s_2\in S} s_2(a')b's_2^{-1}) = r(\varphi(a\otimes b), \varphi(a'\otimes b'))$. □

Remark 1. Lemma 2 and Lemma 3 (and their proofs) are generalizations from Galois extensions to the case of separable extensions of isomorphisms established by Conner and Perlis in [5].

From now on assume that all fields are of characteristic different from two. To prove Theorem 2, we need the following result.

Theorem 4. ([3]) *If two G-forms become isomorphic over an extension of odd degree, then they are isomorphic.*

Suppose that K/k has a normal closure L/k of odd degree. By Lemma 3 and Theorem 4, the G-forms (K, q_K) and $(k[S^{-1}], r)$ are isomorphic. With the same argument as in the first proof of Theorem 1 it is clear that $(k[S^{-1}], r)$ is isomorphic to the direct sum of $[K^G : k]$ copies of the unit G-form $(k[G], q_0)$. This ends the proof of Theorem 2.

Remark 2. If we let G be the trivial group, then Theorem 2 implies the existence of a self-dual basis for all finite separable field extensions K/k with the property that L/k is of odd degree. This generalizes a result by Conner and Perlis (see (I.6.5) in [5] and Proposition 5.1 in [3]).

References

[1] E. Bayer-Fluckiger, Self-dual normal bases, Indag. Math., 51 (1989), 379-383.

[2] D. Bagio, I. Dias and A. Paques, On self-dual normal bases, Indag. Math., 17(1) (2006), 1-11.

[3] E. Bayer-Fluckiger and H. W. Lenstra, Jr., Forms in odd degree extensions and self-dual normal bases, Amer. J. Math., 112 (1990), 359-373.

[4] E. Bayer-Fluckiger and J-P. Serre, Torsions quadratiques et bases normales autoduales, Amer. J. Math., 116 (1994), 1-64.

[5] P. Conner and R. Perlis, *A survey of trace forms of algebraic number fields*, World Scientific, Singapore, 1984.

[6] M. Deuring, Galoissche Theorie und Darstellungsteorie, Math. Ann., 107 (1933), 140-144.

[7] D. S. Kang, Nonexistence of Self-Dual Normal Bases, Comm. Algebra, 32 (2004), 125-132.

[8] S. Lang, *Algebra*, Springer, 2005.

[9] M. Mazur, Remarks on normal bases, Colloq. Math., 87 (2001), 79-84.

[10] E. Noether, Normalbasis bei Körpern ohne höhere Verzweigung, J. Reine Angew. Math., 167 (1932), 147-152.

[11] J-P. Serre, *Corps Locaux*, Hermann, Paris, 1968.

Patrik Lundström
University West
Department of Technology, Mathematics and Computer Science
Gärdhemsvägen 4, Box 957, 461 29 Trollhättan, Sweden
E-mail: patrik.lundstrom@hv.se