BL-bases and unitary groups in characteristic 2

Jean-Pierre Serre

In what follows, K is a commutative field of characteristic 2.

1. A criterion for the existence of a BL-basis

Let L/K be a finite Galois extension, with Galois group G. A basis (e_i) of the K-vector space L is called a *self-dual normal basis* (BL-*basis*, for short) if it has the following two properties (cf. [1], [2], [3]) :

a) $\mathrm{Tr}_{L/K}(e_i.e_j) = \delta^i_j$;

b) G acts transitively on the (e_i).

Note that b) means that (e_i) is a "normal basis" of L/K, while a) says that it is orthonormal with respect to the nondegenerate bilinear form $\mathrm{Tr}_{L/K}(x.y)$.

One finds in [1] and [2] several cases where BL-bases can be proved to exist (or not to exist) :

Existence : when G is of odd order, or when G is abelian and does not contain any element of order 4.

Non-existence : when G has a quotient which is cyclic of order 4.

These results are special cases of :

Theorem 1 - *A BL-basis exists if and only if G is generated by squares and by elements of order 2.*

Note that this criterion does not depend on K, nor of the chosen extension L/K. It only depends on the structure of G. This is quite different from what happens in characteristic $\neq 2$, cf. e.g. [3].

Examples. A BL-basis exists if G is a dihedral group or a simple group; it does not exist if G is a quaternion group.

2. Proof of theorem 1

First, we may assume that K is *perfect*. Indeed, a BL-*basis* for L/K exists if and only if there exists one for the extension $L.K'/K'$, where K' is the perfect closure of K.

Consider now the group algebra $K[G]$, with its usual involution $g \mapsto g* = g^{-1}$. Let U_G^{sch}

be its scheme-theoretic unitary group, which is an algebraic group over K. The group scheme U_G^{sch} is not reduced; call U_G the corresponding reduced scheme; it is a smooth algebraic group over K. We have a natural embedding $G \to U_G^{sch}(K) = U_G(K)$.

Let now $\overline{K}$ be an algebraic closure of K, and put $\Gamma_K = \mathrm{Gal}(\overline{K}/K)$. The given extension L/K corrresponds to a surjective homomorphism $\varphi_L : \Gamma_K \to G$. By composing φ_L with the embedding $G \to U_G(K)$, one may view φ_L as a 1-cocycle of Γ_K with values in $U_G(\overline{K})$. Let $z_L \in H^1(K, U_G)$ be the cohomology class of this cocycle.

Proposition 1 - *We have $z_L = 0$ if and only if L/K has a BL-basis.*

This is explained in [3], § 1.5 when the characteristic of K is $\neq 2$; the case of characteristic 2 is similar. (Loosely speaking, the BL-bases are the K-points of a U_G-torsor which corresponds to z_L.)

Put now :

U_G^o = connected component of U_G ;

G^o = subgroup of G generated by the elements of order 2 and by the squares g^2, where g runs through G.

Proposition 2 - (a) $G^o = G \cap U_G^o$.
(b) *U_G/U_G^o is a finite commutative group of type* (2, ... ,2).

Both (b) and the inclusion $G^o \subset G \cap U_G^o$ are fairly easy. The inclusion $G \cap U_G^o \subset G^o$ requires more work.

Proposition 3 - $H^1(K, U_G^o) = 0$.

This is a special case of a general result on unitary groups, cf. §3, th.2.

Let us now prove half of theorem 1, namely that a BL-basis exists if $G = G^o$. Indeed, in that case, by prop.2, we may view $\varphi_L : \Gamma_K \to G$ as a 1-cocycle with values in $U_G^o(\overline{K})$; let $z_L^o \in H^1(K, U_G^o)$ be the class of this cocycle. The image of z_L^o in $H^1(K, U_G)$ is z_L. By prop.3, we have $z_L^o = 0$, hence $z_L = 0$ and prop.1 shows that L/K has a BL-basis.

It remains to show that, if $G \neq G^o$, there is no BL-basis. To do so, one first remarks that the assumption $G \neq G^o$ is equivalent to the existence of a surjective quadratic character e: $G \to \{\pm 1\}$ with the property that $e(s) = 1$ for every $s \in G$ with $s^2 = 1$. Choose such an e, and assume there exists an element x of L whose G-orbit is a BL-basis. Put :

$$x_0 = \sum_{e(g)=1} g.x \qquad \text{and} \qquad x_1 = \sum_{e(g)=-1} g.x.$$

An explicit computation, similar to the one made in [2], proof of prop.6.1 b), shows that $x_0.x_1 = 0$. Since L is a field, we have either $x_0 = 0$ or $x_1 = 0$, which contradicts the assumption that the $g.x$ are linearly independent.

3. Unitary groups

We continue to assume that K is perfect of characteristic 2.
Let R be a finite-dimensional K-algebra with involution, and let U_R be the corresponding reduced unitary group. Let U_R^o be the connected component of U_R.

Theorem 2 - $H^1(K, U_R^o) = 0$.

Let S be the quotient of U_R^o by its unipotent radical; the algebraic group S is a reductive group over K (it is the largest reductive quotient of U_R^o), and the natural map $H^1(K, U_R^o) \to H^1(K, S)$ is a bijection. Hence proving theorem 2 amounts to proving that $H^1(K, S) = 0$. To do so, we need to describe the structure of S. The result is :

Theorem 3 - *Up to a purely inseparable isogeny, S is a product of classical groups of the following three types:*
(i) *Multiplicative group of a central simple algebra over a finite extension of K.*
(ii) *Unitary group of a central simple algebra with involution* (of first or second kind) *over a finite extension of K.*
(iii) *Special orthogonal group of a nondegenerate quadratic form of even rank > 2 over a finite extension of K.*

This is proved by choosing a maximal torus of U_R^o and looking at the weights of its action on R (by left multiplication), and at the root system of S. Most of the proof can be done under the assumption that K is algebraically closed: the descent from $\overline{K}$ to K is easy.

Once theorem 3 is proved, theorem 2 follows by standard methods in Galois cohomology, based essentially on the fact that $\mathrm{cd}_2(\Gamma_K) \leqslant 1$, and on the following auxiliary result:

Proposition 4 - *Let A be a connected linear algebraic group over K, and let K_1 be a quadratic extension of K. The natural map $H^1(K, A) \to H^1(K_1, A)$ is injective.*
(See e.g. [4], Chap. III, § 2.3, exerc.2 (b).)

Here are a few more properties of the unitary group U_R:

Theorem 4 - (i) *The finite group U_R/U_R^o is commutative of type* (2, ...,2).
(ii) *The map $H^1(K, U_R) \to H^1(K, U_R/U_R^o)$ is injective.*
(iii) *Every commutative smooth subgroup of U_R of multiplicative type is contained in a maximal torus.*
(iv) *If K' is an odd degree extension of K, the map $H^1(K, U_R) \to H^1(K', U_R)$ is injective.*

Properties (i) and (iii) are easy; (ii) follows from (i) and from th.2; (iv) follows from (ii). (It would be interesting to have an *a priori* proof of (iv).)

References

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

[2] 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.

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

[4] J.-P. Serre, *Cohomologie Galoisienne*, cinquième édition, révisée et complétée, LNM **5**, Springer-Verlag, 1994; English translation, SMM Springer-Verlag, 1997.