Доклади на Българската академия на науките
Comptes rendus de l'Académie bulgare des Sciences

Tome 62, No 9, 2009

MATHEMATIQUES
Algèbre

EXACT SEQUENCES IN THE THEORY OF ORTHOGONAL REPRESENTATIONS OF GROUPS

Ivo M. Michailov

(*Submitted by Academician S. Dodunekov on May 26, 2009*)

Abstract

We construct new exact sequences associated to the Pin groups in the theory of orthogonal representations of Galois groups, presented by Fröhlich in [1]. We show some applications to Galois embedding problems related to these exact sequences.

Key words: embedding problem, Galois extension, orthogonal representation, Clifford group
2000 Mathematics Subject Classification: 12F12, 12G20

Let G be a finite group, and let $\{\sigma_1, \ldots, \sigma_k\}$ be a fixed (not necessarily minimal) generating set of G with these properties: $|\sigma_1| = p^{n-1}$ for $n > 1$, the subgroup H generated by $\sigma_2, \ldots, \sigma_k$ is normal in G, and the quotient group G/H is isomorphic to the cyclic group $C_{p^{n-1}}$, i.e., $\sigma_1^i \notin H, 1 \leq i < p^{n-1}$. Take now two arbitrary group extensions

This work is partially supported by project No. RD-05-287/11.03.2009 of Shumen University, Bulgaria.

$$1 \to \mu_p \to G_1 \xrightarrow{\varphi} G \to 1 \tag{0.1}$$

and

$$1 \to \mu_p \to G_2 \xrightarrow{\psi} G \to 1. \tag{0.2}$$

Denote by $\tilde{\sigma}_i = \varphi^{-1}(\sigma_i)$ any preimage of σ_i in G_1 and by $\bar{\sigma}_i = \psi^{-1}(\sigma_i)$ any preimage of σ_i in G_2, $i = 1, \dots k$.

Definition. *We write $G_2 = G_1^{(p^n \to p^{n-1})}$ and say that G_2 can be constructed from G_1 via a $(C_{p^n} \to C_{p^{n-1}})$-modification (regarding σ_1), if*

(1) $|\tilde{\sigma}_1| = p^{n-1}$;

(2) $\bar{\sigma}_1^{p^{n-1}} \in \mu_p, \bar{\sigma}_1^{p^{n-1}} \neq 1$;

(3) *all other relations between the generators of the groups G_1 and G_2 are identical, i.e., $\tilde{\sigma}_i^{\alpha_i} = \zeta^l \prod_{j \neq 1} \tilde{\sigma}_j^{\beta_j} \iff \bar{\sigma}_i^{\alpha_i} = \zeta^l \prod_{j \neq 1} \bar{\sigma}_j^{\beta_j}$ for $i = 2, 3, \dots, k$; $l, \alpha_i, \beta_j \in \mathbb{Z}$; and $[\tilde{\sigma}_i, \tilde{\sigma}_j] = \zeta^l \prod_{s \neq 1} \tilde{\sigma}_s^{\varepsilon_s} \iff [\bar{\sigma}_i, \bar{\sigma}_j] = \zeta^l \prod_{s \neq 1} \bar{\sigma}_s^{\varepsilon_s}$ for $i, j = 1, 2, \dots, k; l, \varepsilon_s \in \mathbb{Z}$.*

We continue with some preliminaries about Clifford algebras taken largely from [3]. Let (V, q) be a quadratic space with $\dim(V) = n$ over F and let $C(q)$ be the Clifford algebra of q, generated by an orthogonal basis $e_1, e_2, \dots, e_n$ of V with multiplication rules $e_i^2 = q(e_i)$ for $i = 1, \dots, n$ and $e_i e_j = -e_j e_i$ for $i \neq j$. Further notations: $C_0(q)$ is the even Clifford algebra; $C(q) = C_0(q) \oplus C_1(q)$; if $x \in C_i(q)$, we write $\partial x = i$; $C^\times(q)$ is the Clifford group defined as the subgroup of $C(q)^\times$, consisting of those invertible elements x, for which $xVx^{-1} = V$. The anisotropic vectors of V are in $C^\times(q)$ and $vuv^{-1} = -T_v(u)$ for $u, v \in V$, where v is anisotropic and T_v is the reflection on the hyperplane $v^\perp$.

This enables us to define a map $r : C^\times(q) \to O(q)$ by $r_x : u \mapsto (-1)^{\partial x} xux^{-1}$. Since $r_v = T_v$ and every isometry is a product of reflections, r is surjective. Thus we obtain the exact sequence

$$1 \to F^\times \to C^\times(q) \xrightarrow{r} O(q) \to 1.$$

Denote by ι the principal involution on $C(q)$, which preserves the scalars, sums and vectors, and reverses products. Denote by $N : C^\times(q) \to F^\times$ the norm given by $N(x) = x\iota(x)$ and by $sp : O(q) \to F^\times/2$ the spinor norm given by $sp(T_v) = \overline{q(v)}$. Finally, put $\mathrm{Pin}(q) = \ker(N)$ and $\mathrm{Spin}(q) = \mathrm{Pin}(q) \cap C_0^\times(q)$. Whence, we have the long exact sequences

$$1 \to \mu_2 \to \mathrm{Pin}(q) \xrightarrow{\ r\ } O(q) \xrightarrow{\ sp\ } F^{\times}/2$$

and

$$1 \to \mu_2 \to \mathrm{Spin}(q) \xrightarrow{\ r\ } SO(q) \xrightarrow{\ sp\ } F^{\times}/2.$$

If we take the separable closure $\bar{F}_{\mathrm{sep}}$ of F, we get the short exact sequences

$$1 \to \mu_2 \to \mathrm{Pin}(\bar{q}) \xrightarrow{\ r\ } O(\bar{q}) \to 1 \tag{0.3}$$

and

$$1 \to \mu_2 \to \mathrm{Spin}(\bar{q}) \xrightarrow{\ r\ } SO(\bar{q}) \to 1. \tag{0.4}$$

We will assume henceforth that $n = \dim(V)$ is even. We will construct some new exact sequences in this case.

Define a map $s : C^{\times}(q) \to O(q)$ by $s_x : u \mapsto xux^{-1}$. Clearly, s_x is an isometry, $s_v = -T_v$ and s is a homomorphism. Set $\epsilon = e_1 e_2 \cdots e_n$ and $d = disc(q)$ from now on.

Notice that $s(\epsilon) = (-T_{e_1})(-T_{e_2}) \cdots (-T_{e_n}) = T_{e_1} T_{e_2} \cdots T_{e_n} = -I \in SO(q)$, where I is the identity of $O(q)$. Therefore, $s(\epsilon v) = T_v$, whence s is surjective. It is known that $C(q)$ is a c.s. algebra over F, so we get another exact sequence

$$1 \to F^{\times} \to C^{\times}(q) \xrightarrow{\ s\ } O(q) \to 1.$$

Define now a map $sp_d : O(q) \to F^{\times}/2$ by $sp_d(T_v) = \overline{dq(v)}$. Since the spinor norm sp is well defined, so is sp_d. Thus we obtain the long exact sequences

$$1 \to \mu_2 \to \mathrm{Pin}(q) \xrightarrow{\ s\ } O(q) \xrightarrow{\ sp_d\ } F^{\times}/2$$

and

$$1 \to \mu_2 \to \mathrm{Spin}(q) \xrightarrow{\ s\ } SO(q) \xrightarrow{\ sp_d\ } F^{\times}/2.$$

Indeed, if $sp_d(T_v) = \bar{1}$, then $\epsilon v/\sqrt{dq(v)} \in \mathrm{Pin}(q)$ and $s(\epsilon v/\sqrt{dq(v)}) = T_v$.

If we take again the separable closure $\bar{F}_{\mathrm{sep}}$ of F, we get the short exact sequences

$$1 \to \mu_2 \to \mathrm{Pin}(\bar{q}) \xrightarrow{\ s\ } O(\bar{q}) \to 1 \tag{0.5}$$

and

$$1 \to \mu_2 \to \mathrm{Spin}(\bar{q}) \xrightarrow{\ s\ } SO(\bar{q}) \to 1. \tag{0.6}$$

Next, let G be a finite group with a faithful orthogonal representation $G \hookrightarrow O(q)$. We are going to compare the group extensions

$$1 \to \mu_2 \to \widetilde{G}^+ \xrightarrow{\ r\ } G \to 1 \tag{0.7}$$

and

$$1 \to \mu_2 \to \widetilde{G}^- \xrightarrow{\ s\ } G \to 1, \tag{0.8}$$

which are obtained by taking the restrictions of the exact sequences (0.3) and (0.5), respectively. Set $G_1 = G \cap SO(q)$. Since each element from G_1 is a product of even number of reflections, the restricted group extensions

$$1 \to \mu_2 \to \widetilde{G}_1^+ \xrightarrow{\ r\ } G_1 \to 1$$

and

$$1 \to \mu_2 \to \widetilde{G}_1^- \xrightarrow{\ s\ } G_1 \to 1$$

are equivalent. We are going to answer the question when the group extensions (0.7) and (0.8) are equivalent and when they are not. Notice that $(G : G_1) \leq 2$. Since the case $(G : G_1) = 1$ is trivial, we will assume that $(G : G_1) = 2$. There are two cases which we need to consider separately.

I. $g^2 \neq 1$ for all $g \in G \setminus G_1$.

Choose arbitrary $g \in G \setminus G_1$ and set $\sigma = g^2 \in G_1$. Now, take a pre-image $\widetilde{g}_+ \in \widetilde{G}^+$ of g. Then $\widetilde{g}_- = (\epsilon/\sqrt{d})\widetilde{g}_+$ is a pre-image of g in $\widetilde{G}^-$.

If we assume that the order of σ is odd, i.e., $|\sigma| = 2k+1$, then $g^{2k+1} \notin G_1$ and $(g^{2k+1})^2 = \sigma^{2k+1} = 1$, which is a contradiction. Therefore, $|\sigma|$ is even. Let $\widetilde{\sigma}_+$ and $\widetilde{\sigma}_-$ be the pre-images of σ in $\widetilde{G}^+$ and $\widetilde{G}^-$, respectively. Then we have $\widetilde{\sigma}_+ = \pm\widetilde{\sigma}_-$, which implies $\widetilde{\sigma}_+^2 = \widetilde{\sigma}_-^2$, so $\widetilde{g}_+$ and $\widetilde{g}_-$ have one and the same order.

Finally, notice that ϵ is in the centre of $C_0(q)$, so the relations between $\widetilde{g}_+$ and the generators of $\widetilde{G}_1^+$ are identical to those between $\widetilde{g}_-$ and the generators of $\widetilde{G}_1^-$. Therefore, the group extensions (0.7) and (0.8) are equivalent in this case.

II. There exists $g \in G \setminus G_1$ such that $g^2 = 1$.

For simplicity, we may assume that g is a reflection: $g = T_v$ for some anisotropic v. Then $\widetilde{g}_+ = v/\sqrt{q(v)} \in \widetilde{G}^+$ and $\widetilde{g}_- = (\epsilon/\sqrt{d})(v/\sqrt{q(v)}) \in \widetilde{G}^-$ are pre-images of g. We have $\widetilde{g}_+^2 = 1$ and $\widetilde{g}_-^2 = (-1)^{n/2+1}$. Therefore, if $n \equiv 2 \pmod 4$, the group extensions (0.7) and (0.8) are equivalent. If $n \equiv 0 \pmod 4$ then $\widetilde{g}_-^2 = -1$, so $\widetilde{G}^- = \widetilde{G}^{+(4\to 2)}$.

There are some other interesting applications of the group modifications defined in this paper. For instance, in [4] we will prove the following:

Theorem 0.1. ([4], Prop. 3.7) *Let G and $H \leq G$ be as at the beginning of our paper for $p = 2$. Let $\varphi : G/H \to \bar{F}^{\times}_{\mathrm{sep}}$ be the homomorphism induced by the isomorphism $G/H \cong \langle \zeta_{2^{n-1}} \rangle$ and the inclusion $\langle \zeta_{2^{n-1}} \rangle \hookrightarrow \bar{F}^{\times}_{\mathrm{sep}}$, where $\zeta_{2^{n-1}}$ is a primitive 2^{n-1}th root of unity. Assume that an orthogonal representation $G \hookrightarrow O(q)$ is given, and takes the restriction $1 \to \mu_2 \to \widetilde{G} \to G \to 1$ of $1 \to \mu_2 \to \mathrm{Pin}(\bar{q}) \to O(\bar{q}) \to 1$. Then there exists a subgroup $\bar{G}$ of $C^{\times}(\bar{q})$, such that*

(i) *The diagram*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu_2 & \longrightarrow & \bar{G} & \xrightarrow{r'} & G & \longrightarrow & 1 \\ & & \big\downarrow N & & \big\downarrow N & & \big\downarrow \varphi & & \\ 1 & \longrightarrow & 1 & \longrightarrow & \bar{F}^{\times}_{\mathrm{sep}} & = & \bar{F}^{\times}_{\mathrm{sep}} & \longrightarrow & 1 \end{array}$$

is commutative with exact rows, where N is the norm and r' is the restriction of $r : C^{\times}(\bar{q}) \to O(\bar{q})$ on $\bar{G}$;

(ii) *Either $\bar{G} = \widetilde{G}^{(2^n \to 2^{n-1})}$, or $\widetilde{G} = \bar{G}^{(2^n \to 2^{n-1})}$.*

The exact sequences under discussion can be used for the purposes of Galois embedding problems. All of the necessary definitions and generalities the reader can find in [2,4]. We will prove in [4] the following theorem, giving the relation between the obstructions to solvability of the embedding problems related to the groups which are connected with the described modifications.

Theorem 0.2. ([4], Theorem 3.4) *Let L/F be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/F)$ as described above, let $K = L^H$ be the fixed subfield of H, and let the groups G_1 and G_2 from* (0.1) *and* (0.2) *be such that $G_2 = G_1^{(p^n \to p^{n-1})}$. Denote by $O_{G_1} \in \mathrm{Br}_p(F)$ – the obstruction of the embedding problem $(L/F, G_1, \mu_p)$, by $O_{G_2} \in \mathrm{Br}_p(F)$ – the obstruction of the embedding problem $(L/F, G_2, \mu_p)$, and by $O_{C_{p^n}} \in \mathrm{Br}_p(F)$ – the obstruction of the embedding problem $(K/F, C_{p^n}, \mu_p)$ given by the group extension $1 \to \mu_p \to C_{p^n} \to G/H \cong C_{p^{n-1}} \to 1$. Then the relation between these obstructions is given by*

$$O_{G_2} = O_{G_1} O_{C_{p^n}} \in \mathrm{Br}_p(F).$$

REFERENCES

[1] Fröhlich A. J. Reine Angew. Math., **360**, 1985, 84–123.

[2] Ishanov V. V., B. B. Lur'e, D. K. Faddeev. The Embedding Problem in Galois Theory, Amer. Math. Soc., Providence, 1997.

[3] Ledet A. Brauer Type Embedding Problems, Fields Institute Monographs **21**, American Mathematical Society, 2005.
[4] Michailov I. On Galois cohomology and realizability of 2-groups as Galois groups (preprint).

Faculty of Mathematics and Informatics
Constantin Preslavski University
9712 Shumen, Bulgaria
e-mail: ivo_michailov@yahoo.com