Group codes of dimension 2 and 3 are abelian

Cristina García Pillado, Santos González, Victor Markov,
Olga Markova and Consuelo Martínez

Abstract

Let F be a finite field and let G be a finite group. We show that if $\mathcal{C}$ is a G-code over F with $\dim_F(\mathcal{C}) \leq 3$ then $\mathcal{C}$ is an abelian group code. Since there exist non-abelian group codes of dimension 4 when $\operatorname{char} F > 2$ (see the examples in [1]), we conclude that the smallest dimension of a non-abelian group code over a finite field is 4.

Introduction

All groups and fields considered in this paper are supposed to be finite. Let F be a field and let G be a group. Following [2] we say that a linear code $\mathcal{C}$ over F is a (left) G-code if its length is equal to $n = |G|$ and there exists a one-to-one mapping $\nu : \{1, \ldots, n\} \to G$ such that

$$\left\{ \sum_{i=1}^{n} a_i \nu(i) : (a_1, \ldots, a_n) \in \mathcal{C} \right\}$$

is a (left) ideal in FG. We will also say that this (left) ideal is *permutation equivalent* to the code $\mathcal{C}$.

A code $\mathcal{C}$ is called an (*abelian*) *group code* if there exists an (abelian) group G such that $\mathcal{C}$ is a G-code.

It was shown in [2] that any one-dimensional group code over a field F is an abelian group code (moreover it is a C-code for a cyclic group C). It seems natural to ask about the lowest dimension of a non-abelian group code.

Since examples of non-abelian group codes of dimension 4 are known [1], a full answer to the above question is given in the main result of this paper.

Theorem 1. *Let $\mathcal{C}$ be a G-code over a finite field F for a finite group G. If $\dim_F(\mathcal{C}) \leq 3$ then $\mathcal{C}$ is an abelian group code.*

The paper is organized as follows. In section 1 we introduce some necessary notation and some auxiliary results are proved. In section 2 we prove Theorem 1.

1 Preliminaries

Let F be a field. We denote its multiplicative group by F^*. Let $M_{n,k}(F)$ be the vector space of $n \times k$ matrices over F, and let $M_n(F)$ be the algebra of all $n \times n$-matrices over F for any integers $n, k \geq 1$. We will use the notation $\mathrm{GL}_n(F)$, $\mathrm{D}_n(F)$, $\mathrm{T}_n(F)$ and $\mathrm{UT}_n(F)$ respectively for the group of all invertible $n \times n$-matrices, all invertible diagonal $n \times n$-matrices, the group of all invertible upper triangular $n \times n$-matrices and the group of all upper unitriangular $n \times n$-matrices, i.e. upper triangular matrices with diagonal elements equal to 1, over the field F.

Let us write $A \leq B$ to express that A is a subgroup of the group B, while $A \lhd B$ means that A is a normal subgroup in B. $Z(G)$ and $Z(R)$ will denote the centers of the group G and of the ring R, respectively. We denote, for short, the set $\{m, m+1, \ldots, n\}$ by $\overline{m, n}$ for any integers $m \leq n$.

We recall the best known sufficient condition for all G-codes to be abelian.

Theorem 1.1 ([2, theorem 3.1])**.** *Let G be a finite group. Assume that G has two abelian subgroups A and B such that every element of G can be written as ab with $a \in A$ and $b \in B$. Then every G-code is an abelian group code.*

We say that a group G *has an abelian decomposition* $G = AB$ if it satisfies the condition of this theorem.

For any finite group G and any subgroup $N \leq G$ we consider the element $N_\Sigma = \sum_{u \in N} u \in FG$. We will use the following properties of N_Σ: $N_\Sigma = uN_\Sigma = N_\Sigma u$ for every $u \in N$, and $N_\Sigma \in Z(FG)$ if and only if $N \lhd G$.

For two finite groups G, H of the same order n and for any one-to-one mapping $\varphi : G \to H$ we define its natural extension $\tilde{\varphi} : FG \to FH$ by the rule

$$\tilde{\varphi}\left(\sum_{g \in G} a_g g\right) = \sum_{g \in G} a_g \varphi(g).$$

If I, J are left (right, two-sided) ideals in the group rings FG and FH, respectively, and there exists a one-to-one mapping $\varphi : G \to H$ such that $\tilde{\varphi}(I) = J$, we say that I and J are *permutation equivalent.*

We say that a subgroup $U \leq G$ acts trivially (from the left) on some set $X \subseteq FG$ if $ux = x$ for every $u \in U$ and $x \in X$. Our proofs are based on Theorem 1.1 and on the following observation.

Lemma 1.2. *Let F be a field and let G, H be two groups of the same order $n < \infty$. Suppose that there exist two normal subgroups $N \lhd G$ and $K \lhd H$ such that $G/N \cong H/K$. If N acts trivially on some (left, right, two-sided) ideal $I \in FG$, then I is permutation equivalent to some (left, right, two-sided) ideal of the ring FH.*

Proof. Let $s = |G/N|$ and denote by $g_1, \ldots, g_s$ a complete set of representatives of G modulo N, thus $G/N = \{g_1N, \ldots, g_sN\}$ and $G = \bigcup_{i=1}^{s} g_iN$. Fixing the isomorphism $f : G/N \to H/K$ we can choose a representative system $\{h_i\}$ of the group H modulo K such that $f(g_iN) = h_iK$, $i \in \overline{1,s}$. For each pair of numbers $i, j \in \overline{1,s}$ let $k(i,j)$ be defined by the equality $g_iNg_jN = g_{k(i,j)}N$. Then we have $g_ig_j = g_{k(i,j)}u_{ij}$ for some $u_{ij} \in N$ and also $h_ih_j = h_{k(i,j)}v_{ij}$ for some $v_{ij} \in K$. Since $|N| = |K| = n/s$ we can fix a one-to-one mapping $\tau : N \to K$. Define $\varphi : G \to H$ as follows: for an arbitrary $x \in G$, x belongs exactly to one class, $x \in g_iN$, of G modulo N. Set $\varphi(x) = h_i\tau(g_i^{-1}x)$. Clearly φ is a well defined one-to-one map.

Suppose now that N acts trivially on an element $x \in FG$. If $x = \sum_{g\in G} a_gg$ then we obtain, comparing coefficients in x and $u^{-1}x$, for $u \in N$, that $a_g = a_{ug}$ for every $g \in G$, so every element $x \in I$ can be presented in the form $x = \sum_{i=1}^{s} b_ig_iN_\Sigma$ where $b_1, \ldots, b_s \in F$. Note that $\tilde{\varphi}(N_\Sigma) = K_\Sigma \in Z(FH)$ and $\tilde{\varphi}(g_iN_\Sigma) = h_iK_\Sigma$. Since the mapping $\tilde{\varphi}$ is evidently F-linear, it is sufficient to prove that if $x \in I$ then $h\tilde{\varphi}(x) \in \tilde{\varphi}(I)$ and $\tilde{\varphi}(x)h \in \tilde{\varphi}(I)$ for any $h \in H$. As we have seen, we can write $x = \sum_{i=1}^{s} b_ig_iN_\Sigma$, where $b_1, \ldots, b_s \in F$, so $\tilde{\varphi}(x) = \sum_{i=1}^{s} b_ih_iK_\Sigma$. If $h \in h_jK$ for (a unique) $j \in \overline{1,s}$, then $h = h_jv$ for some $v \in K$, so

$$\begin{aligned}
h\tilde{\varphi}(x) &= h_jv(\textstyle\sum_{i=1}^{s} b_ih_iK_\Sigma) = h_jvK_\Sigma(\sum_{i=1}^{s} b_ih_i) = (\sum_{i=1}^{s} b_ih_jh_i)K_\Sigma \\
&= \textstyle\sum_{i=1}^{s} b_ih_k(j,i)v_{ji}K_\Sigma = \sum_{i=1}^{s} b_ih_{k(j,i)}K_\Sigma \\
&= \tilde{\varphi}(\textstyle\sum_{i=1}^{s} b_ig_{k(j,i)}N_\Sigma) = \tilde{\varphi}(\sum_{i=1}^{s} b_ig_jg_iu_{ji}^{-1}N_\Sigma) = \tilde{\varphi}(g_jx) \in \tilde{\varphi}(I).
\end{aligned}$$

A similar calculation shows that $\tilde{\varphi}(x)h = \tilde{\varphi}(xg_j)$ with the same element g_j as above. □

Evidently Lemma 1.2 remains valid is we consider the right action instead of the left action.

We have also the following

Lemma 1.3. *Suppose that a normal subgroup N of a finite group G acts trivially (from the left or from the right) on some ideal I of the group ring FG and that G/N has an abelian decomposition. Then I is permutation equivalent to an ideal of a group ring FA for some abelian group A.*

Proof. Consider the group $H = G/N \times C$ where C is a cyclic group of order $|N|$. By Lemma 1.2 I is permutation equivalent to some ideal $\tilde{I}$ of the group ring FH. However the group H has an abelian decomposition so $\tilde{I}$ is permutation equivalent to some ideal in the group ring of an abelian group. □

Corollary 1.4. *If the derived subgroup G' of a finite group G acts trivially (from the left or from the right) on some ideal I of the group ring FG then I is permutation equivalent to an ideal of the group ring FA for some abelian group A.*

Proof. The statement follows from Lemma 1.2 since the group G/G' is abelian and thus it has an abelian decomposition. □

Now we can deduce one statement of [2] from Lemma 1.2.

Corollary 1.5 ([2, Corollary 2.2])**.** *If $\mathcal{C}$ is a one-dimensional left group code over some field F then it is a H-code for some cyclic group H.*

Proof. Consider a left ideal $Fv \in FG$ corresponding to the code $\mathcal{C}$. Then for any $g \in G$ we have $gv = \lambda(g)v$ with $\lambda(g) \in F^*$, so $\lambda : G \to F^*$ is a group homomorphism. Take $N = \ker \lambda$. Then G/N is isomorphic to the subgroup $\mathrm{im}(\lambda) \le F^*$ which is cyclic as a subgroup of the cyclic group F^* [3, Theorem 5.1.9]. Let H be the cyclic group of order $|G|$. Then H contains a subgroup K with $|K| = |N|$ since $|N|$ divides $|G|$, and Lemma 1.2 gives the required property of $\mathcal{C}$. □

2 Proof of Theorem 1

In this section F denotes a finite field with $\mathrm{char}\, F = p$ and $|F| = q = p^r$. G is a finite group.

2.1 Ideals of dimension 2.

Proposition 2.1. *Let I be an ideal in the ring FG such that $\dim_F I = 2$. Then I is permutation equivalent to some ideal in a commutative group ring over F.*

Proof. Suppose first that I is a simple right FG-module. Then by Schur's lemma ([3, Proposition 17.1.1] or [4, Theorem 1.1.1]) its endomorphism ring is a division ring D which is commutative by Wedderburn's theorem [4, Theorem 3.1.1]. Hence the left multiplication on I defines a homomorphism $G \to D^*$ and the derived subgroup G' is contained in its kernel. This implies that G' acts trivially on I from the left. Corollary 1.4 finishes the proof of the proposition in this case.

Suppose on the contrary that I contains a one-dimensional right ideal I_0. Then there exists a basis v_0, v_1 of the vector space I such that $v_0 \in I_0$. The right multiplication by an element $g \in G$ is a linear operator on I

whose matrix with respect to this basis belongs to $\mathrm{T}_2(F)$. Hence we have a homomorphism $f : G \to \mathrm{T}_2(F)$. Let N be the kernel of f. Then G/N is isomorphic to some subgroup S of the group $\mathrm{T}_2(F)$.

Evidently $\mathrm{T}_2(F) = AB$, where $A = \mathrm{D}_2(F)$ and $B = \mathrm{UT}_2(F)$. Since $|A| = (q-1)^2$ and $|B| = q$, the conditions of the following lemma are satisfied.

Lemma 2.2 ([5, Lemma 3] or [6, Lemma 3.2.9])**.** *If the finite soluble group $G = AB$ is the product of two subgroups A and B with coprime orders, then every subgroup S of G has a conjugate S^g with some $g \in G$ such that $S^g = (S^g \cap A)(S^g \cap B)$.*

Since A and B are abelian, the group S has an abelian decomposition and Lemma 1.2 can be applied with $H = S \times K$ for any abelian group K such that $|K| = |N|$, and the proof in this case is finished using Theorem 1.1. $\square$

Remark 2.3. The proof of [2, Proposition 3.3] shows that there exist non-abelian left group codes of dimension 2.

2.2 Ideals of dimension 3.

Lemma 2.4. *Let R be an F-algebra. Suppose that $I \lhd R$ and $\dim_F(I) = 3$. If M is a two-dimensional simple submodule of I_R then M is a fully characteristic submodule of I_R (i.e. $f(M) \subseteq M$ for any $f \in \mathrm{End}(I_R)$), in particular, $M \lhd R$. If I_R/N is a two-dimensional simple factor-module of I_R for some submodule N then N is a fully characteristic submodule of I_R, in particular, $N \lhd R$.*

Proof. Consider an arbitrary homomorphism $f \in \mathrm{End}(I_R)$. Then either $f(M) = 0$ or $\dim(f(M)) = 2$. In the latter case $M \cap f(M) \neq 0$ thus $M = f(M)$.

Similarly, let $\pi : I_R \to I_R/N$ be a natural epimorphism. Then $\pi f(N)$ is a submodule in I_R/N and $\dim(\pi f(N)) \leq 1$, thus $\pi f(N) = 0$ and $f(N) \subseteq N$. Applying these properties to the homomorphism of left multiplication by any element of r we deduce that $L \lhd R$ and $N \lhd R$ under the specified conditions. $\square$

Consider the left and right action of G on I. We fix two group homomorphisms $\varphi, \psi : G \to \mathrm{GL}(I)$ defined as follows:

$$\forall g \in G,\ v \in I, \varphi(g)(v) = gv,\ \psi(g)(v) = vg^{-1}.$$

Note that for any elements $g, h \in G$ and $v \in I$ the associativity law implies

$$\varphi(g)\psi(h)(v) = \varphi(g)(vh^{-1}) = gvh^{-1} = \psi(h)(gv) = \psi(h)\varphi(g)(v).$$

Hence $ab = ba$ for any $a \in \varphi(G)$ and $b \in \psi(G)$.

Proposition 2.5. *Let I be an ideal in the ring FG such that $\dim_F I = 3$. Then either $\varphi(G)$ or $\psi(G)$ has an abelian decomposition.*

Proof. First suppose that I_R has a two-dimensional simple submodule L or a two-dimensional simple factor-module I_R/N. In the first case take a basis v_1, v_2, v_3 of I such that $v_1 \in L$ and $v_2 \in L$. Then it follows from Lemma 2.4 that for any $g \in G$ the operator $\varphi(g)$ on I_R is defined by a matrix of the form

$$\Lambda = \left(\begin{array}{cc|c} \multicolumn{2}{c|}{\Lambda_0} & \overline{v} \\ \hline 0 & 0 & \alpha \end{array}\right)$$

where $\Lambda_0 \in \mathrm{GL}_2(F)$, $\alpha \in F^*$ and $\overline{v}$ is a column of size 2.

Note that Λ_0 defines an automorphism of L so as in the proof of Proposition 2.1 such matrices belong to some subfield $D \subset M_2(F)$. It follows that the group $\varphi(G)$ is contained in the group

$$H_1 = \left\{ \left(\begin{array}{cc|c} \multicolumn{2}{c|}{d} & \overline{v} \\ \hline 0 & 0 & \alpha \end{array}\right) : d \in D^*,\ \alpha \in F^*,\ \overline{v} \in M_{2,1}(F) \right\}$$

which has a decomposition $H_1 = AB$, where

$$A = \left\{ \left(\begin{array}{cc|c} \multicolumn{2}{c|}{\multirow{2}{*}{d}} & 0 \\ & & 0 \\ \hline 0 & 0 & \alpha \end{array}\right) : d \in D^*,\ \alpha \in F^* \right\},$$

$$B = \left\{ \left(\begin{array}{cc|c} 1 & 0 & \beta_1 \\ 0 & 1 & \beta_2 \\ \hline 0 & 0 & 1 \end{array}\right) : \beta_1, \beta_2 \in F \right\}.$$

Since $\dim_D(M_2(F)) = 4/\dim_F(D)$ must be an integer, $\dim_F(D) \in \{1, 2\}$. Thus the groups A and B are abelian and have orders $(q^i-1)(q-1)$, $1 \le i \le 2$, and q^2 respectively, so $|A|$ and $|B|$ are coprime. By Lemma 2.2 we obtain an abelian decomposition of the group $\varphi(G)$.

Similarly, if there is a one-dimensional two-sided ideal N such that I_R/N is simple then we can take a basis v_1, v_2, v_3 of I such that $v_1 \in N$. Thus the group $\varphi(G)$ is contained in the group

$$H_2 = \left\{ \left(\begin{array}{c|cc} \alpha & \multicolumn{2}{c}{\overline{v}'} \\ \hline 0 & \multicolumn{2}{c}{\multirow{2}{*}{d}} \\ 0 & & \end{array}\right) : d \in D^*,\ \alpha \in F^*,\ \overline{v}' \in M_{1,2}(F) \right\},$$

where again $D = \mathrm{End}(I_R/N)$ so D is a field. But the group H_2 has an abelian decomposition $H_2 = AB$, where now

$$A = \left\{ \left(\begin{array}{c|cc} 1 & \alpha_1 & \alpha_2 \\ \hline 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right) : \alpha_1, \alpha_2 \in F \right\},$$

$$B = \left\{ \left(\begin{array}{c|cc} \alpha & 0 & 0 \\ \hline 0 & \multicolumn{2}{c}{\multirow{2}{*}{d}} \\ 0 & & \end{array} \right) : d \in D^*,\ \alpha \in F^* \right\}.$$

Again the conditions of Lemma 2.2 are satisfied so we again obtain an abelian decomposition of the group $\varphi(G)$.

From now on we assume that I_R does not have two-dimensional simple submodules or factor-modules.

For any right module M its *socle* $\mathrm{Soc}(M)$ is defined as the sum of all simple submodules of M, and the following series of submodules can be constructed (see e.g. [7, §1.9]):

$$0 = M_0 \subseteq M_1 \subseteq \ldots, \text{ where } M_{i+1}/M_i = \mathrm{Soc}(M/M_i),\ i = 0, 1, \ldots \qquad (2.1)$$

This series is transfinite in general but if M is a finite module then $M_t = M$ for some $t \geq 0$.

This series is called *socle series* or *Loewy series* of the module M. The least number t such that $M_t = M$ (if it exists) is called the *socle length* or the *Loewy length* of the module M and will be denoted by $l_s(M)$. It is easy to see by induction that all the submodules belonging to Loewy series are fully characteristic.

Consider the following cases.

Case 1. $l_s(I_R) = 1$.
Then we have two possibilities.

If I_R is simple then the arguments used in the proof of Proposition 2.1 are valid and imply that $\varphi(G)$ is an abelian group.

If $I = I_1 \oplus I_2 \oplus I_3$ where each I_k is one-dimensional, $k = 1, 2, 3$, then evidently $\psi(G) \subseteq F^* \times F^* \times F^*$, so $\psi(G)$ is commutative.

Case 2. $l_s(I_R) = 2$.
Then we again have two possibilities.

If $\dim_F \mathrm{Soc}(I_R) = 1$ then $I_R/\mathrm{Soc}(I_R) = V_1 \oplus V_2$ where V_1 and V_2 are simple right R-modules. Hence there exists a basis v_1, v_2, v_3 of I_R such that $v_k + \mathrm{Soc}(I_R)$ generates V_k over F, $k = 1, 2$. Then any matrix in $\psi(G)$ has the form

$$\begin{pmatrix} \alpha & \beta_1 & \beta_2 \\ 0 & \alpha_1 & 0 \\ 0 & 0 & \alpha_2 \end{pmatrix},$$

where $\alpha, \alpha_1, \alpha_2 \in F^*$, $\beta_1, \beta_2 \in F$. This implies that $\psi(G)$ is contained in the group $\mathrm{D}_3(F)M$, where

$$M = \left\{ \begin{pmatrix} 1 & \beta_1 & \beta_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : \beta_1, \beta_2 \in F \right\},$$

and so again $\psi(G)$ has an abelian decomposition by virtue of Lemma 2.2.

If $\dim_F \mathrm{Soc}(I_R) = 2$ then $\mathrm{Soc}(I_R) = I_1 \oplus I_2$ for some one-dimensional right ideals. Taking a basis v_1, v_2, v_3 such that $v_1 \in I_1$ and $v_2 \in I_2$ we obtain the following matrix for any operator in $\psi(G)$:

$$\begin{pmatrix} \alpha_1 & 0 & \gamma_1 \\ 0 & \alpha_2 & \gamma_2 \\ 0 & 0 & \alpha_3 \end{pmatrix}$$

where $\alpha_1, \alpha_2, \alpha_3 \in F^*$, $\gamma_1, \gamma_2 \in F$. This implies that $\psi(G)$ is contained in the group $M\,\mathrm{D}_3(F)$, where

$$M = \left\{ \begin{pmatrix} 1 & 0 & \gamma_1 \\ 0 & 1 & \gamma_2 \\ 0 & 0 & 1 \end{pmatrix} : \gamma_1, \gamma_2 \in F \right\},$$

and so again $\psi(G)$ has an abelian decomposition by virtue of Lemma 2.2.

Case 3. $l_s(I_R) = 3$.
In this case we have the Loewy series $0 = I_0 \subset I_1 \subset I_2 \subset I_3 = I$, where I_1 and I_2 are two-sided ideals in R. Taking a basis v_1, v_2, v_3 of I such that $v_1 \in I_1$, $v_2 \in I_2 \setminus I_1$ and $v_3 \in I_3 \setminus I_2$ we can assume that $\varphi(G)$ and $\psi(G)$ are contained in the group $\mathrm{T}_3(F)$.

A direct computation shows that $|\,\mathrm{UT}_n(F)| = q^{\frac{n(n-1)}{2}}$, $|\,\mathrm{D}_n(F)| = (q-1)^n$ and that $\mathrm{D}_n(F)\,\mathrm{UT}_n(F) = \mathrm{T}_n(F)$ for any $n \geq 1$. Using Lemma 2.2 we can assume without loss of generality that

$$\varphi(G) = (\varphi(G) \cap \mathrm{D}_3(G))(\varphi(G) \cap \mathrm{UT}_3(G)).$$

If $\varphi(G) \cap \mathrm{UT}_3(G)$ is abelian then our claim is true. Suppose now that $\varphi(G) \cap \mathrm{UT}_3(G)$ contains two non-commuting matrices

$$a = \begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{pmatrix}, \qquad a' = \begin{pmatrix} 1 & \alpha' & \beta' \\ 0 & 1 & \gamma' \\ 0 & 0 & 1 \end{pmatrix},$$

for some $\alpha, \beta, \gamma, \alpha', \beta', \gamma' \in F$. It is easy to check that the condition $aa' \neq a'a$ is equivalent to the inequality

$$\alpha\gamma' \neq \alpha'\gamma. \tag{2.2}$$

Let $X = (x_{ij})$ be a matrix in $\psi(G)$. Note that it is an upper triangular matrix. The computation of $aX - Xa$ and $a'X - Xa'$ gives the following equations:

$$\alpha x_{2,2} - \alpha x_{1,1} = \alpha' x_{2,2} - \alpha' x_{1,1} = 0 \tag{2.3}$$
$$\alpha x_{2,3} + \beta x_{3,3} - \beta x_{1,1} - \gamma x_{1,2} = \alpha' x_{2,3} + \beta' x_{3,3} - \beta' x_{1,1} - \gamma' x_{1,2} = 0 \tag{2.4}$$
$$\gamma x_{3,3} - \gamma x_{2,2} = \gamma' x_{3,3} - \gamma' x_{2,2} \tag{2.5}$$

The inequality (2.2) implies that $\alpha \neq 0$ or $\alpha' \neq 0$. Hence (2.3) gives $x_{1,1} = x_{2,2}$. Analogously, (2.5) gives $x_{3,3} = x_{2,2}$. Now (2.4) gives an equation system

$$\begin{cases} \alpha x_{2,3} - \gamma x_{1,2} &= 0 \\ \alpha' x_{2,3} - \gamma' x_{1,2} &= 0. \end{cases}$$

which has non-zero determinant by (2.2). This means that $\psi(G)$ is contained in the set of matrices

$$\left\{ \begin{pmatrix} x & 0 & y \\ 0 & x & 0 \\ 0 & 0 & x \end{pmatrix} : x, y \in F \right\},$$

so $\psi(G)$ is commutative. □

Proof of Theorem 1. It follows immediately from Proposition 2.5 and Lemma 1.3. □

Acknowledgement

The work of the third and the fourth authors was supported by RFBR grants 17-01-00895 and 16-01-00113, respectively. The work of the second and the fifth authors has been supported by the projects MTM2013-45588-C3-1-P from the Spanish Ministey of Economy and GRUPIN14-142 from the "Principado de Asturias".

References

[1] C. García Pillado, S. González, V. Markov and C. Martínez. Non-abelian group codes over an arbitrary finite field. *Fundementalnaya i prikladnaya matematika*, 20:1 (2015), 17–22 (*in Russian*), english translation: J. Math. Sci., 223:5 (2017), 504-507.

[2] J.J. Bernal, Á del Río and J.J. Simón. An intrinsical description of group codes. *Designs, Codes and Cryptography*, 51:3 (2009), 289–300.

[3] S. Lang. Algebra. 3rd edition. Springer, 2002.

[4] I. N. Herstein. Noncommutative Rings. Mathematical Association of America, 1968.

[5] B. Amberg and B. Höfling. On finite products of nilpotent groups. *Arch. Math.*, 63:1 (1994), 1–8.

[6] A. Ballester-Bolinches, R. Esteban-Romero and M. Asaad. Products of Finite Groups. De Gruyter expositions in mathematics (vol. 53), Walter de Gruyter, 2010.

[7] C. Năstăsescu and F. van Oystaeyen. Dimensions of Ring Theory. University of Antwerp, Belgium, 1987.