A GAP-conjecture and its solution: Isomorphism classes of capable special *p*-groups of rank 2

Luise-Charlotte Kappe menger@math.binghamton.edu Binghamton University (joint with H. Heineken and R.F. Morse) **Definition 1.** A group G is said to be capable if there exists a group H such that  $G \cong H/Z(H)$ , or equivalently, G is isomorphic to the inner automorphism group of a group H.

M. Hall and J.K. Senior, *The groups of order*  $2^n$  ( $n \le 6$ ), MacMillan, New York, 1964.

**Definition 1.** A group G is said to be capable if there exists a group H such that  $G \cong H/Z(H)$ , or equivalently, G is isomorphic to the inner automorphism group of a group H.

M. Hall and J.K. Senior, *The groups of order*  $2^n$  ( $n \le 6$ ), MacMillan, New York, 1964.

**Theorem 1**. Let A be a finitely generated abelian group written as

$$A=\mathbb{Z}_{n_1}\oplus\mathbb{Z}_{n_2}\oplus\ldots\oplus Z_{n_k}$$

such that  $n_i \mid n_{i+1}$ , where  $\mathbb{Z}_n = \mathbb{Z}$ , the infinite cyclic group, if n = 0. Then A is capable if and only if  $k \geq 2$  and  $n_{k-1} = n_k$ .

**Definition 1.** A group G is said to be capable if there exists a group H such that  $G \cong H/Z(H)$ , or equivalently, G is isomorphic to the inner automorphism group of a group H.

M. Hall and J.K. Senior, *The groups of order*  $2^n$  ( $n \le 6$ ), MacMillan, New York, 1964.

**Theorem 1**. Let A be a finitely generated abelian group written as

$$A=\mathbb{Z}_{n_1}\oplus\mathbb{Z}_{n_2}\oplus\ldots\oplus Z_{n_k}$$

such that  $n_i \mid n_{i+1}$ , where  $\mathbb{Z}_n = \mathbb{Z}$ , the infinite cyclic group, if n = 0. Then A is capable if and only if  $k \geq 2$  and  $n_{k-1} = n_k$ .

R. Baer, *Groups with preassigned central and central quotient groups*, Trans. Amer. Math. Soc. 44 (1938), 387-412.

F.R. Beyl, U. Felgner, and P. Schmid, *On groups occurring as center factor groups*, J. Algebra 61 (1979), 161-177.

F.R. Beyl, U. Felgner, and P. Schmid, *On groups occurring as center factor groups*, J. Algebra 61 (1979), 161-177.

**Definition 2.** The epicenter  $Z^*(G)$  of a group G is defined as

 $\bigcap \{\phi Z(E); (E, \phi) \text{ is a central extension of } G\}.$ 

F.R. Beyl, U. Felgner, and P. Schmid, *On groups occurring as center factor groups*, J. Algebra 61 (1979), 161-177.

**Definition 2.** The epicenter  $Z^*(G)$  of a group G is defined as

 $\bigcap \{\phi Z(E); (E, \phi) \text{ is a central extension of } G\}.$ 

**Theorem 2.** A group is capable if and only  $Z^*(G) = 1$ .

G. Ellis, *On the capability of groups*, Proc. Edinburgh Math Soc. 41 (1998), 487-495.

G. Ellis, *On the capability of groups*, Proc. Edinburgh Math Soc. 41 (1998), 487-495.

**Theorem 3.**  $Z^*(G) = Z^{\wedge}(G) = \{a \in G \mid a \wedge g = 1_{\wedge}, \forall g \in G\}$ , the exterior center of G.

G. Ellis, *On the capability of groups*, Proc. Edinburgh Math Soc. 41 (1998), 487-495.

**Theorem 3.**  $Z^*(G) = Z^{\wedge}(G) = \{a \in G \mid a \wedge g = 1_{\wedge}, \forall g \in G\}$ , the exterior center of G.

A. Magidin and R.F. Morse, *Capable p-groups*, Proceedings Groups St. Andrews 2013, Lecture Notes LMS 422. (2015), 399-427.

**Definition 3.** A p-group G is special of rank n, if G' is elementary abelian of rank n and G' = Z(G).

**Definition 3.** A *p*-group G is special of rank n, if G' is elementary abelian of rank n and G' = Z(G).

F.R. Beyl, U. Felgner, and P. Schmid, *On groups occurring as center factor groups*, J. Algebra 61 (1979), 161-177.

**Definition 3.** A *p*-group *G* is special of rank *n*, if G' is elementary abelian of rank *n* and G' = Z(G).

F.R. Beyl, U. Felgner, and P. Schmid, *On groups occurring as center factor groups*, J. Algebra 61 (1979), 161-177.

**Theorem 4.** A special p-group of rank 1 (= extra special) is capable if and only if it is dihedral of order 8 or of order  $p^3$  and exponent p, p > 2.

H. Heineken, Nilpotent groups of class 2 that can appear as central quotient groups, Rend. Sem. Mat. Univ. Padova, 84 (1990), 241-248.

H. Heineken, Nilpotent groups of class 2 that can appear as central quotient groups, Rend. Sem. Mat. Univ. Padova, 84 (1990), 241-248.

**Theorem 5.** Let G be a special p-group or rank 2 which is capable. Then

$$p^5 \leq |G| \leq p^7.$$

**Lemma 1.** Let G be a p-group of nilpotency class 2 whose center is an elementary abelian p-group. Then G has exponent at most  $p^2$ .

**Lemma 1.** Let G be a p-group of nilpotency class 2 whose center is an elementary abelian p-group. Then G has exponent at most  $p^2$ .

The case p = 2:

**Theorem 6.** Let G be a capable special 2-group of rank 2. Then G has exponent 4 and there are three isomorphism classes, if  $|G| = 2^5$  and  $2^6$ , and one isomorphism class, if  $|G| = 2^7$ .

From now on: p > 2.

GAP output: special *p*-groups of rank 2 and order  $p^5$  for 2 :

	$\exp G = p$		
р	Total	Capable	
3	1	1	
5	1	1	
7	1	1	
11	1	1	
13	1	1	
17	1	1	
19	1	1	
23	1	1	
29	1	1	
31	1	1	
37	1	1	

GAP output: special *p*-groups of rank 2 and order  $p^5$  for 2 :

	$\exp G = p$		$exp G = p^2$	
р	Total	Capable	Total	Capable
3	1	1	10	3
5	1	1	12	3
7	1	1	14	3
11	1	1	18	3
13	1	1	20	3
17	1	1	24	3
19	1	1	26	3
23	1	1	30	3
29	1	1	36	3
31	1	1	38	3
37	1	1	44	3

GAP output: special *p*-groups of rank 2 and order  $p^6$  for 2 :

GAP output: special *p*-groups of rank 2 and order  $p^6$  for 2 :

	exp G = p		
р	Total	Capable	
3 5 7	3	3	
5	3	3	
7	3	3	
11	3	3	
13	3	3	
17	3	3	
19	3	3	
23	3	3	
29	3	3	
31	3 3 3 3 3 3 3 3 3	3	
37	3	3	

GAP output: special *p*-groups of rank 2 and order  $p^6$  for 2 :

	$\exp G = p$		$exp G = p^2$	
р	Total	Capable	Total	Capable
3	3	3	32	3
5	3	3	38	3
7	3	3	44	3
11	3	3	56	3
13	3	3	62	3
17	3	3	74	3
19	3	3	80	3
23	3	3	92	3
29	3	3	110	3
31	3	3	116	3
37	3	3	134	3

GAP output: special p-groups of rank 2 and order  $p^7$  for 2 :

GAP output: special p-groups of rank 2 and order  $p^7$  for 2 :

	$\exp G = p$		
р	Total	Capable	
3	2	1	
5	2	1	
7	2	1	
11	2	1	

GAP output: special *p*-groups of rank 2 and order  $p^7$  for 2 :

	exp G = p		$exp G = p^2$	
р	Total	Capable	Total	Capable
3	2	1	97	1
5	2	1	136	1
7	2	1	184	1
11	2	1	298	1

**Theorem 7.** Let G be a special p-group of rank 2, exponent p and order  $p^n$ ,  $5 \le n \le 7$ . If G is capable, then there exists exactly one isomorphism class for n = 5 and 7, and three classes for n = 6.

**Theorem 7.** Let G be a special p-group of rank 2, exponent p and order  $p^n$ ,  $5 \le n \le 7$ . If G is capable, then there exists exactly one isomorphism class for n = 5 and 7, and three classes for n = 6.

A. Magidin, On the capability of finite groups of class 2 and prime exponent, Publ. Math. Debrecen, 85 (2014) 309-337.

The case exp  $G = p^2$ :

The case exp  $G=p^2$ : Consider  $G=K\rtimes L$ ,  $K=\langle a,b\mid a^{p^2}=b^{p^2}=1,\ a^b=a^{p+1}\rangle$  and L an elementary abelian p-group of rank n. The case  $\exp G = p^2$ : Consider  $G = K \rtimes L$ ,  $K = \langle a, b \mid a^{p^2} = b^{p^2} = 1$ ,  $a^b = a^{p+1} \rangle$  and L an elementary abelian p-group of rank n.

"Proposition 1." Let p be an odd prime. The groups defined by the following presentations contain all the capable special p-groups of rank 2 of order  $p^{4+n}$  with  $G^p = G'$ , exponent  $p^2$  and  $n \ge 1$ :

The case exp  $G = p^2$ : Consider  $G = K \rtimes L$ ,  $K = \langle a, b \mid a^{p^2} = b^{p^2} = 1$ ,  $a^b = a^{p+1} \rangle$  and L an elementary abelian p-group of rank n.

"Proposition 1." Let p be an odd prime. The groups defined by the following presentations contain all the capable special p-groups of rank 2 of order  $p^{4+n}$  with  $G^p = G'$ , exponent  $p^2$  and  $n \ge 1$ :

$$G(m_{1},...,m_{n}) = \langle a,b,x_{1},...,x_{n} | a^{p^{2}} = b^{p^{2}} = x_{1}^{p} = \cdots = x_{n}^{p} = 1, a^{b} = a^{p+1}, a^{x_{i}} = a^{s_{i}p+1}b^{t_{i}p}, b^{x_{i}} = a^{u_{i}p}b^{-s_{i}p+1}, 1 \leq i \leq n$$

$$[x_{j},x_{k}] = 1, 1 \leq j < k \leq n \rangle,$$

$$(1.1)$$

The case exp  $G=p^2$ : Consider  $G=K\rtimes L$ ,  $K=\langle a,b\mid a^{p^2}=b^{p^2}=1,\ a^b=a^{p+1}\rangle$  and L an elementary abelian p-group of rank n.

"Proposition 1." Let p be an odd prime. The groups defined by the following presentations contain all the capable special p-groups of rank 2 of order  $p^{4+n}$  with  $G^p = G'$ , exponent  $p^2$  and  $n \ge 1$ :

$$G(m_{1},...,m_{n}) = \langle a,b,x_{1},...,x_{n} | a^{p^{2}} = b^{p^{2}} = x_{1}^{p} = \cdots = x_{n}^{p} = 1, a^{b} = a^{p+1}, a^{x_{i}} = a^{s_{i}p+1}b^{t_{i}p}, b^{x_{i}} = a^{u_{i}p}b^{-s_{i}p+1}, 1 \leq i \leq n [x_{j},x_{k}] = 1, 1 \leq j < k \leq n \rangle,$$

$$(1.1)$$

where 
$$0 \le s_i, t_i, u_i < p$$
 and  $m_i = \begin{pmatrix} s_i & t_i \\ u_i & -s_i \end{pmatrix}$  for  $i = 1, \ldots, n$ .

The case exp  $G = p^2$ : Consider  $G = K \rtimes L$ ,  $K = \langle a, b \mid a^{p^2} = b^{p^2} = 1$ ,  $a^b = a^{p+1} \rangle$  and L an elementary abelian p-group of rank n.

**Proposition 1.** Let p be an odd prime. The groups defined by the following presentations are all capable and in particular contain all the capable special p-groups of rank 2 of order  $p^{4+n}$  with  $G^p = G'$ , exponent  $p^2$  and  $n \ge 1$ :

$$G(m_{1},...,m_{n}) = \langle a,b,x_{1},...,x_{n} | a^{p^{2}} = b^{p^{2}} = x_{1}^{p} = \cdots = x_{n}^{p} = 1, a^{b} = a^{p+1}, a^{x_{i}} = a^{s_{i}p+1}b^{t_{i}p}, b^{x_{i}} = a^{u_{i}p}b^{-s_{i}p+1}, 1 \leq i \leq n$$

$$[x_{j},x_{k}] = 1, 1 \leq j < k \leq n \rangle,$$

$$(1.1)$$

where 
$$0 \le s_i, t_i, u_i < p$$
 and  $m_i = \begin{pmatrix} s_i & t_i \\ u_i & -s_i \end{pmatrix}$  for  $i = 1, \ldots, n$ .

**Theorem 8.** There are exactly three isomorphism classes of capable special p-groups of rank 2 and exponent  $p^2$ , if  $|G| = p^5$  and  $p^6$ , and one such class, if  $|G| = p^7$ .

**Theorem 8.** There are exactly three isomorphism classes of capable special p-groups of rank 2 and exponent  $p^2$ , if  $|G| = p^5$  and  $p^6$ , and one such class, if  $|G| = p^7$ .

For  $|G| = p^5$ , we specifically have

**Theorem 8.** There are exactly three isomorphism classes of capable special p-groups of rank 2 and exponent  $p^2$ , if  $|G| = p^5$  and  $p^6$ , and one such class, if  $|G| = p^7$ .

For  $|G| = p^5$ , we specifically have

 $\mathcal{E}_1 = \{G(m) \mid 0 \neq det \ m \ and \ -det \ m \ a \ quadratic \ residue \ mod \ p\},$ 

**Theorem 8.** There are exactly three isomorphism classes of capable special p-groups of rank 2 and exponent  $p^2$ , if  $|G| = p^5$  and  $p^6$ , and one such class, if  $|G| = p^7$ .

For  $|G| = p^5$ , we specifically have

 $\mathcal{E}_1 = \{ \textit{G}(\textit{m}) \mid 0 \neq \textit{ det m and -det m a quadratic residue mod p} \},$   $\mathcal{E}_2 = \{ \textit{G}(\textit{m}) \mid 0 \neq \textit{ det m, and -det m a quadratic nonresidue mod p} \},$ 

**Theorem 8.** There are exactly three isomorphism classes of capable special p-groups of rank 2 and exponent  $p^2$ , if  $|G| = p^5$  and  $p^6$ , and one such class, if  $|G| = p^7$ .

For  $|G| = p^5$ , we specifically have

$$\mathcal{E}_1 = \{ \textit{G}(\textit{m}) \mid 0 \neq \textit{ det m and -det m a quadratic residue mod p} \},$$
 
$$\mathcal{E}_2 = \{ \textit{G}(\textit{m}) \mid 0 \neq \textit{ det m}, \textit{ and -det m a quadratic nonresidue mod p} \},$$

$$\mathcal{E}_3 = \{ extit{G(m)} \mid ext{ det } m = 0 ext{ and } m 
eq egin{pmatrix} 0 & 0 \ u & 0 \end{pmatrix}, u \in \mathbb{Z}_p \}.$$

**Conjecture.** For  $A \in SL(2, p)$  we have  $G(m) \cong G(m^A)$ .

**Conjecture.** For  $A \in SL(2, p)$  we have  $G(m) \cong G(m^A)$ .

No! If 
$$m = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$
,  $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ , then  $m^A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ . But  $G(m) \ncong G(m^A)$ .

**Conjecture.** For  $A \in SL(2, p)$  we have  $G(m) \cong G(m^A)$ .

No! If 
$$m = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$
,  $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ , then  $m^A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ . But  $G(m) \not\cong G(m^A)$ .

**Proposition 2.** Let 
$$m = \begin{pmatrix} s & t \\ u & -s \end{pmatrix}$$
 and  $k \in \mathbb{Z}_p^*$ . Then  $G(m) \cong G(km)$ .

Let 
$$m=\begin{pmatrix} s & t \\ u & -s \end{pmatrix}$$
 and  $\bar{m}=\begin{pmatrix} \bar{s} & \bar{t} \\ \bar{u} & -\bar{s} \end{pmatrix}$ . Set

Let 
$$m=\begin{pmatrix} s & t \\ u & -s \end{pmatrix}$$
 and  $\bar{m}=\begin{pmatrix} \bar{s} & \bar{t} \\ \bar{u} & -\bar{s} \end{pmatrix}$ . Set

$$G(m) = \left\langle a, b, x; a^{p^2}, b^{p^2}, x^p, [a, b] = a^p, \\ [a, x] = a^{ps} b^{pt}, [b, x] = a^{up} b^{-sp} \right\rangle$$

Let 
$$m=\begin{pmatrix} s & t \\ u & -s \end{pmatrix}$$
 and  $\bar{m}=\begin{pmatrix} \bar{s} & \bar{t} \\ \bar{u} & -\bar{s} \end{pmatrix}$ . Set

$$G(m) = \left\langle a, b, x; a^{p^2}, b^{p^2}, x^p, [a, b] = a^p, \\ [a, x] = a^{ps} b^{pt}, [b, x] = a^{up} b^{-sp} \right\rangle$$

and

$$G(\bar{m}) = \left\langle \begin{array}{l} \bar{a}, \bar{b}, \bar{x}; \bar{a}^{p^2}, \bar{b}^{p^2}, \bar{x}^p, [\bar{a}, \bar{b}] = \bar{a}^p, \\ [\bar{a}, \bar{x}] = \bar{a}^{p\bar{s}} \bar{b}^{p\bar{t}}, [\bar{b}, \bar{x}] = \bar{a}^{\bar{u}p} \bar{b}^{-\bar{s}p} \end{array} \right\rangle.$$

Let 
$$m=\begin{pmatrix} s & t \\ u & -s \end{pmatrix}$$
 and  $\bar{m}=\begin{pmatrix} \bar{s} & \bar{t} \\ \bar{u} & -\bar{s} \end{pmatrix}$ . Set

$$G(m) = \left\langle a, b, x; a^{p^2}, b^{p^2}, x^p, [a, b] = a^p, \\ [a, x] = a^{ps} b^{pt}, [b, x] = a^{up} b^{-sp} \right\rangle$$

and

$$G(\bar{m}) = \left\langle \begin{array}{l} \bar{a}, \bar{b}, \bar{x}; \bar{a}^{p^2}, \bar{b}^{p^2}, \bar{x}^p, [\bar{a}, \bar{b}] = \bar{a}^p, \\ [\bar{a}, \bar{x}] = \bar{a}^{p\bar{s}} \bar{b}^{p\bar{t}}, [\bar{b}, \bar{x}] = \bar{a}^{\bar{u}p} \bar{b}^{-\bar{s}p} \end{array} \right\rangle.$$

Find  $\alpha_1$ ,  $\beta_1$ ,  $\gamma_1$ ,  $\alpha_2$ ,  $\beta_2$ ,  $\gamma_2$ ,  $\gamma$  with  $\bar{a}=a^{\alpha_1}b^{\beta_1}x^{\gamma_1}$ ,  $\bar{b}=a^{\alpha_2}b^{\beta_2}x^{\gamma_2}$ ,  $\bar{x}=x^{\gamma}$  such that the relations of  $G(\bar{m})$  are satisfied.

Let 
$$m=\begin{pmatrix} s & t \\ u & -s \end{pmatrix}$$
 and  $\bar{m}=\begin{pmatrix} \bar{s} & \bar{t} \\ \bar{u} & -\bar{s} \end{pmatrix}$ . Set

$$G(m) = \left\langle a, b, x; a^{p^2}, b^{p^2}, x^p, [a, b] = a^p, \\ [a, x] = a^{ps} b^{pt}, [b, x] = a^{up} b^{-sp} \right\rangle$$

and

$$G(\bar{m}) = \left\langle \begin{array}{l} \bar{a}, \bar{b}, \bar{x}; \bar{a}^{p^2}, \bar{b}^{p^2}, \bar{x}^p, [\bar{a}, \bar{b}] = \bar{a}^p, \\ [\bar{a}, \bar{x}] = \bar{a}^{p\bar{s}} \bar{b}^{p\bar{t}}, [\bar{b}, \bar{x}] = \bar{a}^{\bar{u}p} \bar{b}^{-\bar{s}p} \end{array} \right\rangle.$$

Find  $\alpha_1$ ,  $\beta_1$ ,  $\gamma_1$ ,  $\alpha_2$ ,  $\beta_2$ ,  $\gamma_2$ ,  $\gamma$  with  $\bar{a}=a^{\alpha_1}b^{\beta_1}x^{\gamma_1}$ ,  $\bar{b}=a^{\alpha_2}b^{\beta_2}x^{\gamma_2}$ ,  $\bar{x}=x^{\gamma}$  such that the relations of  $G(\bar{m})$  are satisfied.

**Remark.** By Proposition 2 we can assume that  $\gamma = 1$ .

**Proposition 3.** There exist  $\bar{a}, \bar{b}, \bar{x} \in G(m)$  such that the relations  $[\bar{a}, \bar{x}] = \bar{a}^{p\bar{s}} \bar{b}^{p\bar{t}}$  and  $[\bar{b}, \bar{x}] = \bar{a}^{p\bar{u}} \bar{b}^{-p\bar{s}}$  are satisfied if and only if there exists

**Proposition 3.** There exist  $\bar{a}, \bar{b}, \bar{x} \in G(m)$  such that the relations  $[\bar{a}, \bar{x}] = \bar{a}^{p\bar{s}} \bar{b}^{p\bar{t}}$  and  $[\bar{b}, \bar{x}] = \bar{a}^{p\bar{u}} \bar{b}^{-p\bar{s}}$  are satisfied if and only if there exists  $A = \begin{pmatrix} \alpha_1 & \beta_1 \\ \alpha_2 & \beta_2 \end{pmatrix} \in \mathbb{Z}_p^{2\times 2}$  such that  $\begin{pmatrix} s & t \\ u & -s \end{pmatrix} A = A \begin{pmatrix} \bar{s} & \bar{t} \\ \bar{u} & -\bar{s} \end{pmatrix}$ .

**Proposition 3.** There exist  $\bar{a}, \bar{b}, \bar{x} \in G(m)$  such that the relations  $[\bar{a}, \bar{x}] = \bar{a}^{p\bar{s}}\bar{b}^{p\bar{t}}$  and  $[\bar{b}, \bar{x}] = \bar{a}^{p\bar{u}}\bar{b}^{-p\bar{s}}$  are satisfied if and only if there exists  $A = \begin{pmatrix} \alpha_1 & \beta_1 \\ \alpha_2 & \beta_2 \end{pmatrix} \in \mathbb{Z}_p^{2\times 2}$  such that  $\begin{pmatrix} s & t \\ u & -s \end{pmatrix} A = A \begin{pmatrix} \bar{s} & \bar{t} \\ \bar{u} & -\bar{s} \end{pmatrix}$ .

**Remark.** If  $0 \neq \det m = \det \bar{m}$ , then there exists  $A \in SL(2, p)$  such that  $m^A = \bar{m}$ , or equivalently  $mA = A\bar{m}$ . (Note:  $tr(m) = tr(\bar{m}) = 0$ .)

**Goal:** For given  $\alpha_1$ ,  $\alpha_2$ ,  $\beta_1$   $\beta_2$  find  $\gamma_1$ ,  $\gamma_2$  such that  $[\bar{a}, \bar{b}] = \bar{a}^p$  is satisfied.

**Observation:** The relation  $[\bar{a}, \bar{b}] = \bar{a}^p$  results into a  $2 \times 2$  linear system of equations of the form  $B\begin{pmatrix} \gamma_1 \\ \gamma_2 \end{pmatrix} = \begin{pmatrix} \delta_1 \\ \delta_2 \end{pmatrix}$ ,

**Goal:** For given  $\alpha_1$ ,  $\alpha_2$ ,  $\beta_1$   $\beta_2$  find  $\gamma_1$ ,  $\gamma_2$  such that  $[\bar{a}, \bar{b}] = \bar{a}^p$  is satisfied.

**Observation:** The relation  $[\bar{a}, \bar{b}] = \bar{a}^p$  results into a  $2 \times 2$  linear system of equations of the form  $B \begin{pmatrix} \gamma_1 \\ \gamma_2 \end{pmatrix} = \begin{pmatrix} \delta_1 \\ \delta_2 \end{pmatrix}$ , where the entries of B and  $\begin{pmatrix} \delta_1 \\ \delta_2 \end{pmatrix}$  are functions of  $\alpha_1$ ,  $\alpha_2$ ,  $\beta_1$ ,  $\beta_2$  and det  $B \neq 0$ .

**Goal:** For given  $\alpha_1$ ,  $\alpha_2$ ,  $\beta_1$   $\beta_2$  find  $\gamma_1$ ,  $\gamma_2$  such that  $[\bar{a}, \bar{b}] = \bar{a}^p$  is satisfied.

**Observation:** The relation  $[\bar{a}, \bar{b}] = \bar{a}^p$  results into a  $2 \times 2$  linear system of equations of the form  $B \begin{pmatrix} \gamma_1 \\ \gamma_2 \end{pmatrix} = \begin{pmatrix} \delta_1 \\ \delta_2 \end{pmatrix}$ , where the entries of B and  $\begin{pmatrix} \delta_1 \\ \delta_2 \end{pmatrix}$  are functions of  $\alpha_1$ ,  $\alpha_2$ ,  $\beta_1$ ,  $\beta_2$  and det  $B \neq 0$ . There is a nontrivial solution  $\begin{pmatrix} \gamma_1 \\ \gamma_2 \end{pmatrix}$  if  $\begin{pmatrix} \delta_1 \\ \delta_2 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$  and  $\begin{pmatrix} \gamma_1 \\ \gamma_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$  if  $\begin{pmatrix} \delta_1 \\ \delta_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ .

(1) 
$$G(m) \cong G\left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right)$$
 if det  $m = 0$ ;

(1) 
$$G(m) \cong G\left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right)$$
 if det  $m = 0$ ;

(2) 
$$G(m) \cong G\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right)$$
, if  $0 \neq det \ m \ and -det \ m$  is a quadratic residue mod  $p$ .

- (1)  $G(m) \cong G\left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right)$  if det m = 0;
- (2)  $G(m) \cong G\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right)$ , if  $0 \neq det \ m \ and -det \ m$  is a quadratic residue mod p.
- (3)  $G(m) \cong G\left(\begin{pmatrix} 0 & 1 \\ r & 0 \end{pmatrix}\right)$ , where r is a primitive root mod p, if  $0 \neq det\ m$  and  $-det\ m$  is a quadratic nonresidue mod p.