

# A REMARK ON THE EXISTENCE OF $K(\pi, 1)$ 's OVER THE RATIONALS

Patrick Forré and Jochen Gärtner

November 17, 2009

ABSTRACT. Let  $p$  be an odd prime number and  $S$  a finite set of prime numbers  $\equiv 1 \pmod{p}$ . In [Lab06], J. Labute showed that there exists set  $S_0$  of prime numbers  $\equiv 1 \pmod{p}$  with  $|S_0| = |S|$  such that the group  $G_{S \cup S_0}(p)$  is a mild pro- $p$ -group. In particular we have  $cd(G_{S \cup S_0}(p)) = 2$  and the scheme  $\text{Spec}(\mathbb{Z}) \setminus (S \cup S_0)$  is a  $K(\pi, 1)$  for  $p$ . In [Sch07] and in more generality in [Sch08], A. Schmidt extended this result to arbitrary number fields  $k$ . We will show that if  $k = \mathbb{Q}$  it is always possible to enlarge a given set  $S$  of prime numbers  $\equiv 1 \pmod{p}$  by two prime numbers  $\equiv 1 \pmod{p}$  such that the resulting group is mild. Moreover in many cases it is sufficient to add one single prime. Finally we give analogous result in the case  $p = 2$ .

## 1 Construction of strongly free sequences

We make use of the following general criterion by A. Schmidt, cf. [Sch07], Th. 5.5.

**(1.1) Proposition.** *Let  $k$  be a field and  $L(X)$  the free Lie algebra over  $X = \{\xi_1, \dots, \xi_d\}$ . Furthermore let  $\rho_1, \dots, \rho_r \in L(X)$  be given such that*

$$\rho_i = \sum_{1 \leq k < l \leq d} a_{ikl} [\xi_k, \xi_l]$$

for all  $i = 1, \dots, r$  with  $a_{ikl} \in k$ . Assume that there exists a natural number  $a$ ,  $1 \leq a < d$  such that

(i)  $a_{ikl} = 0$  for  $a < k < l \leq d$  and all  $i = 1, \dots, r$ ,

(ii) the  $r \times a(d - a)$ -matrix

$$(a_{ikl})_{i,(k,l)}, \quad 1 \leq i \leq r, \quad 1 \leq k \leq a < l \leq d$$

has rank  $r$ .

Then the sequence  $\rho_1, \dots, \rho_r$  is strongly free.

Applying this criterion we will prove the following lemma:

**(1.2) Lemma.** *Let  $k$  be a field,  $n \geq 2$  and  $L(X)$  the free Lie algebra over  $X = \{\zeta_1, \dots, \zeta_{n+2}\}$ . Let  $\rho_1, \dots, \rho_{n+2} \in L(X)$  be given such that*

$$\begin{aligned} \rho_i &= \sum_{1 \leq k < l \leq n} a_{ikl} [\zeta_k, \zeta_l] + b_i [\zeta_i, \zeta_{n+1}] + c_i [\zeta_i, \zeta_{n+2}], \quad i = 1, \dots, n, \\ \rho_{n+1} &= d [\zeta_{n+1}, \zeta_2], \\ \rho_{n+2} &= e [\zeta_{n+2}, \zeta_1], \end{aligned}$$

where  $a_{il}, b_i, c_i \in k$ , such that

- (i)  $d, e, b_1, c_2 \neq 0$  and
- (ii)  $b_i \neq 0$  or  $c_i \neq 0$  for  $i = 3, \dots, n$ .

Then the sequence  $\rho_1, \dots, \rho_{n+2}$  is strongly free.

*Proof.* We apply (1.1) with  $a = n$ . Since the commutator  $[\zeta_{n+1}, \zeta_{n+2}]$  doesn't occur in any of the  $\rho_i$ ,  $i = 1, \dots, n+2$  condition (i) of (1.1) holds. Furthermore the matrix of condition (ii) of (1.1) is of the form

$$\begin{pmatrix} & [\xi_1, \xi_{n+1}] & [\xi_2, \xi_{n+1}] & \cdots & [\xi_n, \xi_{n+1}] & [\xi_1, \xi_{n+2}] & [\xi_2, \xi_{n+2}] & \cdots & [\xi_n, \xi_{n+2}] \\ \rho_1 & b_1 & 0 & \cdots & 0 & c_1 & 0 & \cdots & 0 \\ \rho_2 & 0 & b_2 & \cdots & 0 & 0 & c_2 & \cdots & 0 \\ \vdots & & & \ddots & & & & & \vdots \\ \rho_n & 0 & 0 & \cdots & b_n & 0 & 0 & \cdots & c_n \\ \rho_{n+1} & 0 & -d & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \rho_{n+2} & 0 & 0 & \cdots & 0 & -e & 0 & \cdots & 0 \end{pmatrix}.$$

This matrix has rank  $n+2$  which follows immediately from the assumptions. This completes the proof.  $\square$

Roughly spoken, the above lemma states the following: If  $n \geq 2$ ,  $L(X)$  is the free Lie Algebra on  $X = \{\zeta_1, \dots, \zeta_n\}$  and a sequence  $\rho'_1, \dots, \rho'_n$  of homogeneous elements of degree 2 in  $L(X)$  is given, then by adding two generators  $\zeta_{n+1}, \zeta_{n+2}$  one can obtain a strongly free sequence  $\rho_1, \dots, \rho_{n+2}$  in  $L(X \cup \{\zeta_{n+1}, \zeta_{n+2}\})$  such that for  $i = 1, \dots, n$  we have  $\rho_i \equiv \rho'_i \pmod{\langle \zeta_{n+1}, \zeta_{n+2} \rangle}$  (here  $\langle \zeta_{n+1}, \zeta_{n+2} \rangle$  denotes the ideal of  $L(X \cup \{\zeta_{n+1}, \zeta_{n+2}\})$  generated by  $\{\zeta_{n+1}, \zeta_{n+2}\}$ ). Under certain conditions one can obtain a strongly free sequence by adding one single extra generator. The precise statement is the following:

**(1.3) Lemma.** *Let  $k$  be a field,  $n \geq 3$  and  $L(X)$  the free Lie algebra over  $X = \{\xi_1, \dots, \xi_{n+1}\}$ . Let  $\rho_1, \dots, \rho_{n+1} \in L(X)$  be given by*

$$\begin{aligned} \rho_i &= \sum_{1 \leq l \leq n} a_{il} [\xi_i, \xi_l] + b_i [\xi_i, \xi_{n+1}], \quad i = 1, \dots, n, \\ \rho_{n+1} &= \sum_{1 \leq l \leq n} c_l [\xi_{n+1}, \xi_l], \end{aligned}$$

where  $a_{il}, b_i, d \in k$ , such that

- (i)  $a_{1n}, a_{n2}, c_1 \neq 0, c_n = 0$  and  
(ii)  $b_i = 0$  if and only if  $i \in \{1, n\}$ .

Then the sequence  $\rho_1, \dots, \rho_{n+1}$  is strongly free.

*Proof.* We apply (1.1) with  $a = n - 1$ . Since  $b_n = c_n = 0$  condition (i) of (1.1) holds and the  $(n + 1) \times 2(n - 1)$ -matrix of condition (ii) is of the form

$$\begin{pmatrix} & [\xi_1, \xi_n] & [\xi_2, \xi_n] & \cdots & [\xi_{n-1}, \xi_n] & [\xi_1, \xi_{n+1}] & [\xi_2, \xi_{n+1}] & \cdots & [\xi_{n-1}, \xi_{n+1}] \\ \rho_1 & \mathbf{a_{1n}} & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \rho_2 & 0 & a_{2n} & \cdots & 0 & 0 & \mathbf{b_2} & \cdots & 0 \\ \vdots & & & \ddots & & & & \ddots & \\ \rho_{n-1} & 0 & 0 & \cdots & a_{n-1,n} & 0 & 0 & \cdots & \mathbf{b_{n-1}} \\ \rho_n & -a_{n1} & -\mathbf{a_{n2}} & \cdots & -a_{n,n-1} & 0 & 0 & \cdots & 0 \\ \rho_{n+1} & 0 & 0 & \cdots & 0 & -\mathbf{c_1} & -c_2 & \cdots & -c_{n-1} \end{pmatrix}$$

where the bold coefficients are non-zero by assumption. This matrix clearly has rank  $n + 1$  and the claim follows.  $\square$

## 2 Arithmetic Results

We want to deduce some arithmetic consequences for  $p$ -extensions with tame ramification over  $\mathbb{Q}$ . We start by recalling some notation:

We fix an odd prime number  $p$ . Let  $S = \{q_1, \dots, q_n\}$  be a finite set of prime numbers  $\equiv 1 \pmod p$ . Let  $G_S(p)$  denote the Galois group of the maximal pro- $p$ -extension of  $\mathbb{Q}$  unramified outside  $S$ . Then  $\dim_{\mathbb{F}_p} H^1(G_S(p), \mathbb{Z}/p\mathbb{Z}) = \dim_{\mathbb{F}_p} H^2(G_S(p), \mathbb{Z}/p\mathbb{Z}) = n$  and  $G_S(p)$  admits a minimal presentation of *Koch type*, i.e. a presentation

$$1 \rightarrow R \rightarrow F \rightarrow G_S(p) \rightarrow 1$$

where  $F$  is the free pro- $p$ -group on generators  $x_1, \dots, x_n$  and  $R$  is generated by  $\rho_1, \dots, \rho_n$  as a normal subgroup of  $F$  with

$$\rho_i \equiv x_i^{q_i-1} \cdot \prod_{j=1, \dots, n} [x_i, x_j]^{a_{ij}} \pmod{F_3}, \quad i = 1, \dots, n,$$

where  $a_{ij} \in \mathbb{F}_p$ ,  $a_{ii} = 0$ , for  $i \neq j$  we have  $a_{ij} = 0$  if and only if  $q_i$  is a  $p$ -th power modulo  $q_j$  (cf. [Koc02], ch. 11.3) and  $(F_i)_{i \geq 1}$  denotes the descending  $p$ -central series of  $F$ . The numbers  $a_{ij}$  are called *linking numbers* of  $S$  with respect to  $p$ . We denote by  $\Gamma_S(p)$  the associated *linking diagram* of  $S$  with respect to  $p$  (cf. [Lab06]).

We make the following notational convention for all upcoming statements in this section:

**(2.1) Notation.** A prime  $q$  is a prime number  $q \equiv 1 \pmod p$ .

**(2.2) Proposition.** *Let  $S = \{q_1, \dots, q_n\}$  be a finite set of primes. Then there exists a prime  $q_{n+1}$  with the additional edges of  $\Gamma_{S \cup \{q_{n+1}\}}(p)$  arbitrarily prescribed. Precisely if  $d_i, e_i \in \{0, 1\}$ ,  $i = 1, \dots, n$  are given, then there exists a prime  $q_{n+1}$  such that for the linking numbers  $a_{ij}$  of  $S \cup \{q_{n+1}\}$  with respect to  $p$  we have  $a_{i,n+1} = 0$  if and only if  $d_i = 0$  and  $a_{n+1,i} = 0$  if and only if  $e_i = 0$ .*

*Proof.* See [Lab06], Prop. 6.1. □

We can now proof the following

**(2.3) Theorem.**

(i) *Let  $n \geq 3$  and  $S = \{q_1, \dots, q_n\}$  a finite set of primes. Suppose there exist pairwise distinct  $i_1, i_2, i_3 \in \{1, \dots, n\}$  such that for the linking numbers  $a_{ij}$  of  $S$  with respect to  $p$  we have  $a_{i_1 i_2}, a_{i_2 i_3} \neq 0$ . Then there exists a prime  $q_{n+1}$  such that the group  $G_{S \cup \{q_{n+1}\}}(p)$  is mild.*

(ii) *Let  $n \geq 2$  and  $S = \{q_1, \dots, q_n\}$  a finite set of primes. Then there exist two primes  $q_{n+1}, q_{n+2}$  such that the group  $G_{S \cup \{q_{n+1}, q_{n+2}\}}(p)$  is mild.*

(For the definition of a mild pro- $p$ -group we refer to [Lab06].)

*Proof.* (i) We may assume that  $i_1 = 1, i_2 = n, i_3 = 2$ . By (2.2) there is a prime  $q_{n+1}$  such that  $a_{1,n+1} = a_{n,n+1} = a_{n+1,n} = 0$ ,  $a_{i,n+1} \neq 0$  for  $i = 2, \dots, n-1$  and  $a_{n+1,1} \neq 0$ . Now (1.3) (ii) applies and  $G_{S \cup \{q_{n+1}, q_{n+2}\}}(p)$  is mild.

(ii) If  $n \geq 2$  and  $S = \{q_1, \dots, q_n\}$  is an arbitrary set of primes, then by (2.2) we can find a prime  $q_{n+1}$  such that  $a_{1,n+1}, a_{n+1,2}$  are both non-zero. Now the claim follows by applying (i) to the set  $S \cup \{q_{n+1}\}$ . Note that one can also directly show this claim by applying the more general lemma (1.2). □

**(2.4) Remark.** Using arithmetic properties of  $G_S(p)$ , in [Sch06], Th. 2.1 A. Schmidt proofs the following result: Let  $S$  be a finite set of primes and assume there is a subset  $T \subseteq S$  such that  $\Gamma_T(p)$  is a non-singular circuit and for each  $q \in S \setminus T$  there is a directed path in  $\Gamma_S(p)$  starting in  $q$  and ending with a prime in  $T$ . Using (2.2) again, from this one can easily deduce that for a given set  $S = \{q_1, \dots, q_n\}$  two primes  $q_{n+1}, q_{n+2}$  can be found such that we have  $cdG_{S \cup \{q_{n+1}, q_{n+2}\}}(p) = 2$ . Note that in (2.3) we obtain the slightly stronger statement that  $G_{S \cup \{q_{n+1}, q_{n+2}\}}(p)$  is a mild pro- $p$ -group.

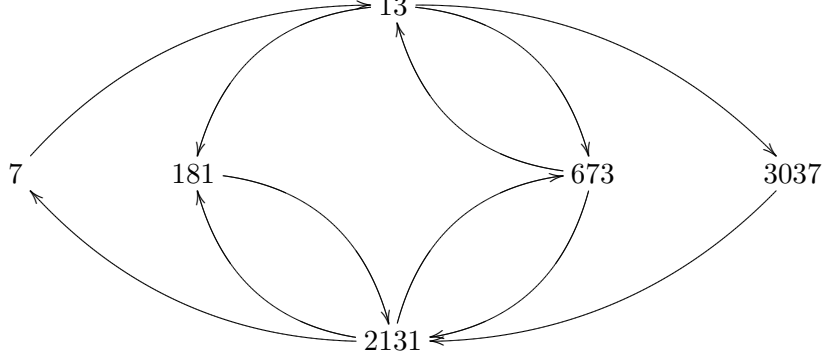
We want to give an example for  $p = 3$ .

**(2.5) Example.** Let  $p = 3$  and  $S = \{q_1, \dots, q_4\}$  where

$$q_1 = 7, \quad q_2 = 181, \quad q_3 = 673, \quad \text{and} \quad q_4 = 3037.$$

The linking diagram of  $S$  with respect to  $p$  has no edges, i.e. we have  $a_{ij} = 0$  for all  $i, j \in \{1, \dots, 4\}$ . In particular we do not know whether  $cd(G_S(3)) = 2$ . Now by (2.3) we can find two primes  $q_5, q_6 \equiv 1 \pmod{3}$  such that  $G_{S \cup \{q_5, q_6\}}(3)$  is mild. First we are looking for a prime  $q_5$  such that the linking numbers satisfy  $a_{15}, a_{52} \neq 0$ . For example, such a prime is given by  $q = 13$ . Finally we'd like to find a prime  $q_6$  such that  $a_{16} = a_{56} = a_{65} = 0$  and  $a_{26}, a_{36}, a_{46}, a_{61} \neq 0$ . We may

choose  $q_6 = 2131$ . More precisely the resulting linking diagram  $\Gamma_{S \cup \{q_5, q_6\}}(3)$  is of the form



and (1.3) applies. Note that the primes  $\{7, 13, 3037, 2131\}$  form a non-singular circuit and since there are edges starting in 181 and 673 respectively and ending in 2131, [Sch06], Th. 2.1 also applies (cf. (2.4)).

### 3 The case $p = 2$

Now we consider the case  $p = 2$ . By quadratic reciprocity clearly proposition (2.2) cannot hold anymore in this case. However we can prove the following analogue of theorem (2.3):

#### (3.1) Theorem.

(i) Let  $n \geq 3$  and  $S = \{q_0, q_1, \dots, q_n\}$  a finite set of odd prime numbers. Suppose that there exist pairwise distinct  $i_0, i_1, i_2, i_3 \in \{0, \dots, n\}$  such that the following holds:

- $q_{i_0}, q_{i_1} \equiv 3 \pmod{4}$ ,
- $q_{i_3} \equiv 1 \pmod{4}$ ,
- $q_{i_3}$  is a square mod  $q_{i_0}$  but is not a square mod  $q_{i_1}$  and  $q_{i_2}$ .

Then there exists a prime number  $q_{n+1} \equiv 1 \pmod{4}$  such that the group  $G_{S \cup \{q_{n+1}\}}(2)$  is a mild pro-2-group.

(ii) Let  $n \geq 2$  and  $S = \{q_0, q_1, \dots, q_n\}$  a finite set of odd prime numbers containing at least two prime numbers  $\equiv 3 \pmod{4}$ . Then there exist two prime numbers  $q_{n+1}, q_{n+2} \equiv 1 \pmod{4}$  such that  $G_{S \cup \{q_{n+1}, q_{n+2}\}}(2)$  is a mild pro-2-group.

(3.2) Corollary. Let  $S$  be a finite set of odd prime numbers. We set  $S_0 := \{q \in S \mid q \equiv 3 \pmod{4}\}$  and

$$\delta := \begin{cases} 3, & \text{if } S = \emptyset \\ 2, & \text{if } S \neq \emptyset, S_0 = \emptyset, \\ 1, & \text{if } \#S_0 = 1, \\ 0, & \text{else.} \end{cases}$$

Then there exist  $k := 2 + \delta$  odd prime numbers  $q_1, \dots, q_k$  such that the group  $G_{S \cup \{q_1, \dots, q_k\}}(2)$  is a mild pro-2-group. In particular if  $S$  is non-empty, there are always four odd primes  $q_1, \dots, q_4$ , such that  $G_{S \cup \{q_1, \dots, q_4\}}(2)$  is mild.

In order to give a proof of (3.1) we need a slight generalization of (1.1) involving quadratic terms. The desired result is the following:

**(3.3) Proposition.** *Let  $G$  be a pro-2-group that admits a presentation*

$$1 \rightarrow R \rightarrow F \rightarrow G \rightarrow 1,$$

where  $F$  is the free pro- $p$ -group on generators  $x_1, \dots, x_d$  and as  $R$  is generated by  $\rho_1, \dots, \rho_r$  as a normal subgroup of  $F$  with

$$\rho_i \equiv \prod_{j=1}^d (x_j^2)^{a_{ij}} \cdot \prod_{1 \leq k < l \leq d} [x_k, x_l]^{a_{ikl}} \pmod{F_3}, \quad i = 1, \dots, r,$$

where  $a_{ij}, a_{ikl} \in \mathbb{F}_2$  and  $(F_i)_{i \geq 1}$  denotes the lower 2-central-series of  $F$ . Moreover, suppose that there is a natural number  $a$  satisfying  $1 \leq a < d$  such that the following conditions hold:

- (i)  $a_{ij} = 0$  for  $a < j \leq d$  and all  $1 \leq i \leq r$ ,
- (ii)  $a_{ikl} = 0$  for  $a < k < l \leq d$  and all  $i = 1, \dots, r$ ,
- (iii) the  $r \times a(d - a)$ -matrix

$$(a_{ikl})_{i,(k,l)}, \quad 1 \leq i \leq r, \quad 1 \leq k \leq a < l \leq d$$

has rank  $r$ .

Then  $G$  is a mild pro-2-group with generator rank  $d$  and relation rank  $r$ . In particular we have  $cd G \leq 2$ .

*Proof.* This is a direct reformulation of [LM09], Th. 1.1. In order to see this, first note that  $\dim_{\mathbb{F}_p} H^1(G) = d$  since  $R \subseteq F_2$ . Now let  $\chi_1, \dots, \chi_d \in H^1(G)$  be the corresponding dual basis of the images of  $x_1, \dots, x_d$  in  $G^{ab}/p$ . Then we have  $a_{ij} = \bar{\rho}_i(\chi_j \cup \chi_j)$  and  $a_{ikl} = \bar{\rho}_i(\chi_k \cup \chi_l)$ . Here  $\bar{\rho}_i$  denotes the image of  $\rho_i$  under the map

$$R \longrightarrow R/R^2[R, F] \xrightarrow{\psi} H^2(G)^*$$

where  $\psi$  is the inverse map of the dual of the transgression isomorphism  $\text{tg}: H^1(R/R^2[R, F]) \xrightarrow{\sim} H^2(G)$  (cf. [NSW08], Th. 3.9.13). Note that by condition (iii) we have  $\dim_{\mathbb{F}_p} H^2(G) = \dim_{\mathbb{F}_p} (R/R^2[R, F]) = r$ , so  $\{\rho_i, i = 1, \dots, r\}$  is a minimal system of defining relations of  $G$ . Let  $U, V$  be the subspaces of  $H^1(G)$  generated by  $\chi_1, \dots, \chi_a$  and  $\chi_{a+1}, \dots, \chi_d$  respectively. Then by conditions (i) and (ii), the cup product is trivial on  $V \times V$  and maps  $U \times V$  surjectively onto  $H^2(G)$  by condition (iii). Thus  $G$  is mild by [LM09], Th. 1.1. (A proof using a different approach from that in [LM09] can also be found in [For10], Cor. 6.5.)  $\square$

*Proof of (3.1).* For the proof of (i) we may assume that  $i_0 = 0$ ,  $i_1 = 1$ ,  $i_2 = 2$  and  $i_3 = n$ . Now we can choose a prime number  $q_{n+1}$  such that the following holds:

- $q_{n+1} \equiv 1 \pmod{4}$ ,
- $q_{n+1}$  is not a square mod  $q_0$ ,
- $q_{n+1}$  is a square mod  $q_1$ ,
- $q_{n+1}$  is not a square mod  $q_i$ ,  $i = 2, \dots, n$ ,
- $q_{n+1}$  is a square mod  $q_n$ .

Let  $G := G_{S \cup \{q_{n+1}\}}(2)$ . Since  $S$  contains a prime number  $\equiv 3 \pmod{4}$ , the group  $\mathbb{B}_S$  and hence also the group  $\mathbb{B}_{S \cup \{q_{n+1}\}}$  vanishes and  $G$  has the presentation  $G = \langle x_0, \dots, x_{n+1} \mid \rho_0, \dots, \rho_{n+1}, \rho \rangle$ , where

$$\rho_i \equiv (x_i^2)^{a_i} \prod_{j=0}^{n+1} [x_i, x_j]^{a'_{ij}} \pmod{F''}, \quad i = 0, \dots, n+1,$$

$$\rho \equiv \prod_{i=0}^{n+1} x_i^{a_i} \pmod{F'},$$

with  $a_i, a'_{ij} \in \mathbb{F}_2$  such that  $a_i = 0$  if and only if  $q_i \equiv 1 \pmod{4}$  and  $a'_{ij} = 0$  if and only if  $q_i$  is a square mod  $q_j$ . Thus since  $q_0 \equiv 3 \pmod{4}$ , we may omit the generator  $x_0$ . Furthermore, we may omit the relation  $\rho_0$  and obtain a minimal presentation  $G = F/R = \langle x_1, \dots, x_{n+1} \mid \rho'_1, \dots, \rho'_{n+1} \rangle$  where

$$\rho_i \equiv (x_i^2)^{a_i} \prod_{j=1}^{n+2} [x_i, x_j]^{a_{ij}} \pmod{F''}, \quad i = 1, \dots, n+2,$$

with

$$a_{ij} = a'_{ij} + a'_{i0}a_j, \quad i, j = 1, \dots, n+2$$

(cf. [Koc02], Ex. 11.12). By the assumptions made and by construction of  $q_{n+1}$  we have  $a_{1,n} = a_{n,1} = a_{2,n} = a_{n,2} = 1$ ,  $a_{1,n+1} = 0$  and  $a_{i,n+1} = 1$  for all  $i = 2, \dots, n-1$ . Furthermore  $a_{n+1,1} = 1$  and for  $i = 2, \dots, n-1$  we have  $a_{n+1,i} = 0$  if and only if  $q_i \equiv 3 \pmod{4}$ . We will now apply (3.3) with  $a = n-1$ . Since  $q_n \equiv q_{n+1} \equiv 1 \pmod{4}$ , we have  $a_n = a_{n+1} = 0$  and hence condition (i) holds. Furthermore we have  $a_{n,n+1} = a_{n+1,n} = 0$ , hence also condition (ii) is fulfilled. Finally the  $(n+1) \times 2(n-1)$ -matrix of condition (iii) is of the form

$$\begin{pmatrix} & [x_1, x_n] & [x_2, x_n] & \cdots & [x_{n-1}, x_n] & [x_1, x_{n+1}] & [x_2, x_{n+1}] & \cdots & [x_{n-1}, x_{n+1}] \\ \rho_1 & 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \rho_2 & 0 & 1 & \cdots & 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & \ddots & & & & \ddots & \\ \rho_{n-1} & 0 & 0 & \cdots & a_{n-1,n} & 0 & 0 & \cdots & 1 \\ \rho_n & 1 & 1 & \cdots & a_{n,n-1} & 0 & 0 & \cdots & 0 \\ \rho_{n+1} & 0 & 0 & \cdots & 0 & 1 & a_{n+1,2} & \cdots & a_{n+1,n-1} \end{pmatrix}$$

and clearly has rank  $n + 1$ . Thus we obtain (i).

For the proof of (ii) let  $n \geq 2$  and  $S = \{q_0, q_1, \dots, q_n\}$  a finite set of odd prime numbers where we may assume  $q_0 \equiv q_1 \equiv 3 \pmod{4}$ . Then we can find a prime  $q_{n+1} \equiv 1 \pmod{4}$  such that  $q_{n+1}$  is a square mod  $q_0$  but is not a square mod  $q_1$  and  $q_2$ . Now the claim follows by applying (i) to the set  $S \cup \{q_{n+1}\}$ .  $\square$

## References

- [For10] Patrick Forré. Strongly free sequences and pro- $p$ -groups of cohomological dimension 2. *to appear in J. Reine u. Angew. Mathematik*, 2010.
- [Koc02] Helmut Koch. *Galois Theory of  $p$ -Extensions*. Springer, 2002.
- [Lab06] John Labute. Mild Pro- $p$ -Groups and Galois Groups of  $p$ -Extensions of  $\mathbb{Q}$ . *J. Reine u. Angew. Mathematik*, 596, 2006.
- [LM09] John Labute, and Ján Mináč. Mild pro-2-groups and 2-extensions of  $\mathbb{Q}$  with restricted ramification. *preprint*, 2009.
- [NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*. second edition. Springer, 2008.
- [Sch06] Alexander Schmidt. Circular sets of prime numbers and  $p$ -extensions of the rationals. *J. Reine u. Angew. Mathematik*, 596, 2006.
- [Sch07] Alexander Schmidt. Rings of integers of type  $k(\pi, 1)$ . *Doc. Math.*, 12, 2007.
- [Sch08] Alexander Schmidt. Über Pro- $p$ -Fundamentalgruppen markierter arithmetischer Kurven. *to appear in J. Reine u. Angew. Mathematik*, 2008.