

# LIFTING PROPERTY FOR FINITE GROUPS

CHANDRASHEKHAR B. KHARE AND ALEXANDER MERKURJEV

ABSTRACT. We classify all finite groups that have lifting property of mod  $p$  representations to mod  $p^2$  representations for all prime  $p$ .

## 1. INTRODUCTION

Let  $R$  be a commutative local ring with maximal ideal  $M$  satisfying  $M^2 = 0$  and residue field  $k$  of positive characteristic  $p$ . For example, one can take  $R = \mathbb{Z}/p^2\mathbb{Z}$  with  $k = \mathbb{F}_p$ , or more generally, for a field  $k$  of characteristic  $p > 0$ ,  $R = W_2(k)$  the ring of the  $p$ -typical length 2 Witt vectors of  $k$ .

The group homomorphism  $\mathrm{GL}_n(R) \rightarrow \mathrm{GL}_n(k)$  is surjective for every  $n$  and its kernel  $A_n(R)$  is an abelian group of exponent  $p$ .

Let  $G$  be a finite group. The following two statements are equivalent:

1. Every group homomorphism  $G \rightarrow \mathrm{GL}_n(k)$  for any  $n > 0$  extends to a group homomorphism  $G \rightarrow \mathrm{GL}_n(R)$ .
2. Every continuous  $k[G]$ -module  $M$  of finite  $k$ -dimension lifts to a  $R[G]$ -module  $N$ , that is  $N$  is free as an  $R$ -module, and  $M \simeq N \otimes_R k$  as  $k[G]$ -modules.

If these two conditions hold for all  $R$  (respectively for  $R = \mathbb{Z}/p^2\mathbb{Z}$ , where  $p$  is a prime integer) we say that  $G$  is *liftable* (respectively,  *$p$ -liftable*). The theorem below shows it to be a very restrictive property for finite groups.

**Theorem 1.1.** *Let  $G$  be a finite group. The following are equivalent:*

- (1)  *$G$  is liftable.*
- (2)  *$G$  is  $p$ -liftable for every prime  $p$ .*
- (3)  *$G$  is isomorphic to one of the following groups:  $C_{2^n}$ ,  $C_3 \times C_{2^n}$  or  $C_3 \rtimes C_{2^n}$ . (The semidirect product is taken with respect the only nontrivial action of  $C_{2^n}$  on  $C_3$ .)*

We say a few words about a context for our result, and earlier related work. The modularity conjecture of Serre [5], proved in [3], asserts that odd, irreducible, 2-dimensional mod  $p$  representations  $\rho$  of  $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ ,

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathrm{GL}_2(k),$$

with  $k$  a finite field, arise from newforms, and in particular lift to characteristic 0. This has led to a lot of work about lifting mod  $p$  representations of absolute Galois groups of local and global fields. For absolute Galois groups of fields, lifting questions have been studied in [4]. The lifting property for finite groups was first studied in [2]: this is almost complementary to the case of absolute Galois groups as, by a theorem of Artin and Schreier, the only finite groups that are absolute Galois groups are 1 and  $C_2$ .

More precisely, in [2],  $G$  is said to be *liftable* (respectively, *p-liftable*), if any homomorphism  $f : G \rightarrow \mathrm{GL}_n(k)$  with  $k$  a finite field (respectively, a finite extension of  $\mathbb{F}_p$ ) lifts to  $\mathrm{GL}_n(W_2(k))$ . The definition of liftable in [2] is *a priori* weaker than our definition, and of *p-liftable* in [2] is *a priori* stronger than our definition. Under either of the definitions, it is easy to see that a finite group  $G$  is *p-liftable* if and only if a Sylow  $p$ -subgroup of  $G$  is *p-liftable*. From this and the equivalence of (1) and (2) of the above theorem, it follows that the definitions of liftable and *p-liftable* here and in loc. cit. are equivalent. Thus the theorem above sharpens Propositions 1.3 and 1.4 of [2], which left open whether the quaternion group  $Q_8$  is liftable: we show in Proposition 4.2 below that  $Q_8$  is not 2-liftable.

## 2. PRELIMINARIES

Let  $R$  be a commutative local ring with maximal ideal  $M$  satisfying  $M^2 = 0$  and residue field  $k$  of characteristic  $p > 0$ . We have an exact sequence

$$(2.1) \quad 1 \rightarrow A_n(R) \rightarrow \mathrm{GL}_n(R) \rightarrow \mathrm{GL}_n(k) \rightarrow 1,$$

where  $A_n(R)$  is an abelian group of exponent  $p$  with a natural structure of a  $\mathrm{GL}_n(k)$ -module.

If  $R = \mathbb{Z}/p^2\mathbb{Z}$  for a prime  $p$ , the group  $A_n(R)$  is identified with the (additive) group  $M_n(\mathbb{F}_p)$  of all  $n \times n$  matrices over  $\mathbb{F}_p$  via  $1 + px \mapsto \bar{x}$ , the residue of  $x$  modulo  $p$ . The group  $\mathrm{GL}_n(\mathbb{F}_p)$  acts on  $M_n(\mathbb{F}_p)$  by conjugation.

**Lemma 2.2.** *Let  $H$  be a finite group and  $X$  and  $Y$  two finite dimensional  $k[H]$ -modules. Then  $X \oplus Y$  is *p-liftable* if and only if  $X$  and  $Y$  are *p-liftable*.*

*Proof.* Let  $n = \dim(X)$ ,  $m = \dim(Y)$ ,  $R = \mathbb{Z}/p^2\mathbb{Z}$  and  $k = \mathbb{F}_p$ . Consider the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & M_{n+m}(k) & \longrightarrow & \mathrm{GL}_{n+m}(R) & \xrightarrow{\gamma} & \mathrm{GL}_{n+m}(k) \longrightarrow 1 \\ & & \parallel & & \uparrow & & \uparrow \alpha \\ 0 & \longrightarrow & M_{n+m}(k) & \longrightarrow & E & \longrightarrow & \mathrm{GL}_n(k) \times \mathrm{GL}_m(k) \longrightarrow 1 \\ & & \beta \downarrow & & \delta \downarrow & & \parallel \\ 0 & \longrightarrow & M_n(k) \oplus M_m(k) & \longrightarrow & \mathrm{GL}_n(R) \times \mathrm{GL}_m(R) & \longrightarrow & \mathrm{GL}_n(k) \times \mathrm{GL}_m(k) \longrightarrow 1, \end{array}$$

where

$$\alpha(S, T) = \begin{pmatrix} S & 0 \\ 0 & T \end{pmatrix}, \quad \beta \begin{pmatrix} A & B \\ C & D \end{pmatrix} = (A, D),$$

$E$  is the inverse image under  $\gamma$  of the image of  $\alpha$ . It consists of all invertible matrices of the form  $\begin{pmatrix} A & pB \\ pC & D \end{pmatrix}$  such that  $A, B, C, D$  are matrices over  $R$ . The map  $\delta$  is a homomorphism taking  $\begin{pmatrix} A & pB \\ pC & D \end{pmatrix}$  to  $(A, D)$ .

Let  $\varepsilon : H \rightarrow \mathrm{GL}_n(k) \times \mathrm{GL}_m(k)$  be a homomorphism afforded by  $X$  and  $Y$ . If  $X \oplus Y$  is *p-liftable*, then there is a homomorphism  $\eta : H \rightarrow \mathrm{GL}_{n+m}(R)$  such that  $\gamma\eta = \alpha\varepsilon$ . It follows that the image of  $\eta$  is contained in  $E$ . Composing  $\eta$  with  $\delta$ , we get a lifting  $H \rightarrow \mathrm{GL}_n(R) \times \mathrm{GL}_m(R)$  of  $\varepsilon$ , hence  $X$  and  $Y$  are *p-liftable*.  $\square$

**Proposition 2.3.** [2, Lemma 2.3] *Let  $G$  be a finite group and  $H \subset G$  a subgroup. If  $G$  is  $p$ -liftable, then so is  $H$ .*

*Proof.* Let  $X$  be a  $k[H]$ -module. Consider the induced  $k[G]$ -module  $Z := k[G] \otimes_H X$ . As a  $k[H]$ -module,  $Z$  contains  $X$  as a direct summand:  $Z = X \oplus Y$  for a  $k[H]$ -module  $Y$ . Since  $Z$  is  $p$ -liftable as a  $k[G]$ -module, it is  $p$ -liftable as a  $k[H]$ -module. By Lemma 2.2, the  $k[H]$ -module  $X$  is  $p$ -liftable, hence  $H$  is  $p$ -liftable.  $\square$

**Proposition 2.4.** [2, Lemma 2.2] *If every Sylow subgroup of a finite group  $G$  is liftable, then  $G$  is liftable.*

*Proof.* Let  $R$  be a commutative local ring with residue field  $k$  of characteristic  $p > 0$  as above. Let  $f : G \rightarrow \mathrm{GL}_n(k)$  be a group homomorphism. The restriction  $h$  of  $f$  to  $G_p$  lifts to a homomorphism  $G_p \rightarrow \mathrm{GL}_n(R)$ , that is the pullback of the sequence (2.1) with respect to  $h$  is splits. Equivalently, the image of the class of (2.1) under the pullback map  $h^* : H^2(\mathrm{GL}_n(k), A_n(R)) \rightarrow H^2(G_p, A_n(R))$  is zero. Since  $A_n(R)$  is  $p$ -torsion and  $[G : G_p]$  is prime to  $p$ , the restriction homomorphism  $H^2(G, A_n(R)) \rightarrow H^2(G_p, A_n(R))$  is injective. Hence the image of the class of (2.1) under the pullback map  $f^* : H^2(\mathrm{GL}_n(k), A_n(R)) \rightarrow H^2(G, A_n(R))$  is also zero, that is  $f$  lifts to a homomorphism  $G \rightarrow \mathrm{GL}_n(R)$ .  $\square$

### 3. CYCLIC GROUPS

Set  $R = \mathbb{Z}/p^2\mathbb{Z}$  and  $k = \mathbb{F}_p$  for a prime  $p$ . Let  $G$  be a finite group and let  $f$  and  $h$  be two elements in  $k[G]$  such that  $fh = 0$ . Choose their lifts  $\hat{f}$  and  $\hat{h}$  in  $R[G]$ . Then  $\hat{f}\hat{h} = pu$  for some  $u \in R[G]$  that is unique modulo  $pR[G]$ . If  $\hat{f} + pv$  and  $\hat{h} + pw$  are two other lifts, then

$$(\hat{f} + pv)(\hat{h} + pw) = p(u + \hat{f}w + v\hat{h}).$$

Thus, the residue of  $u$  is uniquely determined in the quotient group  $k[G]/(fk[G] + k[G]h)$ . We denote this class by  $\theta(f, h)$ .

**Proposition 3.1.** *Let  $G$  be a  $p$ -liftable group. Then for every pair  $f$  and  $h$  of elements in  $k[G]$  such that  $fh = 0$  we have  $\theta(f, h) = 0$ .*

*Proof.* By assumption, the left  $k[G]$ -module  $X := k[G]/I$ , where  $I = k[G]h$ , admits an  $R[G]$ -lifting  $\hat{X}$ . The surjective composition  $R[G] \rightarrow k[G] \rightarrow X$  lifts to a homomorphism of left  $R[G]$ -modules  $R[G] \rightarrow \hat{X}$  that is surjective by Nakayama. Let  $\hat{I}$  be its kernel.

We claim that the left ideal  $\hat{I} \subset R[G]$  is a lifting of  $I$ . Indeed, since  $\hat{X}$  is free as an  $R$ -module, the exact sequence  $0 \rightarrow \hat{I} \rightarrow R[G] \rightarrow \hat{X} \rightarrow 0$  is split as a sequence of  $R$ -modules. It follows that  $\hat{I}$  is free as an  $R$ -module and  $I \simeq \hat{I}/p\hat{I}$ . This proves the claim.

Let  $\hat{h} \in \hat{I}$  be a lift of  $h$ . By Nakayama,  $\hat{h}$  generates  $\hat{I}$ , that is  $\hat{I} = R[G]\hat{h}$ .

Now the map  $k[G] \xrightarrow{r(h)} I$  of right multiplication by  $h$  has a lifting  $R[G] \xrightarrow{r(\hat{h})} \hat{I}$ . Therefore, the kernel  $\hat{J}$  of  $r(\hat{h})$  is a lifting of the kernel  $J$  of  $r(h)$ . In particular, the map  $\hat{J} \rightarrow J$  is surjective and we can choose a lift  $\hat{f} \in \hat{J}$  of  $f$ . Since  $\hat{f}\hat{h} = 0$ , we have  $\theta(f, h) = 0$ .  $\square$

**Corollary 3.2.** [2, Proposition 2.8] *Let  $p > 2$  be a prime and  $n$  a positive integer such that  $n \geq 2$  if  $p = 3$ . Then a cyclic group of order  $p^n$  is not  $p$ -liftable.*

*Proof.* Let  $\sigma$  be a generator of a cyclic group  $G$  order  $p^n$ . Let  $m := p^{n-1} + 1$ . Consider the elements  $f = (1 - \sigma)^m$  and  $h = (1 - \sigma)^{p^n - m}$  in  $k[G]$ . Since  $(1 - \sigma)^{p^n} = 0$ , we have  $fh = 0$ . We will prove that  $\theta(f, h) \neq 0$  and hence  $G$  is not  $p$ -liftable.

Write  $k[G]$  as the quotient of the polynomial ring  $k[t]$  by the ideal generated by  $(1 - t)^{p^n}$ . Since  $m \leq p^n - m$  by assumption, the class  $\theta(f, h)$  is represented by  $Q(\sigma)$  in

$$k[G]/(1 - \sigma)^m = k[t]/(1 - t)^m,$$

where  $Q$  is the integer polynomial  $[(1 - t)^{p^n} - (1 - t^{p^n})]/p$ . Setting  $s := 1 - t$  we have  $Q = [(1 - s)^{p^n} - (1 - s^{p^n})]/p$ . The  $s^{m-1}$ -coefficient of  $Q$  is equal to  $\binom{p^n}{p^{n-1}}/p$  and hence is not divisible by  $p$ . It follows that the class of  $Q(\sigma)$  in  $k[G]/(1 - \sigma)^m = k[s]/(s^m)$  is nontrivial, hence  $\theta(f, h) \neq 0$ .  $\square$

**Proposition 3.3.** *Let  $G$  be a cyclic group of order  $p^n$ . Suppose that for every  $i = 1, 2, \dots, p^n$  there is a monic divisor  $P_i$  of the polynomial  $t^{p^n} - 1$  in  $\mathbb{Z}[t]$  such that  $P_i \equiv (t - 1)^i$  modulo  $p$ . Then  $G$  is liftable.*

*Proof.* Let  $R$  be a commutative local ring with maximal ideal  $M$  satisfying  $M^2 = 0$  and residue field  $k$  of positive characteristic  $p$ . Choose a generator  $\sigma$  of  $G$ . Every finite dimensional  $k[G]$ -module is a direct sum of modules of the form  $M_i = k[G]/(\sigma - 1)^i$  for  $i = 1, 2, \dots, p^n$ , so it suffices to show that every  $M_i$  lifts to an  $R[G]$ -module. Indeed,  $M_i$  lifts to the  $R[G]$ -module  $R[G]/(P_i(\sigma))$ .  $\square$

**Corollary 3.4.** [2, Propositions 2.6 and 2.7] *Every cyclic group of order 3 and  $2^n$  is liftable.*

*Proof.* If  $p = 3$ , the polynomial  $(t - 1)^2$  lifts to the divisor  $t^2 + t + 1$  of  $t^3 - 1$  in  $\mathbb{Z}[t]$ . In the case  $p = 2$ , let  $i = 1, 2, \dots, 2^n$ . Write  $i$  in base 2:  $i = 2^{s_0} + 2^{s_1} + \dots + 2^{s_m}$ , where  $0 \leq s_0 < s_1 < \dots < s_m$ . The polynomial  $t^{2^n} - 1$  is the product  $(t - 1)Q_0Q_1 \cdots Q_{n-1}$  in  $\mathbb{Z}[t]$ , where  $Q_j = t^{2^j} + 1$ . Therefore, we can take  $P_i = Q_{s_0}Q_{s_1} \cdots Q_{s_m}$  for the lift of  $(t - 1)^i$  modulo 2 in  $\mathbb{Z}[t]$ .  $\square$

#### 4. $C_2 \times C_2$ AND $Q_8$ ARE NOT 2-LIFTABLE

Set  $S = M_2(\mathbb{F}_2)$ ,  $T = M_2(\mathbb{Z}/4\mathbb{Z})$ , and

$$x = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \in S, \quad y = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \in T.$$

**Proposition 4.1.** *The Klein group  $C_2 \times C_2$  is not 2-liftable.*

*Proof.* Consider the following 4-dimensional representation of  $C_2 \times C_2 = \langle \sigma, \tau \rangle$ :

$$C_2 \times C_2 \rightarrow \mathrm{GL}_2(S) = \mathrm{GL}_4(\mathbb{F}_2), \quad \sigma \mapsto \begin{bmatrix} 1_S & 1_S \\ 0_S & 1_S \end{bmatrix}, \quad \tau \mapsto \begin{bmatrix} 1_S & x \\ 0_S & 1_S \end{bmatrix}.$$

We claim that this representation is not liftable modulo 4. Suppose it is liftable:

$$\sigma \mapsto A \cdot \begin{bmatrix} 1_T & 1_T \\ 0_T & 1_T \end{bmatrix}, \quad \tau \mapsto B \cdot \begin{bmatrix} 1_T & y \\ 0_T & 1_T \end{bmatrix},$$

where  $A$  and  $B$  are in the kernel of  $\mathrm{GL}_2(T) \rightarrow \mathrm{GL}_2(S)$ . We identify this kernel with  $M_2(S)$  (written additively). The group  $\mathrm{GL}_2(S)$  acts on  $M_2(S)$  by conjugation. Let  $a$  and  $b$  be

two matrices in  $M_2(S)$  corresponding to  $A$  and  $B$ , respectively, under this identification. The relations  $\sigma^2 = 1 = \tau^2$  and  $\sigma\tau = \tau\sigma$  yield

$$a + \sigma(a) = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad b + \tau(b) = \begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix}, \quad a + \tau(a) = b + \sigma(b).$$

in  $M_2(S)$ . Writing  $a = (a_{ij})$  and  $b = (b_{ij})$  with  $a_{ij}$  and  $b_{ij}$  in  $S$ , we have the following relations in  $S$ :

$$\begin{aligned} a_{21} &= b_{21} = 0, \\ a_{11} + a_{22} &= 1, \\ b_{11}x + xb_{22} &= x, \\ a_{11}x + xa_{22} &= b_{11} + b_{22}. \end{aligned}$$

Consider the subspace

$$V := [x, S] = \{xs + sx, s \in S\} \subset S.$$

Note that  $xV = V = x^{-1}V$  since  $x(xs + sx) = x(xs) + (xs)x$ . We then have the following equalities in  $S/V$ :

$$1 = x^{-1}(b_{11}x + xb_{22}) = b_{11} + b_{22} = a_{11}x + xa_{22} = x(a_{11} + a_{22}) = x,$$

hence  $x + 1 \in V$ , a contradiction since  $\text{Trace}(x + 1) \neq 0$ .  $\square$

**Proposition 4.2.** *The quaternion group  $Q_8$  is not 2-liftable.*

*Proof.* Note the relation  $x^2 + x + 1 = 0$  in  $S$ .

Consider the quaternion group  $Q_8 = \langle \sigma, \tau \mid \sigma^2 = \tau^2, \sigma^4 = 1, \tau\sigma = \sigma^3\tau \rangle$  and its 6-dimensional representation over  $\mathbb{F}_2$  given by

$$Q_8 \rightarrow \text{GL}_3(S) = \text{GL}_6(\mathbb{F}_2), \quad \sigma \mapsto j = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}, \quad \tau \mapsto k = \begin{bmatrix} 0 & x & 1 \\ x & x^2 & x \\ x^2 & 0 & x \end{bmatrix}.$$

We claim that this representation is not liftable modulo 4. Suppose it is liftable:

$$\sigma \mapsto J + 2A, \quad \tau \mapsto K + 2B,$$

where  $A$  and  $B$  are two  $3 \times 3$  matrices over  $T$  and

$$J = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}, \quad K = \begin{bmatrix} 0 & y & 1 \\ y & y^2 & y \\ y^2 & 0 & y \end{bmatrix}$$

in  $M_3(T)$ . The equality  $\sigma^2 = \tau^2$  yields  $(J + 2A)^2 = (K + 2B)^2$  in  $M_3(T)$ . Since

$$J^2 = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 2 \\ 1 & 1 & 2 \end{bmatrix}, \quad K^2 = \begin{bmatrix} 2y^2 & 1 & 1 \\ 2 & 1 & 0 \\ 1 & 1 & 2y^2 \end{bmatrix},$$

we get an equality

$$2(JA + AJ) = \begin{bmatrix} 2y^2 & 0 & 0 \\ 2 & 0 & 2 \\ 0 & 0 & 2y \end{bmatrix} + 2(KB + BK)$$

in  $M_3(T)$ , hence

$$(4.3) \quad ja + aj = \begin{bmatrix} x^2 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & x \end{bmatrix} + (kb + bk)$$

in  $M_3(S)$ , where  $a$  and  $b = (b_{ij})$  in  $M_3(S)$  are the residues modulo 2 of  $A$  and  $B$ , respectively. A computation shows that the trace in  $S$  of the  $3 \times 3$  matrix  $ja + aj$  is zero and the trace of  $kb + bk$  is equal to

$$[x, b_{12}] + [x, b_{21}] + [x, b_{32}] + [x, b_{33}] + [x^2, b_{13}] + [x^2, b_{22}].$$

This is contained in  $V = [x, S]$  since  $[x^2, c] = [x + 1, c] = [x, c] \in V$ . It follows from (4.3) that  $1 = x^2 + x \in V$ , hence  $x \in xV = V$ , a contradiction since  $\text{Trace}(x) \neq 0$ .  $\square$

## 5. $C_3 \times C_3$ IS NOT 3-LIFTABLE

**Proposition 5.1.** [4, Claim 5.4] *The group  $C_3 \times C_3$  is not 3-liftable.*

*Proof.* For every  $1 \leq i < j \leq 3$ , let  $e_{ij}$  be the matrix with 1 on the  $(ij)$ -entry, and 0 everywhere else and set  $\sigma_{ij} := 1 + e_{ij}$ . Let  $C_3 \times C_3 \rightarrow \text{GL}_3(\mathbb{F}_3)$  be a 3-dimensional representation taking generators to  $\sigma_{12}$  and  $\sigma_{13}$ , respectively. If this homomorphism lifts to  $\text{GL}_3(\mathbb{Z}/9\mathbb{Z})$ , there should exist two elements  $\rho, \tau \in \text{GL}_3(\mathbb{Z}/9\mathbb{Z})$  such that  $\rho^3 = \tau^3 = [\rho, \tau] = 1$ ,  $\rho$  reduces to  $\sigma_{12}$  modulo 3, and  $\tau$  reduces to  $\sigma_{13}$  modulo 3. We now prove that such  $\rho$  and  $\tau$  do not exist. We have  $\rho = A\sigma_{12}$  and  $\tau = B\sigma_{13}$  in  $\text{GL}_3(\mathbb{Z}/9\mathbb{Z})$ , for some  $A, B \in A_3(\mathbb{Z}/9\mathbb{Z})$ . Identifying  $A_3(\mathbb{Z}/9\mathbb{Z})$  with the additively written group  $M_3(\mathbb{F}_3)$ , we rewrite the relations  $\rho^3 = \tau^3 = [\rho, \tau] = 1$  in the form

$$N_{12}(a) = -e_{12}, \quad N_{13}(b) = -e_{13} \quad \text{and} \quad (\sigma_{13} - 1)a = (\sigma_{12} - 1)b$$

in  $M_3(\mathbb{F}_3)$ , where  $a, b \in M_3(\mathbb{F}_3)$  and  $N_{ij} := 1 + \sigma_{ij} + \sigma_{ij}^2$ . Letting  $a = (a_{ij})$ , a matrix computation shows

$$N_{12}(a) = \begin{pmatrix} 0 & a_{21} & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad -(\sigma_{13} - 1)a + (\sigma_{12} - 1)b = \begin{pmatrix} * & * & * \\ * & * & a_{21} \\ * & * & * \end{pmatrix}.$$

Thus  $-1 = a_{21} = 0$ , a contradiction.  $\square$

## 6. PROOF OF THEOREM 1.1

*Proof.* (1)  $\Rightarrow$  (2) is trivial.

(2)  $\Rightarrow$  (3): Let  $G$  be a  $p$ -liftable finite group for every prime  $p$ . By Proposition 2.3, a Sylow  $p$ -subgroup  $G_p$  of  $G$  is  $p$ -liftable for all  $p$ . If  $p > 3$  then  $G_p = 1$  since otherwise  $G_p$  would contain a cyclic group of order  $p$  which is not  $p$ -liftable by Corollary 3.2. This contradicts Proposition 2.3.

The subgroup  $G_3$  has order at most 3. Indeed, if  $|G_3| > 3$ , then  $G_3$  contains a subgroup of order 9, hence  $G_3$  contains either  $C_3 \times C_3$  or  $C_9$ . The latter two groups are not 3-liftable by Proposition 5.1 and Corollary 3.2. Again, we get a contradiction by Proposition 2.3.

We claim that every abelian subgroup  $H \subset G_2$  (which is 2-liftable by Proposition 2.3) is cyclic. Indeed, if  $H$  were not cyclic, it would contain a subgroup  $C_2 \times C_2$ . This contradicts Propositions 4.1 and 2.3. The claim is proved.

By [1, Chapter IV, Corollary 6.6], a 2-group with all abelian subgroups cyclic is either cyclic or generalized quaternion group  $Q_{2^n}$ ,  $n \geq 3$ , generated by  $\sigma$  and  $\tau$  subject to the relations  $\sigma^{2^{n-2}} = \tau^2$ ,  $\tau^4 = 1$  and  $\tau\sigma\tau^{-1} = \sigma^{-1}$ . The subgroup of  $Q_{2^n}$  generated by  $\sigma^{2^{n-3}}$  and  $\tau$  is isomorphic to  $Q_8$  which is not 2-liftable by Proposition 4.2. It follows from Proposition 2.3 that  $G_2$  is cyclic. Thus, we proved that all Sylow subgroups of  $G$  are cyclic and the order of  $G$  divides  $3 \cdot 2^n$ . It follows from the proof of [2, Proposition 2.4] that  $G$  is one of the groups in the list (3).

(3)  $\Rightarrow$  (1): By Proposition 2.4 it suffices to prove that all Sylow subgroups  $G_p$  of  $G$  are liftable. The group  $G_p$  is either trivial or cyclic of order 3 or  $2^n$ . By Corollary 3.4,  $G_p$  is liftable.  $\square$

## REFERENCES

- [1] ADEM, A., AND MILGRAM, R. J. *Cohomology of finite groups*, vol. 309 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1994.
- [2] KHARE, C. B., AND LARSEN, M. Liftable groups, negligible cohomology and Heisenberg representations. In *Arithmetic geometry*, vol. 41 of *Tata Inst. Fundam. Res. Stud. Math.* [2024], pp. 315–344.
- [3] KHARE, C. B., AND WINTENBERGER, J.-P. Serre’s modularity conjecture. I, *Invent. Math.* 178, 3 (2009), 485–504.
- [4] MERKURJEV, A., AND SCAVIA, F. Galois representations modulo  $p$  that do not lift modulo  $p^2$ . *J. Amer. Math. Soc.* 39, 1 (2026), 73–94.
- [5] SERRE J.-P. Sur les représentations modulaires de degré 2 de  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ . *Duke Math. J.* 54, 1 (1987), 179–230.

Email address: shekhar84112@gmail.com

Email address: merkurev@math.ucla.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, LOS ANGELES, CA 90095-1555, USA