

SYLOW-CONJUGATE NUMBER FIELDS

ALEXANDER LUBOTZKY AND DANNY NEFTIN

Dedicated to Moshe Jarden

ABSTRACT. By a classical result of Neukirch and Uchida, a number field K is determined by the structure of its absolute Galois group $\text{Gal}(K)$. We show that K is not determined by the structure of the Sylow subgroups of $\text{Gal}(K)$, answering a question raised by Florian Pop.

1. INTRODUCTION

Let $K \subseteq \overline{\mathbb{Q}}$ be a number field, i.e., a finite extension of the field of rational numbers \mathbb{Q} embedded in a fixed algebraic closure $\overline{\mathbb{Q}}$ of \mathbb{Q} . The seminal results of Neukirch and Uchida [9, 14] assert that K is determined by the structure of its absolute Galois group $\text{Gal}(K) = \text{Gal}(\overline{\mathbb{Q}}/K)$. Namely, if L is a number field with $\text{Gal}(L)$ isomorphic to $\text{Gal}(K)$ as profinite groups, then L is isomorphic to K . Moreover, already the structure of the maximal prosolvable quotient of $\text{Gal}(K)$ determines K [15]. Recent works of Pop–Topaz [11], Saidi–Tamagawa [12], and others show that even much smaller quotients of $\text{Gal}(K)$ determine K .

The natural question whether the structure of the p -Sylow subgroups $\text{Gal}(K)_p$ of $\text{Gal}(K)$, where p runs over all primes, already suffices to determine K was raised by Florian Pop. The goal of this note is to show that this is not the case. To state it precisely, let us first define:

Definition 1.1. *Two number fields K and L are said to be Sylow-conjugate if for every prime p , the p -Sylow subgroups of $\text{Gal}(K)$ and $\text{Gal}(L)$ are conjugate in $\text{Gal}(\mathbb{Q})$.*

In particular, the absolute Galois groups of two Sylow-conjugate number fields have isomorphic p -Sylow subgroups. Furthermore, it is not difficult to see (Corollary 2.5 below) that two Sylow-conjugate number fields K, L have the same degrees $[K : \mathbb{Q}] = [L : \mathbb{Q}]$ and the same Galois closure M over \mathbb{Q} . Still we will give many examples for which K and L are not isomorphic to each other. Here are some such pairs:

Claim 1.2. *The following pairs (K, L) are Sylow-conjugate but not isomorphic:*

(a) $K = \mathbb{Q}(\alpha)$ and $L = \mathbb{Q}(\beta)$, where α and β , respectively, are the roots of:

$$p_7(x) = x^7 - 7x + 3 \text{ and } q_7(x) = x^7 + 14x^4 - 42x^2 - 21x + 9.$$

(b) $K = \mathbb{Q}(\alpha)$ and $L = \mathbb{Q}(\beta)$, where α and β , respectively, are the roots of:

$$\begin{aligned} p_8(x) &= x^8 - 4x^7 - 4x^6 + 26x^5 + 2x^4 - 52x^3 + 31x + 1, \text{ and} \\ q_8(x) &= x^8 + 12x^7 + 30x^6 - 108x^5 - 402x^4 + 342x^3 + 1256x^2 - 687x - 337. \end{aligned}$$

In Section 2, we will show, using (mainly) group theoretic methods, how one can get many more such examples. Some of these extensions are solvable, that is, admit a solvable Galois group $\text{Gal}(M/\mathbb{Q})$, and some are not. For example in case (a) above the Galois group $\text{Gal}(M/\mathbb{Q})$ is the nonsolvable group $\text{PSL}_3(2)$, while in case (b) it is the solvable group $\text{GL}_2(3)$. We will see that the degree 7 examples in (a) are of minimal possible degree over \mathbb{Q} , while in the examples in (b) the order of $\text{Gal}(M/\mathbb{Q})$ is 48 and this is minimal. Along the way, we will see that in many cases, Sylow conjugacy implies conjugacy: for example, if K is a solvable extension of prime degree, then it is determined by Sylow-conjugation, see Theorem 3.1.

Finally, Sylow-conjugation of number fields has some similarities with arithmetic equivalence, i.e. number fields with the same Dedekind zeta function. We discuss this in Section 4, showing that they are still very different: neither one implies the other. We shall also see that there exist pairs (K, L) which are both Sylow-conjugate and arithmetically equivalent and still not isomorphic.

This paper is dedicated to Moshe Jarden on his 80th birthday. Moshe is one of the leading figures of the area of Field Arithmetic and the founding father of this school in Israel. His work has had a lasting impact on both of us – for which we are very grateful.

We thank Robert Guralnick for valuable discussions. This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 882751) and from the Israel Science Foundation (grant no. 353/21). Both authors gratefully acknowledge the support and hospitality of the Institute for Advanced Study. All computer computations were carried out using MAGMA.

2. NONISOMORPHIC SYLOW-CONJUGATE NUMBER FIELDS

2.1. A group theoretic criterion. Let us start with some notation and terminology. If G is a profinite group, and p is a prime, we will denote its p -Sylow subgroup by G_p . Subgroups of profinite groups will always be assumed to be closed. We say

that two subgroups $U, V \leq G$ are *Sylow-conjugate* if U_p is conjugate to V_p within G for every prime p .

Lemma 2.1. *Let G be a group, $N \triangleleft G$ a normal subgroup, and $U, V \leq G$ two subgroups containing N . Then:*

- (a) *U and V are conjugate in G if and only if U/N and V/N are conjugate in G/N .*
- (b) *If G is profinite, U and V are Sylow-conjugate in G if and only if U/N and V/N are Sylow-conjugate in G/N .*

Proof. (a) is clear. For (b): If U and V are Sylow-conjugate, then clearly so are U/N and V/N , since the image of U_p in G/N is a p -Sylow subgroup of U/N . For the converse, first assume G is finite. Since $U_p N/N$ is a p -Sylow subgroup of U/N , our assumption yields that $U_p N/N$ and $V_p N/N$ are conjugate in G/N . Thus $g^{-1}U_p N g = V_p N$ for some $g \in G$. As both $g^{-1}U_p g$ and V_p are p -Sylow subgroups of $V_p N$, they are conjugate in G and hence so are U_p and V_p . This property then extends to profinite groups by a standard inverse limit argument. \square

Similarly, the following lemma is first verified easily for finite groups and then follows to profinite groups. For $U \leq G$, denote by $U^G = \bigcap_{g \in G} U^g$ the *core* of U in G , that is, the maximal normal subgroup of G contained in U .

Lemma 2.2. *Let G be a profinite group and U, V two Sylow-conjugate subgroups of G . Then $U^G = V^G$ and $[G : U] = [G : V]$.*

To translate these assertions to Sylow-conjugacy of number fields, we recall:

Remark 2.3. Every isomorphism between two fields $K, L \subseteq \overline{\mathbb{Q}}$ extends to an automorphism of $\text{Gal}(\overline{\mathbb{Q}})$, so that $K \cong L$ if and only if $\text{Gal}(K)$ and $\text{Gal}(L)$ are conjugate in $\text{Gal}(\overline{\mathbb{Q}})$. Letting $K^{(p)}$ denote the fixed field of a p -Sylow subgroup of $\text{Gal}(K)$, it follows that K and L are Sylow-conjugate if and only if $K^{(p)} \cong L^{(p)}$ for all primes p .

In view of this remark, the above lemmas give:

Proposition 2.4. *Let K and L be two number fields, and M/\mathbb{Q} a Galois extension containing both. Let $U := \text{Gal}(M/K)$ and $V := \text{Gal}(M/L)$ be subgroups of $G := \text{Gal}(M/\mathbb{Q})$. Then:*

- (a) *K and L are Sylow-conjugate if and only if U and V are Sylow-conjugate in G .*
- (b) *K and L are isomorphic if and only if U and V are conjugate in G .*

Proof. (b) is given by Remark 2.3 and Lemma 2.1.(a). To see (a), note that by definition K and L are Sylow-conjugate if and only if $\text{Gal}(K)$ and $\text{Gal}(L)$ are. By Lemma 2.1.(b), this happens if and only if U and V are Sylow-conjugate in G . \square

In particular, it follows that:

Corollary 2.5. *Let K and L be two Sylow-conjugate number fields. Then K/\mathbb{Q} and L/\mathbb{Q} have the same Galois closure and the same degrees.*

Proof. Let M, G, U, V be as in Proposition 2.4, so that U and V are Sylow-conjugate by the proposition. Recall that the core $C := \text{core}_G(U)$ is the largest subgroup of U which is normal in G , so that M^C is the Galois closure of K/\mathbb{Q} . To show that the normal closure of K/\mathbb{Q} and L/\mathbb{Q} coincide, it suffices to show that C and $D := \text{core}_G(V)$ coincide. Since every p -Sylow subgroup of C is of the form $U_p \cap C$ and $C \triangleleft G$, the groups $U_p \cap C$ and $V_p \cap C$ are conjugate p -Sylow subgroups of C . Since V contains a p -Sylow subgroup of C for every p , it follows that V and hence D contain C . By symmetry, $C = D$, proving the claim.

To show that $[K : \mathbb{Q}] = [L : \mathbb{Q}]$, note that as U and V are Sylow-conjugate, the largest p -powers dividing $|U|$ and $|V|$ coincide for every prime p . Thus, $|U| = |V|$ and hence $[K : \mathbb{Q}] = |G|/|U| = |G|/|V| = [L : \mathbb{Q}]$ as claimed. \square

Finally, Proposition 2.4 gives the following recipe for producing examples of pairs K and L which are Sylow-conjugate but not isomorphic.

Corollary 2.6. *Let G be a finite group which appears as the Galois group of a Galois extension M/\mathbb{Q} . Assume U and V are Sylow-conjugate subgroups of G that are nonconjugate, and let $K = M^U$ and $L = M^V$. Then K and L are nonisomorphic Sylow-conjugate number fields.*

A well known conjecture asserts that every finite group appears as the Galois group of some Galois extension of \mathbb{Q} .

2.2. Examples. One can produce many examples of tuples (G, U, V) satisfying the conditions of Corollary 2.6. Here are some ways to do so:

Example 2.7. Recall that for a set of primes Π , a subgroup H of a finite group G is called a Π -Hall subgroup if all prime divisors of $|H|$ are in Π , while all prime divisors of $[G : H]$ are not in Π . Note that two Π -Hall subgroups $U, V \leq G$ are always Sylow-conjugate by Sylow's theorem. Thus, every group G which appears as a Galois group over \mathbb{Q} and has two nonconjugate Π -Hall subgroups fits into Corollary 2.6.

For example, one may pick $G = \text{PSL}_2(11)$ and $\Pi = \{2, 3\}$. In this case G contains copies U and V of A_4 and the Dihedral group D_6 (of order 12), respectively, as Π -Hall subgroups. The subgroups U and V are clearly nonconjugate in G since they are nonisomorphic. There are many polynomials whose splitting field M has Galois

group $\text{Gal}(M/\mathbb{Q}) \cong \text{PSL}_2(11)$. For example, Malle–Matzat [7, Satz 4] show that

$$\begin{aligned} f_{11}(t, x) = & 2x^{11} - 2541x^9 - 45254x^8 + 1026201x^7 + 51653448x^6 + 900904653x^5 \\ & + 8705450754x^4 + 50915146293x^3 + 180040201308x^2 + 355871173680x \\ & + 303064483392 - 2t(x^3 + 22x^2 + 165x + 396)^2(x^3 - 22x^2 - 319x - 924) \end{aligned}$$

has Galois group G over $\mathbb{Q}(t)$, and hence by Hilbert’s irreducibility theorem $f(t_0, x)$ has Galois group G over \mathbb{Q} for infinitely many values $t_0 \in \mathbb{Q}$. Taking M to be the splitting field of such $f(t_0, x)$ yields examples of a pair $K = M^U$ and $L = M^V$ of nonisomorphic Sylow-conjugate number fields.

We note that such examples do not exist when G is solvable since a classical result of P. Hall [5, Theorem 9.3.1] asserts that G has Π -Hall subgroups and that these are all conjugate.

Example 2.8. In fact $G = \text{PSL}_2(11)$ has two nonconjugate subgroups U, V isomorphic to A_5 , see Appendix by Feit in [6]. These U, V are $\{2, 3, 5\}$ -Hall subgroups of G . Thus, letting M be a splitting field of the above polynomial $f_{11}(2, x)$, we again have that $K = M^U$ and $L = M^V$ are nonisomorphic but Sylow-conjugate. Explicitly, a computation using MAGMA shows that K and L are realized as the root fields of the polynomials:

$$\begin{aligned} p_{11}(x) = & x^{11} - 5090x^9 + 181368x^8 + 8224744x^7 - 828043392x^6 + 28884349472x^5 \\ & - 558216962688x^4 + 6529632151680x^3 - 46178757504000x^2 \\ & + 182555783258112x - 310931533135872, \text{ and} \\ q_{11}(x) = & x^{11} - 15270x^9 + 586696x^8 + 44022852x^7 - 3226512608x^6 + 230394820408x^5 \\ & - 12244387399904x^4 + 151382377029664x^3 - 3610663124873728x^2 \\ & + 20030100743110656x - 31953398556524544. \end{aligned}$$

Example 2.9. Let F be a finite field whose order q is a power of a prime p , let $d \geq 3$ be an integer, and $G = \text{PSL}_d(q)$. Let U be the stabilizer of some fixed 1-dimensional subspace, i.e. $U = \text{Stab}_G(\mathbb{F}_q \cdot e_1)$, where e_1, \dots, e_d is a basis for \mathbb{F}_q^d . Let V be the stabilize of the hyperplane W spanned by e_2, \dots, e_d . Then U and V are maximal parabolic subgroups of G which are nonconjugate in G (although they are isomorphic and in fact conjugate under an outer automorphism of G).

We claim that U and V are Sylow-conjugate in G . To see this, note that the p -Sylow subgroup of G is contained in a Borel subgroup and hence each parabolic subgroup contains a p -Sylow subgroup. In particular, U and V contain p -Sylow subgroups of G which are necessarily conjugate in G . For every other prime $\ell \neq p$, the subgroups U and V contain a common ℓ -Sylow subgroup of G , so that U and V are Sylow-conjugates.

We note that the groups $\text{PSL}_d(q)$ are known to appear as Galois groups $\text{Gal}(M/\mathbb{Q})$ for many pairs (d, q) , but not in general. Here is an especially interesting case:

Example 2.10. Let $G = \mathrm{PSL}_3(2)$, and U and V be its index-7 subgroups from Example 2.9. Note that $G \cong \mathrm{PSL}_2(7)$ as abstract groups. It is well known that G appears as a Galois group over \mathbb{Q} . Moreover, $K = M^U$ and $L = M^V$ can be chosen to be the fields $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$, respectively, where α and β are the roots of the pair of polynomials p_7, q_7 from Claim 1.2.(a) given by Trinks [13], or roots of one of the pairs of polynomials given by Erbach–Fischer–McKay [2], e.g.:

$$u_7(x) := x^7 - 154x + 99, \text{ and } v_7(x) := x^7 - 231x^3 - 462x^2 + 77x + 66.$$

In Section 3, we will show that this is a minimal example in the sense that there is no pair of nonisomorphic Sylow-conjugate fields whose degree over \mathbb{Q} is less than 7.

Example 2.11. Let U and V be two nonisomorphic finite groups satisfying: for every prime p , the p -Sylow subgroup of U is isomorphic to the p -Sylow subgroup of V . There are many such examples: e.g. U is the cyclic group of order 2ℓ , ℓ prime (or any odd number), and V the Dihedral group of order 2ℓ .

Embed both U and V into S_n , for $n = |U| = |V|$, via the regular permutation representation. One can see that for a p -Sylow subgroup P of U (or V), the permutation representation is a union of $|U|/|P|$ copies of the regular representation of P . Thus U_p and V_p are conjugate within S_n . It is classical that S_n is the Galois group of many extensions M/\mathbb{Q} , so that the triples (S_n, U, V) give many pairs $K = M^U$ and $L = M^V$ of nonisomorphic Sylow-conjugates.

Up to now, all of our examples were nonsolvable. One can produce also solvable examples such as the following.

Example 2.12. Let $G = \mathrm{GL}_2(3)$ be a group of order $48 = 16 \times 3$. Letting P be the 3-Sylow subgroup generated by

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

We let $U := \langle P, A \rangle$ and $V := \langle P, B \rangle$, where

$$A := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \text{ and } B := \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix},$$

are conjugate involutions normalizing P , so that U and V are Sylow-conjugate. We claim that U and V are nonconjugate. Indeed, as their 3-Sylow subgroups coincide and are unique in each of them, if U and V are conjugate, they are conjugate in the normalizer $N := N_G(P)$ of P . Since the number of 3-Sylow subgroups in G is $[G : N_G(P)] = 4$ (e.g. using the Sylow theorems), we see that $|N_G(P)| = 12$, and hence $N_G(P)$ is generated by A, B and P . However, A and B are nonconjugate in $\langle A, B, P \rangle = N_G(P)$ (which consists of upper triangular matrices), proving the claim.

By Shafarevich's theorem, every solvable group appears as the Galois group of a polynomial. The polynomial p_8 in Claim 1.2 is a well known example of a polynomial with Galois group $\mathrm{GL}_2(3)$ over \mathbb{Q} with point stabilizer S_3 . A direct computation shows that a root field of the polynomial q_8 from the claim is the fixed field of a nonconjugate copy of S_3 . In Section 3, we will show that in this example G is of smallest possible order.

3. WHEN SYLOW-CONJUGATION IMPLIES ISOMORPHISM

In this section, we state conditions under which Sylow conjugation does imply isomorphism. We first show that two Sylow-conjugate number fields K and L of prime degree p over \mathbb{Q} are “usually” isomorphic. The following result makes use of the classification of finite simple groups (CFSG).

Theorem 3.1. *Let K, L be two Sylow-conjugate number fields of prime degree p over \mathbb{Q} . Then K and L are isomorphic unless their common Galois closure M/\mathbb{Q} satisfies one of the following:*

- (a) $p = 11$, $\mathrm{Gal}(M/\mathbb{Q}) \cong \mathrm{PSL}_2(11)$, and K and L are number fields of the type described in Example 2.8 (the fixed fields of the two different conjugation classes of A_5 in $\mathrm{PSL}_2(11)$).
- (b) There exists a prime $d \geq 3$ and a prime power q , such that

$$(1) \quad p = \frac{q^d - 1}{q - 1},$$

and $\mathrm{Gal}(M/\mathbb{Q})$ is an almost simple group with socle $\mathrm{PSL}_d(q)$. Here K and L are the fixed fields of two nonconjugate subgroups U' and V' in G whose intersection with $\mathrm{PSL}_d(q)$ are equal to the two maximal parabolic subgroups described in Example 2.9.

In particular, the following is the direct consequence for solvable groups, which however does not require the classification:

Corollary 3.2. *If K and L are solvable (i.e. $\mathrm{Gal}(M/\mathbb{Q})$ is solvable) Sylow-conjugate extensions of prime degree, then they are isomorphic.*

Proof of Theorem 3.1. Let $G := \mathrm{Gal}(M/\mathbb{Q})$, and $U, V \leq G$ be the index- p subgroups fixing K and L , respectively. Then G acts faithfully on G/U (and on G/V) as a degree p permutation group. As p is prime, Burnside's theorem [8] shows that either (i) G is solvable, in which case it is a subgroup of $\mathrm{Aff}_1(\mathbb{F}_p) = \mathbb{F}_p \rtimes \mathbb{F}_p^\times$, or (ii) G is doubly transitive, and hence almost simple [1, Theorem 7.2E].

In case (i), G is isomorphic to $\mathbb{F}_p \rtimes C$ with $|C| \mid p-1$ and in particular $|C|$ is prime to p . Hence $H^1(C, \mathbb{F}_p) = 0$ and \mathbb{F}_p has a unique complement under conjugation. Thus, every two subgroups of G of index p are conjugate.

In case (ii), let S be the socle of G , and note that since U is of index p and has trivial core, $S \cap U$ is of index p in S . We next append to the work of Guralnick [4] who classifies, using CFSG, all the finite simple groups S with a subgroup of prime power index. The cases where S has a subgroup of index p are: (a') $S \cong \text{PSL}_2(11)$ with $p = 11$; (b') $S \cong \text{PSL}_d(q)$ in the action described in (b) with $p = (q^d - 1)/(q - 1)$; (c) the alternating group $S \cong A_p$ for arbitrary prime p ; and (d) $S \cong M_{23}$ with $p = 23$ or $S \cong M_{11}$ with $p = 11$. In (c), the index- p subgroups of the alternating group A_p (resp. of the symmetric group $S_p = \text{Aut}(A_p)$) are conjugate. Similarly, the index- p subgroups are conjugate for the Mathieu groups in (d) (which are the unique almost simple groups with the given socle). In (b'), G is as in (b) and d is prime as well [4]. Note that $d \geq 3$ since for $d = 2$ the index- p subgroups are conjugate. In (a'), the degree-11 action of $\text{PSL}_2(11)$ does not extend to a degree-11 action of $\text{PGL}_2(11)$, and hence $G = S \cong \text{PSL}_2(11)$ as in (a). \square

Remark 3.3. Note that case (a) indeed gives a counterexample as described in Example 2.8. Also if for a prime p , (1) has a solution with $d \geq 3$ and a prime power q , then indeed $G = \text{PSL}_d(q)$ has two subgroups U and V of index p which are Sylow-conjugate but nonconjugate, see Example 2.9 above.

What is unknown is whether $G = \text{PSL}_d(q)$ is indeed always a Galois group over \mathbb{Q} . It is also unknown if there are infinitely many primes for which (1) has such solutions q and d , see [3] for a discussion. But certainly there are some, for example:

$$13 = \frac{3^3 - 1}{3 - 1}, 31 = \frac{5^3 - 1}{5 - 1}, 73 = \frac{8^3 - 1}{8 - 1}, \text{ and } 1772893 = \frac{11^9 - 1}{11^3 - 1}.$$

We note that in the class of nilpotent groups Sylow conjugacy implies conjugacy:

Lemma 3.4. *Let K and L be Sylow-conjugate number fields whose common Galois closure M/\mathbb{Q} has a nilpotent Galois group G . Then K and L are isomorphic.*

Proof. As G nilpotent, it is the product $\prod_p G_p$ of its p -Sylow subgroups, and hence $U_p = V_p^{x_p}$ are already conjugate by an element $x_p \in G_p$, for every prime p . Since the elements x_p , p prime, commute, it follows that $U = V^x$, where $x = \prod_p x_p$. \square

We give one more infinite family for which Sylow-conjugacy implies conjugacy.

Proposition 3.5. *Suppose $G = A \rtimes H$, where A is an abelian group which is irreducible as an H -module. Let M/\mathbb{Q} be a G -extension and K and L be Sylow-conjugate subfields fixed by complements of A in G . Then K and L are isomorphic.*

Proof. Let $U = \text{Gal}(M/K)$ and $V = \text{Gal}(M/L)$ be the corresponding complements of A in G . Since A is an irreducible H -module, A is an elementary abelian p -group for some prime p . Let $\pi : G \rightarrow H$ the natural projection modulo A .

We first claim that the restriction map $\text{res}_p : H^1(U, A) \rightarrow H^1(U_p, A)$ is injective. Indeed, letting $\text{cor}_p : H^1(U_p, A) \rightarrow H^1(U, A)$ denote the corestriction map, it is well known that $\text{cor}_p \circ \text{res}_p$ is the multiplication-by- $[U : U_p]$ map. Since $[U : U_p]$ is coprime to $|A|$, this multiplication map is an isomorphism, so that res_p is injective.

Since U and V are complements of A in G there is a cocycle $\chi \in Z^1(U, A)$ for which the homomorphism $f_\chi : U \rightarrow G$, $u \mapsto u \cdot \chi(u)$ maps U isomorphically to V . The subgroup $f_\chi(U_p)$ is a p -Sylow subgroup of V , which we denote by V_p . Note that since $\text{Im } \chi \in A$, we have $U_p A = V_p A$. Let $H_p := \pi(U_p) = \pi(V_p)$.

Since U and V are Sylow-conjugate, there exists $g \in G$ such that $U_p^g = V_p$. Thus $\pi(g)$ is in the normalizer $N_H(H_p)$ of H_p in H , so that $g \in \pi^{-1}(N_H(H_p)) = N_U(U_p)A$, where the latter equality holds since π maps $N_U(U_p)$ isomorphically to $N_H(H_p)$ (as U and U_p are mapped isomorphically to H and H_p , respectively). Writing $g = na$ for $n \in N_U(U_p)$ and $a \in A$, we see that $V_p = U_p^{na} = (U_p^n)^a = U_p^a$, so that U_p and V_p are conjugate by $a \in A$.

We claim that the latter implies that the restriction $\chi_p := \text{res}_p(\chi)$ has a trivial class in $H^1(U_p, A)$. Indeed, since U_p and V_p are conjugate in $U_p A = V_p A$, by composing $f_{\chi_p} : U_p \rightarrow V_p$ with inner conjugation by a^{-1} , we obtain a map $f_{\chi'_p} : U_p \rightarrow U_p$ for some $\chi'_p \in Z^1(U_p, A)$ cohomologically equivalent to χ_p . Thus $f_{\chi'_p}(u) = u\chi'_p(u) \in U_p$, so that $f_{\chi'_p}(u)u^{-1} \in A \cap U = 1$, that is, $f_{\chi'_p}(u) = u$ and $\chi'_p(u) = 1$ for all $u \in U_p$.

Finally, since by the above claim res_p is injective, this implies $[\chi] \in H^1(U, A)$ is trivial, and hence that U and V are conjugate as desired. \square

Finally, we show that Sylow-conjugate number fields which are “smaller” than those in Claim 1.2 are isomorphic.

Proposition 3.6. *Let K and L be two Sylow-conjugate number fields with common Galois closure M/\mathbb{Q} and Galois group $G = \text{Gal}(M/\mathbb{Q})$. Assume that either $[K : \mathbb{Q}] = [L : \mathbb{Q}] \leq 6$ or that $|G| < 48$. Then K and L are isomorphic.*

Proof. Set $d := [K : \mathbb{Q}] = [L : \mathbb{Q}]$ and first assume $d \leq 6$. By Proposition 2.4 and Lemma 2.2, the subgroups $U = \text{Gal}(M/K)$ and $V = \text{Gal}(M/L)$ are Sylow-conjugate subgroups of G of index d with trivial core. In particular, we may identify G with a subgroup of S_d . We claim that U and V are conjugate. We checked this using MAGMA, as well as analyzed by hand as follows:

First note that if the order of U and V is a power of a prime, as they are Sylow-conjugate, they are conjugate. Henceforth, assume $|U|, |V|$ are not prime powers.

For $d \leq 2$, one has $U, V \triangleleft G$ and hence $U = V$. For $d = 3$, since $U, V \leq G$ have trivial core, $G = S_3$, and U, V are 2-Sylow subgroups of G . As U, V are Sylow-conjugate they are conjugate. For $d = 4$: if $G = S_4$, it has a unique conjugacy class of index 4 subgroups. For $G \subsetneq S_4$, as $d = 4$, it follows that $|U|, |V|$ are prime powers. The case $d = 5$ is covered by Theorem 3.1 as d is a prime.

The case $d = 6$ is more interesting: If $G = S_6$ or A_6 , then G indeed has two different conjugacy classes of index 6 subgroups. One is $U = S_5$ (resp. $U = A_5$) and the second is the image V of the action $S_5 \rightarrow \text{Sym}\{P_1, \dots, P_6\} = S_6$ of S_5 on its six 5-Sylow subgroups P_1, \dots, P_6 . Indeed, U and V are nonconjugate in S_6 (resp. A_6) since U fixes a point while V does not. But at the same time, the 3-Sylow subgroups U_3 and V_3 of U and V , which are of order 3, are nonconjugate as well since U_3 has a fixed point while V_3 does not.

Henceforth assume $G \subsetneq S_6$ is a proper subgroup other than A_6 . The maximal subgroups $G \leq S_6$ (resp. $G \leq A_6$) satisfying the above are of order 48, 72, and 120 (resp. 24, 36, and 60).

The only subgroup of order 120 (resp. $G \leq A_6$ of order 60) is S_5 (resp. A_5). If $G = S_5$ (resp. A_5), it has a unique conjugacy class of index 6 subgroups, namely the Frobenius group of order 20 (resp. Dihedral group of order 10) normalizing a 5-Sylow subgroup. If $G \subsetneq S_5$ (resp. $G \subsetneq A_5$) is a proper subgroup other than A_5 , then $|G|/6$ is a prime power, so that in this case as well U and V are conjugate.

The only subgroup of S_6 of order 72 (resp. of A_6 of order 36) is the stabilizer of a partition into two blocks of size 3, so that here we may assume $G \leq S_3 \wr C_2 = (S_3 \times S_3) \rtimes C_2$. The only such subgroups for which $|G|/6$ is not a prime power are $S_3 \wr C_2$ and its subgroups of order 36. Letting G be one of those groups, $G_3 = C_3 \times C_3$ is normal in G , and hence the subgroup $U_3 = G_3 \cap U$ of order 3 is normal $U_3 \triangleleft U$. Since U_3 is normalized by U , a subgroup of index 6, and by G_3 , the normalizer $N_G(U_3)$ is of index ≤ 2 in G . If $N_G(U_3) = G$, i.e. $U_3 \triangleleft G$, then $V_3 = U_3$. In this case, since $U_2 = V_2^x$ for some $x \in G$, one has $V^x = V_3^x V_2^x = U_3 U_2 = U$. Otherwise, $[G : N_G(U_3)] = 2$, and U_2 is also a 2-Sylow subgroup of $N_G(U_3)$. Similarly V_2 is a 2-Sylow of $N_G(V_3)$. Moreover, as $V_3^x = U_3$ for some $x \in G$, one has $N_G(V_3)^x = N_G(U_3)$, and so V_2^x is also a 2-Sylow subgroup of $N_G(U_3)$. Thus $V_2^{xy} = U_2$ for some $y \in N_G(U_3)$, so that

$$V^{xy} = V_2^{xy} V_3^{xy} = U_2 U_3^y = U_2 U_3 = U.$$

Finally if $G \leq S_6$ is of order 48 (resp. $G \leq A_6$ is of order 24) or a subgroup of it, then $|G|/6$ is of prime power order, completing the proof in case $d \leq 6$.

Assume $|G| < 48$ (and d is arbitrary), and $U, V \leq G$ are Sylow-conjugate. Note that when $d := [G : U] = [G : V]$ is either prime or of degree 4 or 6, then the claim follows from Theorem 3.1 and the first assertion of the proposition. Thus to deduce the second assertion, it suffices to note that if $|G| < 48$ and $[G : U] = [G : V] \geq 8$ is not a prime, then $|U|, |V|$ are prime powers, so that U and V are conjugate.

□

4. BETWEEN SYLOW-CONJUGACY AND ARITHMETIC EQUIVALENCE

Two number fields K and L are said to be arithmetically equivalent if their Dedekind zeta function are equal $\zeta_K(s) = \zeta_L(s)$. It is well known [10] that this happens if and only if K and L have a common Galois closure M/\mathbb{Q} satisfying the following: The subgroups $U = \text{Gal}(M/K)$ and $V = \text{Gal}(M/L)$ of $G = \text{Gal}(M/\mathbb{Q})$ satisfy $|C \cap U| = |C \cap V|$ for every conjugacy class C of G . So arithmetic equivalence, just like Sylow conjugation is a weak form of conjugation. This and other¹ similarities may suggest that the two properties are equivalent. In what follows we will show that this is not the case (Examples 4.1 and 4.2). Example 4.3 will show that there are number fields which are Sylow-conjugate as well as arithmetically equivalent and still not isomorphic.

Example 4.1. Let p be an odd prime, $U = C_{2p}$ the cyclic group of order $2p$, and $V = D_{2p}$ the Dihedral group of order $2p$. Embed them regularly in $\text{Sym}(2p)$. Every element of C_{2p} (resp. D_{2p}) of order 2 gives rise to a product of p distinct transpositions, and an element of order p induces a product of two disjoint p -cycles. Now, U and V are therefore Sylow-conjugate in $\text{Sym}(2p)$, but are clearly not arithmetically equivalent, as C_{2p} has an element of order $2p$ but D_{2p} does not. As $\text{Sym}(2p)$ is a Galois group over \mathbb{Q} , this induces (as in Example 2.11) pairs of number fields which are Sylow-conjugate but not arithmetically equivalent.

Example 4.2. Let p be a prime, $U = C_p \times C_p \times C_p$ and

$$V = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \mid a, b, c \in \mathbb{F}_p \right\}$$

the Heisenberg group over the field \mathbb{F}_p . Embed U and V regularly into $\text{Sym}(p^3)$. Every nontrivial element of U (resp. V) when acting on U (resp. V) induces a permutation which is a product of p^2 disjoint p -cycles. Then by the above criterion,

¹We show above that Sylow-conjugacy implies conjugacy if the degree is < 7 or, in case G is solvable, if the degree is a prime. Similar results are also proved by Perlis for arithmetic equivalence: The case of degree < 7 is given in [10, Theorem 3], while the case where G is solvable and the degree is a prime p is covered by [10, Theorem 2(g)] (since stabilizers are of order coprime to p).

U and V are arithmetically equivalent, but they are clearly not Sylow-conjugate, as they are nonisomorphic p -groups.

Example 4.3. Let us take a second look at Example 2.9. We showed that these two maximal parabolic subgroups $U, V \leq G$ are Sylow-conjugate and nonconjugate. We claim now that the examples are also arithmetically equivalent. Indeed, the above group theoretic criterion is equivalent to saying that the linear representation of G on $\mathbb{C}[G/U]$ is isomorphic to the one on $\mathbb{C}[G/V]$. (Note that U and V are conjugate if and only if the permutational representations are isomorphic).

To show that the two linear representations are isomorphic it suffices to show that $\text{tr}(g|_{\mathbb{C}[G/U]}) = \text{tr}(g|_{\mathbb{C}[G/V]})$ for every $g \in G$. Next note that:

- (a) In the linear representation induced by a permutational representation $\text{tr}(g)$ is equal to the number of fixed points.
- (b) In our case the action of G on G/U is equivalent to the action of G on the 1-dimensional subspaces of \mathbb{F}_q^d , while the action on G/V is equivalent to that on hyperplanes.

Whenever $g \in G$ preserves a 1-dimensional subspace L , its transpose g^t preserves the hyperplane L^\perp perpendicular to L . Thus, $\text{tr}(g|_{\mathbb{C}[G/U]}) = \text{tr}(g^t|_{\mathbb{C}[G/V]})$. But g and g^t are conjugate in $\text{PSL}_d(q)$ and hence $\text{tr}(g|_{\mathbb{C}[G/U]}) = \text{tr}(g|_{\mathbb{C}[G/V]})$, and U and V give rise to arithmetically equivalent nonisomorphic number fields, provided $\text{PSL}_d(q)$ is a Galois group. This is the case at least for $\text{PSL}_3(2)$, which gives the examples in Claim 1.2.(b).

REFERENCES

- [1] J. D. Dixon, B. Mortimer, *Permutation Groups*. GTM 163, Springer-Verlag, New York, 1996.
- [2] D. W. Erbach, J. Fischer, J. McKay, Polynomials with $\text{PSL}(2, 7)$ as Galois group. *J. Number Theory* 11 (1979), 69–75.
- [3] D. Estes, R. M. Guralnick, M. Schacer, E. Straus Equations in prime powers. *Pacific J. Math.* 118 (1985), 359–387.
- [4] R. M. Guralnick, Subgroups of Prime Power Index in a Simple Group. *J. Algebra* 81 (1983), 304–311.
- [5] M. Hall, *The Theory of Groups*. The Macmillan Company, New York, N.Y. 1959.
- [6] S. Lang, *Introduction to modular forms*. Corrected reprint of the 1976 original. Grundlehren der mathematischen Wissenschaften, 222. Springer-Verlag, Berlin, 1995.
- [7] G. Malle, H. Matzat, Realisierung von Gruppen $\text{PSL}_2(\mathbb{F}_{11})$ als Galoisgruppen über \mathbb{Q} . *Math. Ann.* 272 (1985), 549–565.
- [8] P. Müller, Permutation groups of prime degree, a quick proof of Burnside’s theorem. *Archiv der Mathematik* 85 (2005), 15–17.
- [9] J. Neukirch, Kennzeichnung der p -adischen und der endlichen algebraischen Zahlkörper. *Invent. Math.* 6 (1969), 296–314.

- [10] R. Perlis, On the equation $\zeta_K(s) = \zeta_{K'}(s)$. J. Number Theory 9 (1977), 342–360.
- [11] F. Pop, A. Topaz, Towards a minimalistic Neukirch-Uchida Theorem. Talk at the MFO workshop “Homotopic and Geometric Galois Theory”, 3/2021.
- [12] M. Saidi, A. Tamagawa, The m -step solvable anabelian geometry of number fields. Preprint, arXiv:1909.08829.
- [13] W. Trinks, Ein Beispiel eines Zahlkörpers mit der Galoisgruppe $\mathrm{PSL}(3, 2)$ über \mathbb{Q} . Manuscript, Universität Karlsruhe, 1968.
- [14] K. Uchida, Isomorphism of Galois groups, Math. Soc. Japan 28 (1976), 617–620.
- [15] K. Uchida, Isomorphisms of Galois groups of solvably closed Galois extensions. Tohoku Math. J. 31 (1979), 359–362.

DEPARTMENT OF MATHEMATICS, WEIZMANN INSTITUTE OF SCIENCE, REHOVOT, ISRAEL

Email address: alexander.lubotzky@weizmann.ac.il

DEPARTMENT OF MATHEMATICS, TECHNION - ISRAEL INSTITUTE OF TECHNOLOGY, HAIFA, ISRAEL

Email address: dneftin@technion.ac.il