New York Journal of Mathematics

New York J. Math. **25** (2019) 558–573.

On a question of Perlis and Stuart regarding arithmetic equivalence

Guillermo Mantilla-Soler

Abstract. Let K be a number field. The K-arithmetic type of a rational prime ℓ is the tuple $A_K(\ell) = (f_1^K, ..., f_{g_\ell}^K)$ of the residue degrees of ℓ in K, written in ascending order. A well known result of Perlis from the 70's states that two number fields have the same Dedekind zeta function if and only if for almost all primes ℓ the arithmetic types of ℓ in both fields coincide. By the end of the 90's Perlis and Stuart asked if having the same zeta function implies that for ramified primes the sum of the ramification degrees coincide. Here we study and answer their question for a nontrivial and interesting class of cases.

Contents

1. Introduction

Two number fields are called *arithmetically equivalent* if they have the same Dedekind zeta function. It is of continuous interest to several authors, see for instance recent works by [2], [13], [1] and others, to study arithmetic equivalence in number fields, and their geometric counterparts from the point of view of function fields.

Let K be a number field and let ℓ be a rational prime. Recall that the *arithmetic type* of ℓ in K is the ordered tuple

$$A_K(\ell) := (f_1^K, ..., f_{g^K}^K)$$

where the f_i^K's are the residue degrees of ℓ in K and

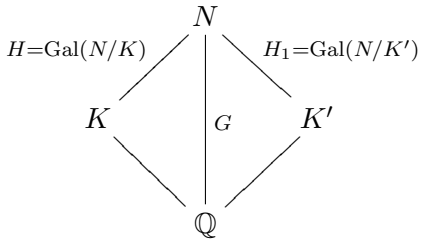
$$f_1^K \leq ... \leq f_{g^K}^K.$$

Received May 20, 2019.
2010 *Mathematics Subject Classification.* 11R42.
Key words and phrases. Arithmetic equivalence, Septic fields.

ISSN 1076-9803/2019

Let e_i^K be the ramification degree of ℓ corresponding to the residue degree f_i^K. In the early 70's Perlis showed that the Dedekind zeta function of a number field is completely determined by the residue degrees over every rational prime. Further, he gave a group theoretic characterization for the equivalence to occur:

Suppose that K, K' are two number fields and let N be the compositum of their Galois closures. Let $G = \mathrm{Gal}(N/\mathbb{Q})$, and let H, H_1 be the corresponding subgroups of K and K' via the Galois correspondence



Definition 1.1. *We say that K and K' are quasi-conjugate if the groups H and H_1 are quasi-conjugate in G i.e., if for every conjugacy class C of G we have that*

$$\#(C \cap H) = \#(C \cap H_1).$$

Remark 1.2. Notice that if H and H_1 are conjugate subgroups in G then they are quasi-conjugate. Also, since conjugacy classes are a partition of G we have that $\#H = \#H_1$ whenever H and H_1 are quasi-conjugate

Theorem 1.3 ([8])**.** *Let K, K' be two number fields. Then, the following are equivalent:*

(a) *The fields K, K' are arithmetically equivalent.*
(b) *For almost every prime ℓ the arithmetic types of ℓ in K and K' are the same.*
(c) *The fields K, K' are quasi-conjugate.*

One useful application of the above theorem is that of easily checking when a field K is *arithmetically solitary*, i.e., there is no field K' non-isomorphic and arithmetically equivalent to K. For example, using this and some group theory, Perlis [8] has proved that if the degree of K is at most 6 then it is arithmetically solitary. Moreover if K is septic and it is not arithmetically solitary then K is a $\mathrm{PSL}_2(\mathbb{F}_7)$ septic field i.e., the Galois group of its Galois closure is the simple group of order 168 (see [5] or [12]).

1.1. The question and its answer. In the late 90's Perlis and Stuart gave a new surprising characterization for arithmetic equivalence; They showed that it is enough to know the length of the arithmetic types, at almost every prime, to know the Dedekind zeta function. Explicitly:

Theorem 1.4 (Perlis, Stuart [11]). *Let K, K' be number fields. Then, K, K' are arithmetically equivalent if and only if for almost every prime ℓ the number of prime factors lying over ℓ in O_K and $O_{K'}$ is the same.*

Perlis and Stuart asked if not only the residue degrees or the number of prime factors are determined by the zeta function, but if the ramification degrees are determined as well. This is not the case, as shown by Perlis. However, Perlis and Stuart pointed out that it was not known if the sum of the ramification degrees can differ. Suppose that K, K' are arithmetically equivalent number fields and let ℓ be a rational prime. Let $A_K(\ell) = (f_1, ..., f_g) = A_{K'}(\ell)$ be the common arithmetic type tuples for ℓ. Let $(e_1^K, ..., e_g^K)$ and $(e_1^{K'}, ..., e_g^{K'})$ be the corresponding tuples of ramification degrees. Based on their work on split and arithmetic equivalence, and the examples they studied, Perlis and Stuart ended their paper with the following question:

Question 1.5 (Perlis, Stuart [11]). *Does it follow that the sum of the ramification degrees is the same for all prime ℓ?*

$$e_1^K + ... + e_g^K = e_1^{K'} + ... + e_g^{K'}$$

In principle the only obvious restriction on the ramification degrees is given by the following:

$$f_1 e_1^K + ... + f_g e_g^K = f_1 e_1^{K'} + ... + f_g e_g^{K'} = [K : \mathbb{Q}].$$

1.1.1. Septic fields. Since number fields of degree less than 7 are arithmetically solitary the first interesting case of study for Question 1.5 is that of septic number fields. As it turns out, in degree 7, under certain restrictions on the ramification types Question 1.5 is positively answered:

Theorem (cf. Theorem 3.4). *Let K be a degree 7 number field, and let ℓ be a rational prime. Suppose that the arithmetic type of ℓ in K does not belong to*

$$\{(1,3), (1,1,2), (1,1,1,2)\}.$$

Then for any K' arithmetically equivalent to K

$$e_1^K + ... + e_g^K = e_1^{K'} + ... + e_g^{K'}.$$

From this and from the fact that septic fields that are non arithmetically solitary have a Galois closure with simple Galois group, we obtain:

Corollary (cf. Corollary 3.5). *Let K, K' be degree 7 arithmetically equivalent number fields. Suppose ℓ is a rational prime which is not wildly ramified in either K or K', and let v_ℓ the usual ℓ-adic valuation. If $e_1^K + ... + e_g^K \neq e_1^{K'} + ... + e_g^{K'}$ then $v_\ell(\mathrm{disc}(O_K)) \in \{2, 4\}$.*

1.2. What about general non arithmetically solitary septic fields? Based on the above results we use an algorithm that searches for possible examples giving a negative answer to Question 1.5. First we search for pairs of septic fields with same discriminant, and signature, with not too many ramified primes; actually to make things easier we start with only two prime factors. Moreover, using the remark after Corollary 3.5, we take the prime $\ell = 2$ as one of the two primes. Similarly, thanks to Corollary 3.5, we know the valuation of the discriminant at the other prime divisor as well. Among the candidates found, we select the ones such that their ramified primes have arithmetic type belonging to the list appearing in Theorem 3.4. From those, we take the $\mathrm{PSL}_2(\mathbb{F}_7)$ fields and see if there is any couple of arithmetically equivalent fields for which the sum of ramification degrees differ. More explicitly:

1.2.1. Algorithm. The input is a list of septic fields up to some discriminant bound, and the output is either a list either empty or containing pairs of examples, within the discriminant bound, giving a negative answer to Question 1.5.

(i) Look in the list for number fields with discriminant of the form $2^{2a}p^{2b}$ where $a \in \{3, 4\}$ and $b \in \{1, 2\}$.

(ii) Select pairs of fields from step (i) that have equal signature and discriminant and such that their ramification types, at 2 or p, belong to the list appearing in Theorem 3.4.

(iii) From (ii) select the ones that have Galois group $\mathrm{PSL}_2(\mathbb{F}_7)$.

(iv) Verify, using Theorem 3.8, whether or not the fields obtained in (iii) are arithmetically equivalent.

(v) From each pair of arithmetically equivalent fields obtained check whether or not there are pairs for which the sum of ramification degrees, at the ramified primes, are different.

Using the algorithm described above with John Jones' data base of number fields, and writing some MAGMA code, we found out that Theorem 3.4 is optimal for getting a positive answer to Question 1.5; in other words:

Theorem (cf. Theorem 3.7)**.** *For each tuple $\mathcal{F} \in \{(1,3), (1,1,2), (1,1,1,2)\}$ there are examples of pairs (K, K') of non-isomorphic arithmetically equivalent number fields, and a prime ℓ, with common arithmetic type $\mathcal{F}$ in K and K' such that*

$$e_1^K + ... + e_g^K \neq e_1^{K'} + ... + e_g^{K'}.$$

1.2.2. Overview of the contents. In Section §2 we recall most of the standard facts of Arithmetic equivalence from the point of Galois representations. Nothing in this section is new and it is well known to experts but we could not find a suitable reference that contains these results in the context of $G_{\mathbb{Q}}$ representations. For example, even though that from the point of view of Galois representations Theorem 2.5 is elementary we have not found a presentation of that result in such a natural form. In Section §3 we give proofs of our main results and exhibit examples, found following the algorithm described above, that give a negative answer to Question 1.5.

2. Arithmetic equivalence via Galois representations

Suppose that the Dedekind zeta function of a number field K is written as

$$\zeta_K(s) := \sum_{n=0}^{\infty} \frac{a_n(K)}{n^s}.$$

Then interpreting the zeta function as a counting function it should be true, as in the case of Tate's isogeny theorem, that $\zeta_K(s)$ is completely determined by the values $a_\ell(K)$ at primes ℓ. Since $a_\ell(K)$ is equal to the number of 1's appearing in the tuple $A_K(\ell)$ knowing the values $a_\ell(K)$ is a priori weaker than knowing the arithmetic type of ℓ in K. However, as suggested above, the knowledge of the $a_\ell(K)$ for almost all ℓ indeed determines the function $\zeta_K(s)$. In this section, using the rudiments of Galois representations, we briefly recall how these results can be obtained.

Let K be a degree n number field, and let us denote by $\widetilde{K}$ its Galois closure over $\mathbb{Q}$. We start by recalling the construction of an n-dimensional complex Galois representation ρ_K of the absolute Galois group $G_{\mathbb{Q}}$ such that the Artin L-function associated to ρ_K is $\zeta_K(s)$. Let $\mathrm{Emb}(K)$ be the set of complex embeddings of K. The absolute Galois group $G_{\mathbb{Q}}$ acts continuously on $\mathrm{Emb}(K)$ via composition. The continuity follows since the kernel of the action is the open group $G_{\widetilde{K}}$. Since $n = \#\mathrm{Emb}(K)$ the above gives a continuous permutation representation $G_{\mathbb{Q}} : \pi_K \to S_n$, which by composition with the permutation representation $\iota_n : S_n \to \mathrm{GL_n}(\mathbb{C})$ produces an n-dimensional complex representation

$$\rho_K : G_{\mathbb{Q}} \to \mathrm{GL_n}(\mathbb{C}).$$

Definition 2.1. *Let K be a number field. The continuous $\mathbb{C}[G_{\mathbb{Q}}]$-module T_K is the $G_{\mathbb{Q}}$-module attached to the representation ρ_K. In other words, $T_K := \bigoplus_{\sigma \in \mathrm{Emb}} \mathbb{C}\sigma$ with the action of $G_{\mathbb{Q}}$ on each element of the basis given by composition.*

The relevance of this representation to our purposes is that the Artin formalism gives us the following:

Proposition 2.2. *Let K be a number field and let us denote by $L(\rho, s)$ the Artin L-function attached to a representation ρ. Then $L(\rho_K, s) = \zeta_K(s)$.*

Proof. By Galois correspondence ρ_K factorizes through

$$\mathrm{Res}^{\overline{\mathbb{Q}}}_{\widetilde{K}}(\rho_K) : \mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \to \mathrm{GL_n}(\mathbb{C}).$$

Again, by basic Galois theory, the action of $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ in $\mathrm{Emb}(K)$ is isomorphic to the permutation representation of $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ in the set of cosets $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})/\mathrm{Gal}(\widetilde{K}/K)$. Hence, $\mathrm{Res}^{\overline{\mathbb{Q}}}_{\widetilde{K}}(\rho_K) \cong \mathrm{Ind}^{\mathrm{Gal}(\widetilde{K}/\mathbb{Q})}_{\mathrm{Gal}(\widetilde{K}/K)} 1_{\mathrm{Gal}(\widetilde{K}/K)}$. Thanks to Artin's formalism

$$L(\rho_K, s) = L\left(\mathrm{Res}^{\overline{\mathbb{Q}}}_{\widetilde{K}}(\rho_K), s\right) = L\left(\mathrm{Ind}^{\mathrm{Gal}(\widetilde{K}/\mathbb{Q})}_{\mathrm{Gal}(\widetilde{K}/K)} 1_{\mathrm{Gal}(\widetilde{K}/K)}, s\right) =$$

$$L(1_{\mathrm{Gal}(\widetilde{K}/K)}, s) = \zeta_K(s).$$

□

Since the Dedekind zeta function is an Artin L-function then its prime terms correspond to traces of Frobenius elements:

Corollary 2.3. *Let K be a number field and ℓ be a prime unramified*[1] *under ρ_K. Let $Frob_\ell$ be the conjugacy class of the element Frobenius at ℓ. Then,*

$$\mathrm{Trace}(\rho_K(Frob_\ell)) = a_\ell(K).$$

Proposition 2.2 gives not only a simple way to express the trace of Frobenius but it also gives a useful generalization of the above corollary to calculate its characteristic polynomial $\det(X - \rho_K(\mathrm{Frob}_\ell))$.

Lemma 2.4. *Let K be a number field and ℓ be a prime, unramified in K, and let $(f_1, ..., f_g)$ be the arithmetic type of ℓ in K. Then,*

$$\det(X - \rho_K(\mathrm{Frob}_\ell)) = \prod_{i=1}^{g}(X^{f_i} - 1).$$

Proof. Let $B_1, ..., B_g$ be the primes in O_K lying over the prime ℓ. Then, the ℓ-factor in the Euler product for $\zeta_K(s)$ is given by

$$\prod_{i=1}^{g}(1 - ||B_i||^{-s})^{-1} = \prod_{i=1}^{g}(1 - \ell^{-sf_i})^{-1}.$$

On the other hand, since $\zeta_K(s)$ is also the Artin L-function of the representation ρ_K, the ℓ-factor above is also equal to $\det(I - \ell^{-s}\rho_K(\mathrm{Frob}_\ell))^{-1}$. The result follows from substituting ℓ^{-s} by X.

□

[1]This is the same as being unramified in K since the conductor of ρ_K is the discriminant of K.

2.0.1. An analogy with the isogeny theorem. The zeta function $\zeta_K(s)$ is the Artin L-function of the trivial representation of $\mathrm{Gal}(\overline{K}/K)$, however knowing this is not very useful in our context since for two different number fields we would get representations from different groups. By looking at a Galois representation of $G_{\mathbb{Q}}$ for which $\zeta_K(s)$ is its Artin L-function one can actually obtain results about the number field in question. This, as straightforward as it is, gives a simpler characterization for arithmetic equivalence which is completely reminiscent of Tate's isogeny theorem on rational elliptic curves, where the $G_{\mathbb{Q}}-$module T_K plays the role of Tate's module.

Theorem 2.5. *Let K, K_1 be two number fields. The following are equivalent:*

(i) *There is a $\mathbb{C}$-isomorphism of $T_K \cong T_{K_1}$ as $G_{\mathbb{Q}}$-modules.*
(ii) $\zeta_K(s) = \zeta_{K_1}(s)$.
(iii) *For almost all primes ℓ, $a_\ell(K) = a_\ell(K_1)$.*
(iv) *For almost all primes ℓ, $\#\mathrm{Spec}(O_K)(\mathbb{F}_\ell) = \#\mathrm{Spec}(O_{K_1})(\mathbb{F}_\ell)$ i.e., K and K_1 have the same number of $\mathbb{F}_\ell$ points.*

Proof. We first make the following observations:

- By the uniqueness theorem for Dirichlet series we have that $\zeta_K(s) = \zeta_{K_1}(s)$ implies that $a_\ell(K) = a_\ell(K_1)$ for all prime ℓ.
- Thanks to Corollary 2.3 $a_\ell(K) = a_\ell(K_1)$ for all primes ℓ implies that
$$\mathrm{Trace}(\rho_K(Frob_\ell)) = \mathrm{Trace}(\rho_{K_1}(Frob_\ell))$$
for almost all primes ℓ.
- By Chebotarev's density theorem
$$\mathrm{Trace}(\rho_K(Frob_\ell)) = \mathrm{Trace}(\rho_{K_1}(Frob_\ell))$$
for almost all primes ℓ is equivalent to $\mathrm{Trace}(\rho_K(g)) = \mathrm{Trace}(\rho_{K_1}(g))$ for all $g \in G_{\mathbb{Q}}$.
- Since Artin representations have finite images, the fact that
$$\mathrm{Trace}(\rho_K(g)) = \mathrm{Trace}(\rho_{K_1}(g))$$
for all $g \in G_{\mathbb{Q}}$ implies that ρ_K and ρ_{K_1} are isomorphic representations.
- If the representations ρ_K and ρ_{K_1} are isomorphic then, thanks to Proposition 2.2, $\zeta_K(s) = \zeta_{K_1}(s)$.

The above argument shows the equivalence between (i), (ii) and (iii). Suppose that K is defined by a monic polynomial $p(x) \in \mathbb{Z}[x]$, and suppose that $\ell \nmid \mathrm{disc}(p)$. The equivalence with (iv) follows since

$$\#\mathrm{Spec}(O_K)(\mathbb{F}_\ell) = \{\alpha \in \mathbb{F}_\ell \mid f(\alpha) = 0\} = \#\{f \in A_K(\ell) \mid f = 1\} = a_\ell(K).$$

□

Remark 2.6. Conditions (iii) or (iv) in Theorem 2.5 are a priori weaker conditions for arithmetic equivalence than the ones given by Perlis and others; even though condition (iii) seems quite natural as an equivalence for the equality between Dedekind zeta functions it's not normally mentioned in this form. Here it is the usual formulation of this equivalence:

Corollary 2.7. *Let K, K_1 be two number fields. Then K and K_1 are arithmetically equivalent if and only if for almost all rational primes ℓ*

$$\#\{f \in A_K(\ell) \mid f = 1\} = \#\{f \in A_{K_1}(\ell) \mid f = 1\}.$$

Proof. Since

$$a_\ell(K) = \#\{\mathcal{B} \in \mathrm{Max}(O_K) \mid [O_K : \mathcal{B}] = \ell\} = \#\{f \in A_K(\ell) \mid f = 1\}$$

the result follows from Theorem 2.5 □

2.0.2. Invariants under arithmetic equivalence. Some of the invariants determined by arithmetic equivalence are the degree, the discriminant, the signature, the Galois closure, the roots of unity and the unit group (see for example [6, III, §1, Theorem 1.1]). All of them can be easily explained by the Galois representation ρ_K. For instance the degree is the dimension of ρ_K, the number of real embeddings of K is $\mathrm{Trace}(\rho_K(\text{complex conjugation}))$, the discriminant is equal to the conductor of ρ_K (see [14, VI, §3, Corollary 1]), etc.

Other invariants determined under arithmetic equivalence are the rational trace form, or under some ramification conditions the integral trace form. To see how those can be deduced also from ρ_K the reader can see [7] or [10].

Quasi-conjugate subgroups. The classic group theoretical characterization of Perlis [8] and Gassmann [3] for arithmetic equivalence, see Theorem 1.3 (c)-(a), can be made quite clear from the point of view of the representation ρ_K. More precisely:

Corollary 2.8. *Let K, K_1 be number fields and let N be a Galois number field such that $KK_1 \subseteq N$. Let $G := \mathrm{Gal}(N/\mathbb{Q})$, and H, H_1 be the subgroups of G corresponding to K and K_1 via Galois correspondence. Then $\zeta_K(s) = \zeta_{K_1}(s)$ if and only if H and H_1 are quasi-conjugate in G.*

Proof. Since N is Galois over $\mathbb{Q}$ it contains $\widetilde{K}$ and $\widetilde{K}_1$. Using Artin's formalism as in the proof of Proposition 2.2 we see that $\zeta_K(s) = L(\rho_K, s) = L\left(\mathrm{Res}^{\overline{\mathbb{Q}}}_N(\rho_K), s\right) = L\left(\mathrm{Ind}^G_H 1_H, s\right)$, resp. the analogous statement for H_1. Therefore, thanks to Lemma 2.9, if H and H_1 are quasi conjugate then $\zeta_K(s) = \zeta_{K_1}(s)$. On the other hand if $\zeta_K(s) = \zeta_{K_1}(s)$ then we see, from Theorem 2.5, that the representations ρ_K and ρ_{K_1} are isomorphic. Restricting this isomorphism to $G_N = \mathrm{Gal}(\overline{\mathbb{Q}}/N)$ it follows, from Lemma

2.9, that H and H_1 are quasi-conjugate since $\mathrm{Res}_N^{\overline{\mathbb{Q}}}(\rho_K) \cong \mathrm{Ind}_H^G 1_H$ and $\mathrm{Res}_N^{\overline{\mathbb{Q}}}(\rho_K) \cong \mathrm{Ind}_{H_1}^G 1_{H_1}$ □

Lemma 2.9. *Let G be a finite group and let H and H_1 two subgroups. Then H and H_1 are quasi-conjugate if and only if* $\mathrm{Ind}_H^G 1_H \cong \mathrm{Ind}_{H_1}^G 1_{H_1}$.

Proof. Let χ_H be the character afforded by the representation $\mathrm{Ind}_H^G 1_H$ and let C be a conjugacy class in G. A calculation shows that

$$\chi_H(C) = \frac{\#(C \cap H)\#G}{\#C\#H}.$$

Taking the trivial conjugacy class we see that the order of H is determined by the representation, hence the result follows from the above equality and from the definition of quasi-conjugate subgroups(see Remark 1.2). □

3. Proofs of our results

Let K be a number field with maximal order O_K and let ℓ be a rational prime. Recall that the arithmetic type of ℓ in K is the tuple $A_K(\ell) = (f_1^K, ..., f_{g_\ell}^K)$ written in ascending order where g_ℓ^K is the number of prime factors of ℓ in O_K and the $f_i's$ are the residue degrees of ℓ. Let e_i^K be the ramification degree corresponding to the residue degree f_i^K. We call *the factorization type* of a prime ℓ the ordered pair

$$\{(f_1, ..., f_g), (e_1, ..., e_g)\}$$

where the first tuple is the arithmetic type and the second is the tuple of ramification indices corresponding to each residue degree. In this section we study the possible factorization types for primes in septic number fields.

3.1. $\mathbf{PSL_2(\mathbb{F}_7)}$ number fields. Since septic number fields that are not arithmetically solitary are $\mathrm{PSL}_2(\mathbb{F}_7)$ fields it is of interest for us to study what happens with ramification in $\mathrm{PSL}_2(\mathbb{F}_7)$ number fields.

Proposition 3.1. *Let K be a septic number field with Galois closure having Galois group isomorphic to* $\mathrm{PSL}_2(\mathbb{F}_7)$. *If ℓ is a rational prime, then its factorization type is not equal to $\mathcal{T} := \{(1,2,2),(3,1,1)\}$*

Proof. Let ℓ be a prime and suppose that its factorization type is equal to $\mathcal{T}$. Let P_1, P_2 and P_3 be the primes in O_K lying over ℓ and such that

$$\ell O_K = P_1^3 P_2 P_3.$$

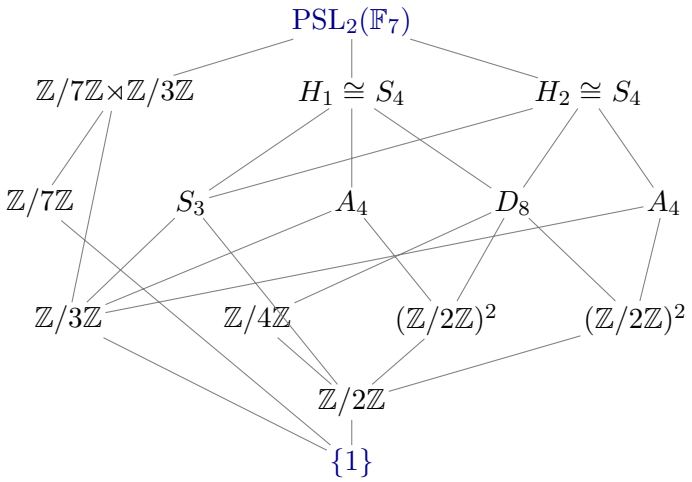
Let L be the Galois closure of K over $\mathbb{Q}$. For each $i = 1, 2, 3$ let e_i, f_i and g_i be respectively the ramification index, inertia degree and number of prime factors in O_L of the prime P_i. By the hypothesis on K and ℓ we have that

$$e_i f_i g_i = 24$$

for all $i = 1, 2, 3$. Moreover, if e, f and g are the respective values for the extension $L/\mathbb{Q}$ and the prime ℓ then

$$\begin{aligned} e &= 3e_1 = e_2 = e_3 \\ f &= f_1 = 2f_2 = 2f_3 \\ g &= g_1 + g_2 + g_3 \end{aligned}$$

It follows from the above equations that $g_2 = g_3$ and that $2g_1 = 3g_2$. In particular, $g = \frac{7}{2}g_2$ is a multiple of 7. Therefore ef, which is the order of a decomposition group over ℓ in the extension $L/\mathbb{Q}$, must be a divisor of 24. Since $3 \mid e$ and $2 \mid f$ we have that $ef \in \{6, 12, 24\}$. Now, let $D_i \leq \mathrm{Gal}(L/K)$ be a decomposition subgroup of for the prime P_i. Since decomposition groups can be extended there is, for the prime ℓ, a decomposition subgroup $E_i \leq \mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{PSL}_2(\mathbb{F}_7)$ such that $E_i \cap \mathrm{Gal}(L/K) = D_i$. Thus the group E_i, which has order ef, has for each i a subgroup of order $e_i f_i$. We recall the lattice of sub-groups of $\mathrm{PSL}_2(\mathbb{F}_7)$, modulo conjugacy:



We show separately that none of the possibilities, $\{6, 12, 24\}$, can occur as the value of ef:

- $ef = 12$. It follows from the equations above that $e_2 f_2 = 6$. Hence, the order 12 group E_i has an order 6 subgroup. This is a contradiction since A_4 has no subgroups of order 6 and, see diagram above, every subgroup of $\mathrm{PSL}_2(\mathbb{F}_7)$ of order 12 is isomorphic to A_{12}.

- $ef = 24$. It follows from the equations above that $g_1 = 3$, $e_2 f_2 = 12$ and $g_2 = g_3 = 2$. Since none of the g_i's is equal to 1 the group $\mathrm{Gal}(L/K)$ can't be conjugate to a decomposition group over ℓ; otherwise K would be the fixed field of a decomposition group of a prime $\mathcal{B}$ in O_L lying over ℓ. In particular the prime $P := \mathcal{B} \cap O_K$ would have only one prime factor in O_K, which is a contradiction since $P = P_i$

for some i. Therefore we may assume that E_i is not conjugate to $\mathrm{Gal}(L/K)$. Looking at the lattice of subgroups of $\mathrm{PSL}_2(\mathbb{F}_7)$ we see that no subgroup of order 12 is the intersection of two non-conjugate subgroups of order 24.

- $ef = 6$. It follows from the equations above that $e_1 f_1 = 3$ and $e_2 f_2 = 2$. From the lattice of subgroups we see that the intersection of a group of order 24 with one of order 6 can't have order 2.

□

Proposition 3.2. *Let K be a septic number field with Galois closure having Galois group isomorphic to $\mathrm{PSL}_2(\mathbb{F}_7)$. If ℓ is a rational prime, then its factorization type is not equal to either $\{(1,2),(3,2)\}$ or $\{(1,2),(5,1)\}$.*

Proof. The case $\{(1,2),(5,1)\}$ is clear since $5 \nmid 168$. Let ℓ be a prime and suppose that its factorization type is equal to $\{(1,2),(3,2)\}$. Let P_1 and P_2 be the primes in O_K lying over ℓ and such that

$$\ell O_K = P_1^3 P_2^2.$$

Let L be the Galois closure of K over $\mathbb{Q}$. For each $i = 1, 2$ let e_i, f_i and g_i be respectively the ramification index, inertia degree and number of prime factors in O_L of the prime P_i. By the hypothesis on K and ℓ we have that

$$e_i f_i g_i = 24$$

for all $i = 1, 2$. Moreover, if e, f and g are the respective values for the extension $L/\mathbb{Q}$ and the prime ℓ then

$$\begin{aligned} e &= 3e_1 = 2e_2 \\ f &= f_1 = 2f_2 \\ g &= g_1 + g_2. \end{aligned}$$

It follows from the above equations that $4g_1 = 3g_2$. In particular, $g = \frac{7}{4} g_2$ is a multiple of 7. Therefore ef, which is the order of a decomposition group over ℓ in the extension $L/\mathbb{Q}$, must be a divisor of 24. Since $6 \mid e$ and $2 \mid f$ we have that $ef \in \{12, 24\}$. As before, we deal with each possible value of ef separately:

- $ef = 12$. It follows from the equations above that $e = 6$. Since the inertia subgroup at ℓ has order $e = 6$ and A_4 has no subgroups of order 6 this case can't happen.

- $ef = 24$. From the equations we have that $e_1 f_1 = 8$ and $e_2 f_2 = 6$. Furthermore, either $e = 12$ or $e = 6$. In the former case $e_2 = 6$ and then we would have a group of order 12, inertia, with a subgroup of order 6 which is impossible in $\mathrm{PSL}_2(\mathbb{F}_7)$. In the latter case $e_1 = 2$

and $f_1 = 4$, therefore D_1 is an order 8 group with a cyclic quotient of order 4; this is a contradiction since $\mathrm{PSL}_2(\mathbb{F}_7)$ has no such subgroup. □

Remark 3.3. Similarly to Proposition 3.2 there is no $\mathrm{PSL}_2(\mathbb{F}_7)$ septic field K and a prime ℓ such that its factorization type is $\{(1,2),(1,3)\}$. This, together with the last proposition, shows that in K the arithmetic type of a prime ℓ can never be $(1,2)$. We do not prove this here since we already have the necessary material to prove one or our main results:

Theorem 3.4. *Let K be a degree 7 number field, and let ℓ be a rational prime. Suppose that the arithmetic type of ℓ in K does not belong to*

$$\{(1,3),(1,1,2),(1,1,1,2)\}.$$

Then for any K' arithmetically equivalent to K

$$e_1^K + ... + e_g^K = e_1^{K'} + ... + e_g^{K'}.$$

Proof. Let $(f_1, ..., f_g)$ be the arithmetic type of ℓ in either field. The arithmetic type together with the ramification degrees gives a partition of 7, $f_1e_1 + ... + f_ge_g = 7$, so we analyze each partition of 7 of size g and see what are the possibilities for sum of the ramification degrees given the knowledge of the arithmetic type.

- $g = 1$.
  In this case the ramification degree is completely determined by the value of the residue degree.
- $g = 7$.
  - $1+1+1+1+1+1+1$. In this case all the ramification degrees are equal to 1.
- $g = 6$.
  - $1 + 1 + 1 + 1 + 1 + 2$. In this case all the five ramification degrees are 1 and the last one is completely determined by its corresponding residue degree.
- $g = 5$. In principle for this case one could have different ramification degrees for same arithmetic types, however the sum of the ramification degrees is the same:
  - $1 + 1 + 1 + 1 + 3$. In this case four residue degrees are 1, and so they are their corresponding ramification degrees. In either case for this partition the last residue degree determine the last ramification degree. Moreover if the last residue degree is 3 the sum of the ramification degrees is 5 otherwise it's 7.
  - $1 + 1 + 1 + 2 + 2$. In this case three residue degrees are 1, and so they are their corresponding ramification degrees. For this partition the knowledge of the arithmetic type determines the remaining ramification degrees (they are 1 or 2). On the other hand the only way in which this partition could have the same

arithmetic type of the above partition is that all the residue degrees are equal to 1(four of them are already 1 and the remaining one must divide 2 and 3). In such a case the remaining ramification degrees are equal to 2 and the sum of the ramification degrees is 7 which coincides with the previous case.

For the partitions of size $4, 3, 2$ we list all the possible candidates to factorization type:

$$\{(f_1, ..., f_g), (e_1, ..., e_g)\} \text{ where } f_1e_1 + ...f_ge_g = 7.$$

We only list possibilities where at least one of the entries in the ramification tuples is bigger than 1. We finish by collecting the sets with equal arithmetic types such that their ramification tuples add to different values.

- $g = 4$.

  - $1 + 1 + 1 + 4$: $\{(1,1,1,1),(1,1,1,4)\}, \{(1,1,1,2),(1,1,1,2)\}$.
  - $1 + 1 + 2 + 3$: $\{(1,1,1,1),(1,1,2,3)\}, \{(1,1,1,3),(1,1,2,1)\}$, $\{(1,1,1,2),(1,1,3,1)\}$.
  - $1 + 2 + 2 + 2$: $\{(1,1,1,1),(1,2,2,2)\}, \{(1,1,1,2),(1,2,2,1)\}$, $\{(1,1,2,2),(1,2,1,1)\}$.

  In this case we have the pair

  $$\{(1,1,1,2),(1,1,1,2)\}, \{(1,1,1,2),(1,1,3,1)\}$$

  with ramification sums equal to 5 and 6 respectively and the pair

  $$\{(1,1,1,2),(1,1,1,2)\}, \{(1,1,1,2),(1,2,2,1)\}$$

  with the same pattern as the first pair.

- $g = 3$.

  - $1 + 1 + 5$. $\{(1,1,1),(1,1,5)\}$.
  - $1+2+4$: $\{(1,1,1),(1,2,4)\}, \{(1,1,2),(1,2,2)\}, \{(1,1,2),(1,4,1)\}$, $\{(1,1,4),(1,2,1)\}, \{(1,2,2),(1,1,2)\}$.
  - $1 + 3 + 3$: $\{(1,1,1),(1,3,3)\}, \{(1,1,3),(1,3,1)\}$.
  - $2+2+3$: $\{(1,1,1),(1,2,3)\}, \{(1,1,2),(2,3,1)\}, \{(1,1,3),(2,2,1)\}$, $\{(1,2,2),(3,1,1)\}, \{(1,2,3),(2,1,1)\}$.

  In this case we have the pair

  $$\{(1,1,2),(1,2,2)\}, \{(1,1,2),(1,4,1)\}$$

  with ramification sums equal to 5 and 6 respectively and the pair

  $$\{(1,1,2),(1,2,2)\}, \{(1,1,2),(2,3,1)\}$$

with the same pattern as the first pair. Additionally we have

$$\{(1,2,2),(1,1,2)\},\{(1,2,2),(3,1,1)\}.$$

Since non arithmetically solitary septic number fields are $\mathrm{PSL}_2(\mathbb{F}_7)$ number fields (see for instance [5] or [12]) it follows from Proposition 3.1 that a number field that is not arithmetically solitary can not have a prime with factorization type equal to $\{(1,2,2),(3,1,1)\}$.

- $g=2$.

  · $1+6$: $\{(1,1),(1,6)\},\{(1,2),(1,3)\},\{(1,3),(1,2)\}$
  · $2+5$: $\{(1,1),(2,5)\},\{(1,5),(2,1)\},\{(1,2),(5,1)\}$
  · $3+4$: $\{(1,1),(3,4)\},\{(1,2),(3,2)\},\{(1,3),(4,1)\}$, $\{(1,4),(3,1)\},\{(2,3),(2,1)\}$.

  In this case we have the pair

  $$\{(1,3),(1,2)\},\{(1,3),(4,1)\}$$

  with ramification sums equal to 3 and 5 respectively and the trio

  $$\{(1,2),(1,3)\},\{(1,2),(3,2)\},\{(1,2),(5,1)\}.$$

  These last cases are covered thanks to Proposition 3.2. See also Remark 3.3.

□

Using that not arithmetically solitary septic fields have simple Galois group we narrow the possibilities of prime powers appearing in the discriminant of fields for which Question 1.5 could have a negative answer.

Corollary 3.5. *Let K,K' be degree 7 arithmetically equivalent number fields. Suppose ℓ is a rational prime which is not wildly ramified in either K or K', and let v_ℓ the usual ℓ-adic valuation. If $e_1^K+...+e_g^K \neq e_1^{K'}+...+e_g^{K'}$ then $v_\ell(\mathrm{disc}(O_K))\in\{2,4\}$.*

Proof. Thanks to Theorem 3.4 we see that the sum of the inertia degrees, at every prime ℓ, in either field is either 3,4 or 5. Since for non wildly ramified primes $v_\ell(\mathrm{disc}(O_K))=[K:\mathbb{Q}]-(f_1+...+f_g)$ we see that $v_\ell(\mathrm{disc}(O_K))\in\{2,3,4\}$. On the other hand a septic field with simple Galois group must have square discriminant since its Galois closure embeds in A_7, hence the result. □

Remark 3.6. From Theorem 3.4 we see that the only primes that could give a negative answer to Question 1.5 and that are wildly ramified in both fields are 2 and 3. For instance, if $\ell=2$ a similar argument as the above shows that $v_\ell(\mathrm{disc}(O_K))\in\{6,8\}$.

Finally we show that Theorem 3.4 is the best we can get in terms of Perlis and Stuart's question:

Theorem 3.7. *For each tuple $\mathcal{F} \in \{(1,3),(1,1,2),(1,1,1,2)\}$ there are examples of pairs (K,K') of non-isomorphic arithmetically equivalent number fields, and a prime ℓ, with common arithmetic type $\mathcal{F}$ in K and K' such that*

$$e_1^K + ... + e_g^K \neq e_1^{K'} + ... + e_g^{K'}.$$

Proof. For $i = 1, 2$ consider the pairs of septic number fields $(K_i,\ K_i')$ defined by the following pairs of polynomials (f_i, g_i) respectively:

- $f_1 := x^7 - 3x^6 + 4x^5 - 5x^4 + 3x^3 - x^2 - 2x + 1$ and $g_1 := x^7 - x^5 - 2x^4 - 2x^3 + 2x^2 - x + 4$.
- $f_2 := x^7 - 7x^5 - 14x^4 - 7x^3 - 7x + 2$ and $g_2 := x^7 - 14x^3 - 14x^2 + 7x + 22$.

The first two fields have discriminant $2^6 691^2$ and the second two have discriminant $2^8 7^8$. A calculation, done in MAGMA, shows that $[K_i K_i' : \mathbb{Q}] \leq 28$. Since the fields have prime degree over $\mathbb{Q}$ it follows, thanks to Theorem 3.8 below, that K_i and K_i' are arithmetically equivalent.

For the given prime ℓ, and the given field, the factorization type

$$\{(f_1, ..., f_g), (e_1, ..., e_g)\}$$

is:

(1) $\ell = 2$
   (a) $K_1;\ \{(1,3),(4,1)\}$.
   (b) $K_1';\ \{(1,3),(1,2)\}$.

(2) $\ell = 691$
   (a) $K_1; \{(1,1,1,2),(1,1,1,2)\}$.
   (b) $K_1'; \{(1,1,1,2),(2,1,2,1)\}$.

(3) $\ell = 2$
   (a) $K_2;\ \{(1,1,2),(1,4,1)\}$.
   (b) $K_2';\ \{(1,1,2),(1,2,2)\}$.

□

Theorem 3.8 (Perlis [9])**.** *Let K, K' be two number fields. Suppose that they have the same prime degree p over $\mathbb{Q}$. Then K and K' are arithmetically equivalent if and only if the degree of KK' over $\mathbb{Q}$ is strictly less than p^2.*

References

[1] Cornelissen, Gunther; Kontogeorgis, Aristides; Van der Zalm, Lotte. Arithmetic equivalence for function fields, the Goss zeta function and a generalisation. *J. Number Theory* **130** (2010), no. 4, 1000–1012. MR2600417, Zbl 1197.11112, arXiv:0906.4424, doi: 10.1016/j.jnt.2009.08.002. 558

[2] Cornellisen, Gunther; Marcolli, Matilde. Quantum statistical mechanics, L-series and anabelian geometry. Preprint, 2010. arXiv:1009.0736. 558

[3] Gassmann, Fritz. Bemerkungen zu der vorstehenden Arbeit von Hurwitz. *Math. Z.* **25** (1926), 661–675. MR1544832, JFM 52.0156.03, doi: 10.1007/BF01283860. 565

[4] Jones, John W.; Roberts, David P. A data base of number fields. *LMS J. Comput. Math.* **17** (2014), no. 1, 595–618. MR3356048, Zbl 1360.11121, arXiv:1404.0266, doi: 10.1112/S1461157014000424.

[5] Klingen, Norbert. Rigidity of decomposition laws and number fields. *J. Austral. Math. Soc. Ser. A* **51** (1991), no. 2, 171–186. MR1124549, Zbl 0745.11047, doi: 10.1017/S1446788700034182. 559, 571

[6] Klingen, Norbert. Arithmetical similarities. Prime decomposition and finite group theory. Oxford Mathematical Monographs. Oxford Science Publications. *The Clarendon Press, Oxford University Press, New York*, 1998. x+275 pp. ISBN: 0-19-853598-8. MR1638821, Zbl 0896.11042, doi: 10.1112/S0024609399236156. 565

[7] Mantilla-Soler, Guillermo. Weak arithmetic equivalence. *Canad. Math. Bull.* **58** (2015), no. 1, 115–127. MR3303214, Zbl 1312.11088, arXiv:1310.2990, doi: 10.4153/CMB-2014-036-7. 565

[8] Perlis, Robert. On the equation $\zeta_K = \zeta_{K'}$. *J. Number Theory* **9** (1977), no. 3, 342–360. MR0447188, Zbl 0389.12006, doi: 10.1016/0022-314X(77)90070-1. 559, 565

[9] Perlis, Robert. A remark about zeta functions of number fields of prime degree. *J. Reine Angew. Math.* **293/294** (1977), 435–436. MR0447189, Zbl 0352.12012, doi: 10.1515/crll.1977.293-294.435. 572

[10] Perlis, Robert. On the analytic determination of the trace form. *Canad. Math. Bull.* **28** (1985), no. 4, 422–430. MR0812117, Zbl 0578.12009, doi: 10.4153/CMB-1985-051-2. 565

[11] Perlis, Robert; Stuart, David M.A. A new characterization of arithmetic equivalence. *J. Number theory* **53** (1995), no. 2, 300–308. MR1348765, Zbl 0863.11082, doi: 10.1006/jnth.1995.1092. 560

[12] Praeger, Cheryl E. Kronecker classes of field extensions of small degree. *J. Austral. Math. Soc. Ser. A* **50** (1991), no. 2, 297–315. MR1094925, Zbl 0733.12007, doi: 10.1017/S1446788700032766. 559, 571

[13] Prasad, Dipendra. A refined notion of arithmetically equivalent number fields, and curves with isomorphic Jacobians. *Adv. Math.* **312** (2017), 198–208. MR3635810, Zbl 06713697, arXiv:1409.3173, doi: 10.1016/j.aim.2017.03.017. 558

[14] Serre, Jean-Pierre. Local fields. Translated from the French by Marvin Jay Greenberg. Graduate Texts in Mathematics, 67. *Springer-Verlag, New York-Berlin*, 1979. viii+241 pp. ISBN: 0-387-90424-7. MR0554237 (82e:12016), Zbl 0423.12016, doi: 10.1007/978-1-4757-5673-9. 565

(Guillermo Mantilla-Soler) Department of Mathematics, Universidad Konrad Lorenz, Bogotá, Colombia

gmantelia@gmail.com

This paper is available via http://nyjm.albany.edu/j/2019/25-25.html.