Graduate J. Math. **5** (2020), 28 – 37

On locally GCD equivalent number fields

Francesco Battistoni

Abstract

Local GCD Equivalence is a relation between extensions of number fields which is weaker than the classical arithmetic equivalence. It was originally studied by Lochter under the name "Weak Kronecker Equivalence." Among the many results he got, Lochter discovered that number fields extensions of degree ≤ 5 which are locally GCD equivalent are in fact isomorphic. This fact can be restated saying that number fields extensions of low degree are uniquely characterized by the splitting behaviour of a restricted set of primes: in particular, also extensions of degree 3 and 5 are uniquely determined by their inert primes, just like the quadratic fields.

The goal of this note is to present this rigidity result with a different proof, which insists especially on the densities of sets of prime ideals and their use in the classification of number fields up to isomorphism. Alongside Chebotarev's Theorem, no harder tools than basic Group and Galois Theory are required.

MSC 2010. Primary: 11R16, 11R44; Secondary: 11R45.

1 Introduction

1.1 Equivalence relations defined with splitting types

Let K/F be a finite extension of number fields, and let $\mathcal{O}_K$ and $\mathcal{O}_F$ be the corresponding rings of integers. Given a non zero prime ideal $\mathfrak{p} \subset \mathcal{O}_F$, a classic problem in Algebraic Number Theory consists in studying the factorization of the ideal

$$\mathfrak{p}\mathcal{O}_K = \mathcal{Q}_1 \cdots \mathcal{Q}_r$$

as finite product of prime ideals $\mathcal{Q}_i \subset \mathcal{O}_K$.

If $\mathfrak{p}$ is unramified in K (i.e. the primes $\mathcal{Q}_i$ are all distinct) part of the desired information is provided by the inertia degree $f_i = [\mathcal{O}_K/\mathcal{Q}_i : \mathcal{O}_F/\mathfrak{p}]$ where $\mathcal{O}_F/\mathfrak{p} \subseteq \mathcal{O}_K/\mathcal{Q}_i$ is an extension of finite fields: the r-tuple of inertia degrees $(f_1, \dots, f_r) =: f_K(\mathfrak{p})$ is called the *splitting type of* $\mathfrak{p}$ *in* K.

Splitting types have been involved in several problems, some of which are the following: are number fields uniquely defined by the splitting type of primes? If two number fields share a common set of primes with specified splitting type, are they isomorphic? If not, do they share some common number theoretic invariant?

Answers to these questions have been provided by studying equivalence relations between number fields defined by splitting types, an example given by arithmetical equivalence. Two number field extensions K/F and L/F are said to be *arithmetically equivalent over* F if $f_K(\mathfrak{p}) = f_L(\mathfrak{p})$ for every prime $\mathfrak{p} \subset \mathcal{O}_F$ which is unramified in both K and L.

This relation is strong enough to provide interesting arithmetical characterizations. In fact, let K and L be F-arithmetically equivalent fields: then, Perlis [9] proved the following rigidity results.

- K and L have the same degree $[K : F] = [L : F]$ over F.
- If $[K : F] \leq 6$ and $[L : F] \leq 6$, then K and L are isomorphic.
- If one between K/F and L/F is Galois, then $K = L$.

What happens if one decides to weaken the conditions imposed on the equivalence relation and the splitting types? An example is given by *Kronecker equivalence*. Given K/F and L/F, we say that K and L are F-Kronecker equivalent if

$$1 \in f_K(\mathfrak{p}) \leftrightarrow 1 \in f_L(\mathfrak{p})$$

for every prime $\mathfrak{p} \subset \mathcal{O}_F$ unramified in both K and L.

This relation is weaker than arithmetical equivalence, and this suggests that the characterizations provided by arithmetical equivalence may either not be obtained or need stronger additional hypotheses to be reached. Jehne [2] proved that, if K and L are F-Kronecker equivalent, the following things happen.

- K and L may have different degrees over F.
- If K/F is Galois, then L/F may not be Galois.
- If both K/F and L/F are Galois, then $K = L$.

Klingen [3] showed that Kronecker equivalence may be formulated in a different way: K and L are F-Kronecker equivalent if and only if, for every prime $\mathfrak{p} \subset \mathcal{O}_F$ which is unramified in both K and L, we have the equality of additive semigroups

$$\begin{aligned} & \mathbb{N}f_{1,K}(\mathfrak{p}) + \mathbb{N}f_{2,K}(\mathfrak{p}) + \cdots + \mathbb{N}f_{t,K}(\mathfrak{p}) \\ = \; & \mathbb{N}f_{1,L}(\mathfrak{p}) + \mathbb{N}f_{2,L}(\mathfrak{p}) + \cdots + \mathbb{N}f_{t',L}(\mathfrak{p}) \end{aligned} \tag{1.1}$$

where $f_K(\mathfrak{p}) := (f_{1,K}(\mathfrak{p}), \ldots, f_{t,K}(\mathfrak{p}))$, and $f_L(\mathfrak{p}) := (f_{1,L}(\mathfrak{p}), \ldots, f_{t',L}(\mathfrak{p}))$.

This suggests the chance of defining an even weaker relation, introduced firstly by Lochter [8], called *local GCD equivalence*. Two number fields K and L are locally GCD equivalent over a number field F if

$$\begin{aligned} & \gcd(f_{1,K}(\mathfrak{p}), \ldots, f_{t,K}(\mathfrak{p})) \\ = \; & \gcd(f_{1,L}(\mathfrak{p}), \ldots, f_{t',L}(\mathfrak{p})) \end{aligned} \tag{1.2}$$

for every prime $\mathfrak{p} \subset \mathcal{O}_F$ which is unramified in both K and L.

This relation, which is the main object of study of this note, was originally called *Weak Kronecker Equivalence*, since condition (1.1) implies condition (1.2); the name *Local GCD Equivalence* has been introduced afterwards by Linowitz, McReynolds and Miller [7].

Lochter's work focused on the arithmetical properties implied by the local GCD equivalence: among the several results, he proved the following rigidity theorem.

Theorem 1.1. *Let K/F and L/F be number field extensions which are locally GCD equivalent over F.*

a) If K/F and L/F are both Galois, then $K = L$.

b) If $[K : F], [L : F] \leq 5$, then K and L are isomorphic.

Our interest in this result is motivated by a different formulation of Theorem 1.1 and a new approach to its proof which shall be presented in the next lines.

1.2 Local GCD equivalence, inert primes and prime densities

Let K/F be a number field extension, and consider the corresponding set of inert primes, i.e. the prime ideals $\mathfrak{p} \subset \mathcal{O}_F$ such that $\mathfrak{p}\mathcal{O}_K$ is still a prime ideal in $\mathcal{O}_K$ (warning: this set may be empty). It is known that, if $[K : F] = 2$, then there exist infinite inert primes and they determine uniquely K; one could wonder if something similar holds for extensions of higher degree, like cubic extensions.

An equivalent formulation of the problem is the following: given K/F and L/F which have the same inert primes, are then K and L isomorphic? We do not expect this to be true for higher degrees, but possibly one could recover some result when dealing with extensions of low degree. In this setting, we notice that we are considering a couple of number fields which share a common set of prime ideals, and not only this set may be infinite, but it also admits a proper "density" in the set of all prime ideals (in a sense which is going to be specified later). So what can be said about fields with common set of primes having a prescribed density?

An answer to this problem, however not stated directly and with no references elsewhere, is provided exactly by Lochter's result in Theorem 1.1, thanks to an equivalent formulation which involves explicitly the inert primes.

Theorem 1.2. *Let K/F and L/F be number fields extensions of degree 2, 3 or 5. If K and L have the same inert primes, then they are isomorphic.*
If $[K : F] = [L : F] = 4$, and K and L share the same inert primes and the same primes with splitting type $(2, 2)$, then K and L are isomorphic.

The aim of this note is to give a new proof of Theorem 1.1 by showing its equivalence with Theorem 1.2 and using the approach typical of this new formulation, which is different from Lochter's original one. While he relied consistently on several tools of Representation Theory, we obtained this result by comparing the prime densities of equivalent fields: in fact, besides Chebotarev's Theorem, no other strong tools are required in this new proof, and we need just basic Group and Galois Theory.

Section 2 presents the technical tools necessary for our new proof: Chebotarev's Theorem, recalls from Algebraic Number Theory, references for the properties of the groups which will be considered in later sections. Furthermore, this section contains a direct proof of Theorem 1.1.a and an explicit example of computation of prime densities.

Section 3 gives a summary of the two procedures under which all the considered cases of local GCD equivalence can be reduced to isomorphism, and which will be applied consistently in later sections. Sections 4, 5 and 6 prove Theorem 1.1.b by showing in detail how locally GCD equivalent extensions of degree 3, 4 and 5 are actually isomorphic: this is done with the techniques and procedures described in Section 2 and 3. Finally, in Section 7 we present some final remarks and considerations.

1.3 Notation and definitions

• Given a number field extension K/F and an unramified prime $\mathfrak{p} \subset \mathcal{O}_F$, its *splitting type* is the t-tuple $f_K(\mathcal{P}) := (f_{1,K}(\mathfrak{p}), \ldots, f_{t,K}(\mathfrak{p}))$ given by the inertia degrees $f_{1,K} \leq f_{2,K} \leq \cdots f_{t,K}$ of the prime factors $\mathfrak{q}_1, \ldots, \mathfrak{q}_t$ of $\mathfrak{p}\mathcal{O}_K$.

• If $\mathfrak{p}$ is unramified and $f_K(\mathfrak{p}) = (1, \ldots, 1)$, then $\mathfrak{p}$ is said to be a *splitting prime*; if $f_K(\mathfrak{p}) = ([K : F])$, then $\mathfrak{p}$ is said to be an *inert prime*.

• A splitting type of the form $\underbrace{(f, \ldots, f)}_{n \text{ times}}$ will be written in the form $(f \times n)$. In a Galois extension, every splitting type has this form.

• Given a number field extension K/F, its *Galois closure* $\widehat{K}$ is the smallest Galois extension of F containing K. Its Galois group will be denoted as G_K.

• Given a set A of prime ideals of $\mathcal{O}_F$, its *prime density* is the number (if it exists)

$$\begin{aligned}\delta_{\mathcal{P}}(A) &:= \lim_{x\to+\infty} \frac{\#\{\mathfrak{p}\in A\colon \mathrm{N}(\mathfrak{p})\le x\}}{\#\{\mathfrak{p}\subset\mathcal{O}_F\colon \mathrm{N}(\mathfrak{p})\le x\}}\\ &= \lim_{x\to+\infty} \frac{\#\{\mathfrak{p}\in A\colon \mathrm{N}(\mathfrak{p})\le x\}}{x/\log x}\end{aligned}$$

where $\mathrm{N}(\mathfrak{p}) := \#\mathcal{O}_F/\mathfrak{p}$.

• A property P holds *for almost all primes in a set A of primes* if P holds for every prime in A up to a subset of A with null prime density (in particular, whenever the set of exceptions is finite).

• Given $\mathfrak{p}\subset\mathcal{O}_F$, the *residue field of* $\mathfrak{p}$ is the finite field $\mathbb{F}_{\mathfrak{p}} := \mathcal{O}_F/\mathfrak{p}$.

• Given a finite Galois extension L/F with Galois group G, an unramified prime $\mathfrak{p}\subset\mathcal{O}_F$ and the prime factors $\mathfrak{q}_1,\dots,\mathfrak{q}_t$ of $\mathfrak{p}\mathcal{O}_L$, the *decomposition group of* $\mathfrak{q}_i$ is the set $G_{\mathfrak{q}_i} := \{\sigma\in G\colon \sigma(\mathfrak{q}_i)=\mathfrak{q}_i\}$. The groups $G_{\mathfrak{q}_i}$ are cyclic subgroups of G and are conjugated between them.

• For every $i=1,\dots,t$ there is a group isomorphism

$$\Psi_i : G_{\mathfrak{q}_i} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{q}_i}/\mathbb{F}_{\mathfrak{p}}) = \langle\phi_i\rangle$$

where $\phi_i : \mathbb{F}_{\mathfrak{q}_i}\to\mathbb{F}_{\mathfrak{q}_i}$ is the Frobenius automorphism of the finite field $\mathbb{F}_{\mathfrak{q}_i}$.

• The *Frobenius symbol of* $\mathfrak{p}$ is the conjugation class $(L/F,\mathfrak{p}) := \{\Psi_i^{-1}(\phi_i)\colon i=1,\dots,t\}$.

1.4 Acknowledgements

The author thanks Harry Smit from the University of Utrecht, for several discussions about Local GCD Equivalence, Sandro Bettin from University of Genova for the suggestion that prime densities could be relevant for this problem, and Simone Maletto, for interesting insights about this topics.

2 Technical tools and first characterizations

2.1 Computing prime densities

Let us begin recalling the only "heavy" theorem needed, which is the classic Chebotarev's Theorem, necessary for any density argument involving primes in number fields.

Theorem 2.1 (Chebotarev). *Let L/F be a finite Galois extension of number fields with Galois group G. Let $C\subset G$ be a union of conjugation classes in the group. Then, the set of primes $\mathfrak{p}\subset\mathcal{O}_F$ such that $(L/F,\mathfrak{p})=C$ is infinite and has prime density equal to $\#C/\#G$.*

Proof. See Chapter VIII, Section 4, Theorem 10 of [6]. □

It follows that the set $S_f := \{\mathfrak{p}\subset\mathcal{O}_F\colon f_L(\mathfrak{p}) = (f,\dots,f)\}$ has prime density equal to $n_f/\#G$, where n_f is the number of elements with order f in G. In particular, splitting primes have density $1/[L:F]$ in a Galois extension L/F.

If we are interested in similar computations also for non-Galois extensions, we need the following proposition.

Proposition 2.2. *Let E/F be a finite Galois number field extension with Galois group G, and let L/F be an intermediate extension. Let $H := \mathrm{Gal}(E/L)$.*
Let $X := \{H, g_1H\dots, g_rH\}$ be the set of left cosets of H. Let $\mathfrak{p}\subset\mathcal{O}_F$ and let $g\in G$ be an element of the Frobenius symbol of $\mathfrak{p}$ in G. Consider the action of the group generated by g on X given by left multiplication. Then there is a bijection

$$\{\textit{orbits of the action}\} \leftrightarrow \{\textit{primes of } \mathcal{O}_L \textit{ dividing } \mathfrak{p}\}.$$

Moreover, if $(f_1,\dots,f_t)$ is the t-tuple representing the size of the orbits, then $f_L(\mathfrak{p}) = (f_1,\dots,f_t)$.

Proof. See Chapter III, Prop.2.8 of [1]. □

In particular, the density of inert primes is given by the number of elements of order $[L:F]$ in G.

Remark 2.3. From now on, we can assume that every prime $\mathfrak{p}$ is unramified in any given extension, because ramified primes occur only in a finite amount once the extensions are fixed, and a finite set does not modify the values of the prime densities.

Chebotarev's Theorem and Proposition 2.2 are the tools which allow us to compute the prime densities in number field extensions of degree less or equal than 5. At this purpose, we also need a complete knowledge of the transitive subgroups of the permutation groups S_n with $n\le 5$, because these are the only possible choices for the Galois groups $\mathrm{Gal}(\widehat{K}/F)$ of the Galois closures we are going to consider. The list of these groups and the respective properties can be found in several number fields databases, like Klüners-Malle's database [5].

In the next lines we illustrate an instance of prime density computation.

Example 2.4. Let K/F be an extension of degree 3 which is not Galois. This means that the Galois closure $\widehat{K}$ has Galois group $G_K = S_3 = \langle\sigma,\tau|\sigma^2=\tau^3=(\sigma\tau)^2=1\rangle$, and the field K corresponds to a subgroup $H\le S_3$ of order 2; assuming $H=\langle\sigma\rangle$, the left cosets of H are H,τH and τ^2H.

If we study the action of the cyclic subgroups of S_3 on these cosets given by left multiplication, we notice that the only elements giving a unique, transitive orbit are τ and τ^2, which form a conjugation class. Thus, by

Chebotarev's Theorem and Proposition 2.2, the density of inert primes in K is $2/6 = 1/3$.

Similar computations allow to compute every prime density for every splitting type in extensions of degree ≤ 5.

2.2 Splitting primes and equivalence of Galois fields

Let us recall now a few results from Algebraic Number Theory, which combined will give the proof of Theorem 1.1.a.

Lemma 2.5. *Let K/F and L/F be finite number field extensions and let KL/F be its composite extension. Then $\mathfrak{p} \subset \mathcal{O}_F$ splits completely in KL if and only if it splits completely in both K and L.*

Proof. See Chapter III, Prop. 2.5, 2.6 of [1]. □

Corollary 2.1. *Let K/F be a finite number field extension and let $\widehat{K}/F$ be its Galois closure with group G_K. Then an unramified prime $\mathfrak{p} \subset \mathcal{O}_F$ splits completely in K if and only if it splits completely in $\widehat{K}$.*

Proof. We know that $\widehat{K}$ is the compositum field of all the fields $\sigma(K)$ where $\sigma \in \mathrm{Gal}(\widehat{K}/F)$; but if a prime splits completely in K, it must be totally split in $\sigma(K)$ as well. The claim follows then from Lemma 2.5. □

Corollary 2.2. *Let K/F and L/F be finite Galois extensions of number fields and assume that they share the same set of splitting primes (up to exceptions of null prime density). Then K and L coincide.*

Proof. Let KL/F be the composite Galois extension. By the previous lemma it follows, up to exceptions of null prime density,

$$\{\mathfrak{p} \subset \mathcal{O}_F \colon f_{KL}(\mathfrak{p}) = (1, \ldots, 1)\} = \{\mathfrak{p} \subset \mathcal{O}_F \colon f_K(\mathfrak{p}) = (1, \ldots, 1) \text{ and } f_L(\mathfrak{p}) = (1, \ldots, 1)\}.$$

Applying Chebotarev's Theorem, the identity above gives the equality

$$\frac{1}{[K : F]} = \frac{1}{[KL : F]} = \frac{1}{[L : F]}$$

which immediately implies $K = KL = L$. □

Proof of Theorem 1.1.a. If K/F is Galois, every prime ideal $\mathfrak{p} \subset \mathcal{O}_F$ unramified in K has splitting type equal to an r-tuple formed by identical numbers. Thus, $1 \in f_K(\mathfrak{p})$ if and only if $\mathfrak{p}$ is a splitting prime in K.

If K/F and L/F are both Galois and they are locally GCD equivalent, then K and L share the same splitting primes, and so $K = L$ by Corollary 2.2. □

2.3 Equivalence in degree 2

We consider now the (easy) case of local GCD equivalence between quadratic fields, and we give also some density results concerning these fields.

We recall that the only splitting types available for a quadratic field are $(1, 1)$ and (2).

Proposition 2.6. *Let K and L be two quadratic fields over F.*

1) If K and L are locally GCD equivalent over F, then they are isomorphic.

2) If $\{\mathfrak{p} \subset \mathcal{O}_F \colon f_K(\mathfrak{p}) = f_L(\mathfrak{p}) = (1, 1)\}$ has prime density strictly greater than $1/4$, then $K = L$.

3) The set $\{\mathfrak{p} \subset \mathcal{O}_F \colon f_K(\mathfrak{p}) = f_L(\mathfrak{p})\}$ has prime density $\geq 1/2$. K and L are equal if and only if the strict inequality holds.

Proof.

1) This follows by Theorem 1.1.a because every quadratic extension of characteristic 0 fields is Galois.

2) Assume that $K \neq L$: then their composite field KL is a Galois field of degree 4 over F, and it would be

$$\{\mathfrak{p} \subset \mathcal{O}_F \colon f_{KL}(\mathfrak{p}) = (1, 1, 1, 1)\} = \{\mathfrak{p} \subset \mathcal{O}_F \colon f_K(\mathfrak{p}) = f_L(\mathfrak{p}) = (1, 1)\}.$$

But this is a contradiction, since the first set has prime density equal to $1/4$, while the second one has a greater density by the assumption.

3) Let $K = F[x]/(x^2 - \alpha)$ and $L = F[x]/(x^2 - \beta)$, with $\alpha \neq \beta$: the set $\{\mathfrak{p} \subset \mathcal{O}_F \colon f_K(\mathfrak{p}) = f_L(\mathfrak{p})\}$ is identified with the set of splitting primes in $F[x]/(x^2 - \alpha\beta)$. The claim follows immediately. □

3 The two procedures

In this interlude section we give a short overview of the procedures which we shall use to prove Theorem 1.1.b. The proof presents several distinct cases, each one consisting of two locally GCD equivalent extensions which in the end are seen to be isomorphic. Nonetheless, all these cases present many similarities and in fact they can be solved by employing two specific procedures.

We present now these two different techniques, each one marked by a symbol: in the next sections, every studied case is meant to be solved with the procedure related to the corresponding symbol.

(•) We have called the technique marked with this symbol "technique of the *Galois companion*", and it has proved to be useful whenever one deals with equivalent extensions of degree ≤ 4. The procedure runs as follows.

Given two equivalent extensions K and L, we look for two non trivial Galois subextensions $K_n \subset K$ and $L_n \subset L$ such that $[K_n : F] = [L_n : F] = n$ and $\mathrm{Gal}(K_n/F) = \mathrm{Gal}(L_n/F)$. Using group actions like in Proposition 2.2, one is able to recover information on the density of primes with certain splitting types which are shared by K_n and L_n, and these common primes force $K_n = L_n$ thanks to either Theorem 1.1.a or Proposition 2.6.

From this equality, one employs again prime density arguments in order to get $\widehat{K} = \widehat{L}$, and the last equality gives the desired isomorphism $K \simeq L$.

(**) This symbol means that we are using a different technique, which we call "technique of the *Big Galois Closure*": this second procedure is needed when we deal with equivalent extensions of degree 5 such that their Galois closures have group equal to either A_5 or S_5. Such cases cannot be solved by looking for a Galois companion, because the considered fields do not have non trivial Galois subextensions (or, in the case S_5, the unique quadratic subextension does not provide enough information).

The procedure works as follows: consider two equivalent fields K and L, and assume that their are not isomorphic. If $K \cap L$ is a field of degree > 2, then is not Galois because of the group assumptions and by Corollary 2.1 it must be a field with the same splitting primes of $\widehat{K}$ and $\widehat{L}$, forcing then $\widehat{K} = \widehat{L}$ and $K \simeq L$.

If this is not the case, one considers the composite field KL and take its Galois closure $\widehat{KL}$: its Galois group turns out to be a subgroup with low index of $G_K \times G_L$ which has the same number n_5 of elements of order 5 as the bigger group. Applying Chebotarev's Theorem and Proposition 2.2 to the tower of extensions $\widehat{KL}/K/F$, the density of the inert primes in K is then equal to $n_5/(\#\,\mathrm{Gal}(\widehat{KL}/F))$; this density results to be strictly smaller than true density of inert primes in all the considered cases, thus giving a contradiction.

4 Equivalence in degree 3

4.1 Galois Groups for cubic fields

Let K be a field of degree 3 over F, and let $\widehat{K}$ be its Galois closure with Galois group G_K. The group G_K can be one of the following:

(i) $G_K = C_3$, the cyclic group of order 3. Then $K = \widehat{K}$ is a cubic Galois extension over F. The only possible splitting types are $(1,1,1)$ and (3), and furthermore

$$\delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(\mathfrak{p}) = (1,1,1)\} = 1/3,$$

$$\delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(\mathfrak{p}) = (3)\} = 2/3.$$

(ii) $G_K = S_3$, the symmetric group with 6 elements. Then $\widehat{K}$ has degree 6 over F, it contains three isomorphic cubic extensions over F and a quadratic extension K_2/F.

Furthermore there are infinitely many primes with splitting type $(1,2)$, each one having Frobenius symbol equal to the elements of order 2 in S_3.

Looking at the densities in detail, one has:

$$\delta_{\mathfrak{p}}\{p\colon f_K(\mathfrak{p}) = (1,1,1)\} = 1/6,$$

$$\delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(\mathfrak{p}) = (1,2)\} = 1/2,$$

$$\delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(\mathfrak{p}) = (3)\} = 1/3.$$

All density computations are derived from Chebotarev's Theorem and Proposition 2.2.

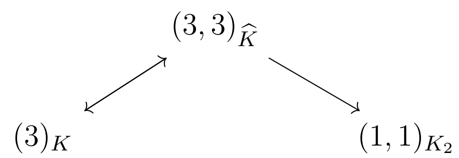
4.2 Locally GCD equivalent cubic fields

The equivalence problem in this degree can be solved by means of the sole Galoic companions technique.

Let K and L be two cubic fields over F which are locally GCD equivalent. It is almost immediate to see that if one of them (assume K) is Galois, then the other extension is Galois, because of the density of the inert primes. But then $K = L$ for Theorem 1.1.a.

• Let us assume that both K and L are not Galois. Consider their Galois closures $\widehat{K}$ and $\widehat{L}$, and the quadratic Galois subextensions K_2 and L_2, which are the Galois companions.

Using Proposition 2.2, it is easy to show the following correspondence among the splitting types of the fields involved:



One gets the following identity:

$$\begin{aligned} &\{\mathfrak{p}\colon f_{K_2}(\mathfrak{p}) = (1,1), f_K(\mathfrak{p}) = (3)\} \\ &= \{\mathfrak{p}\colon f_{L_2}(\mathfrak{p}) = (1,1), f_L(\mathfrak{p}) = (3)\}. \end{aligned} \tag{4.1}$$

This implies that $\{\mathfrak{p}\colon f_{K_2}(\mathfrak{p}) = (1,1) = f_{L_2}(\mathfrak{p})\}$ has prime density greater than 1/3, and by Proposition 2.6 one has $K_2 = L_2$.

The remaining splitting primes in K_2, which have prime density equal to $1/2 - 1/3 = 1/6$, are exactly the splitting primes in $\widehat{K}$. But this fact, together with $K_2 = L_2$ and Equality (4.1), force $\widehat{K}$ and $\widehat{L}$ to have the same splitting primes, i.e. $\widehat{K} = \widehat{L}$, which in turn implies $K \simeq L$ (because the cubic extensions over F in $\widehat{K}/F$ are isomorphic).

5 Equivalence in degree 4

5.1 Galois groups for quartic fields

Let K be a field of degree 4 over F, and let $\widehat{K}$ be its Galois closure with Galois group G_K. The group G_K can be one of the following:

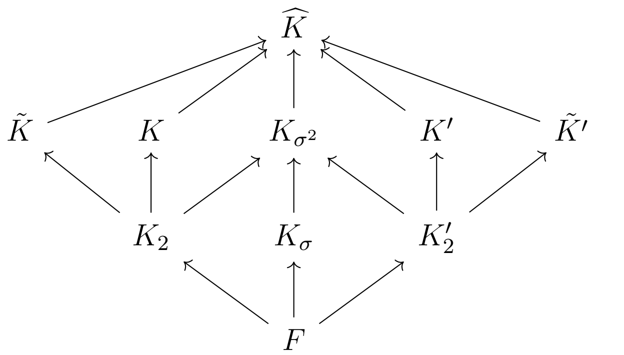
(i) $G_K = C_4$, the cyclic group of order 4. Then $K = \widehat{K}$ is Galois over F and the splitting types and densities are as follows:

$$\begin{aligned} \delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(\mathfrak{p}) = (1,1,1,1)\} &= 1/4, \\ \delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(\mathfrak{p}) = (2,2)\} &= 1/4, \\ \delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(\mathfrak{p}) = (4)\} &= 1/2. \end{aligned}$$

(ii) $G_K = C_2 \times C_2$: then $K = \widehat{K}$ is Galois over F and

$$\begin{aligned} \delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(\mathfrak{p}) = (1,1,1,1)\} &= 1/4, \\ \delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(\mathfrak{p}) = (2,2)\} &= 3/4. \end{aligned}$$

(iii) $G_K = D_4 := \langle \sigma, \tau | \sigma^4 = \tau^2 = 1, \tau\sigma\tau = \sigma^3 \rangle$. Then $\widehat{K}$ has degree 8 over F, it contains 5 quartic fields and 3 quadratic fields, the lattice of sub-extensions being as follows:



(5.1)

The quartic fields form 3 distinct classes of isomorphism: $\{K, \tilde{K}\}$, $\{K', \tilde{K}'\}$ and $\{K_{\sigma^2}\}$. The extension K_{σ^2}/F is Galois with Galois group $C_2 \times C_2$.

Assuming that $\mathrm{Gal}(\widehat{K}/K) = \langle \tau \rangle$, Proposition 2.2 yields

$$\begin{aligned} \delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(\mathfrak{p}) = (1,1,1,1)\} &= \delta_{\mathcal{P}}\{\mathfrak{p}\colon (\widehat{K}/F, \mathfrak{p}) = 1_{D_4}\} \\ &= 1/8, \end{aligned}$$

$$\begin{aligned} \delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(p) = (1,1,2)\} &= \delta_{\mathcal{P}}\{\mathfrak{p}\colon (\widehat{K}/F, \mathfrak{p}) = \{\tau, \sigma^2\tau\}\} \\ &= 1/4, \end{aligned}$$

$$\delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(p) = (2,2), (\widehat{K}/F, \mathfrak{p}) = \sigma^2\} = 1/8,$$

$$\delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(p) = (2,2), (\widehat{K}/F, \mathfrak{p}) = \{\sigma\tau, \tau\sigma\}\} = 1/4,$$

$$\begin{aligned} \delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(p) = (4)\} &= \delta_{\mathcal{P}}\{\mathfrak{p}\colon (\widehat{K}/F, \mathfrak{p}) = \{\sigma, \sigma^3\}\} \\ &= 1/4. \end{aligned}$$

If $\mathrm{Gal}(\widehat{K}/K) = \langle \sigma\tau \rangle$, simply reverse the roles of τ and $\sigma\tau$ in the description above.

(iv) $G = A_4$, the alternating group with 12 elements. Then $\widehat{K}$ has degree 12 over F, it contains 4 quartic fields (each one isomorphic to the others) and a Galois cubic extension K_3/F. There are no inert primes, and the splitting types and densities are the following:

$$\begin{aligned} \delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(\mathfrak{p}) = (1,1,1,1)\} &= 1/12, \\ \delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(\mathfrak{p}) = (1,3)\} &= 2/3, \\ \delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(\mathfrak{p}) = (2,2)\} &= 1/4. \end{aligned}$$

(v) $G = S_4$: then $\widehat{K}$ has degree 24 over F and contains a Galois extension K_6/F of degree 6, while all the quartic extensions over F contained in $\widehat{K}$ are isomorphic. The splitting types and decomposition are as follows:

$$\begin{aligned} \delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(\mathfrak{p}) = (1,1,1,1)\} &= 1/24, \\ \delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(\mathfrak{p}) = (1,1,2)\} &= 1/4, \\ \delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(\mathfrak{p}) = (1,3)\} &= 1/3, \\ \delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(\mathfrak{p}) = (2,2)\} &= 1/8, \\ \delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(\mathfrak{p}) = (4)\} &= 1/4. \end{aligned}$$

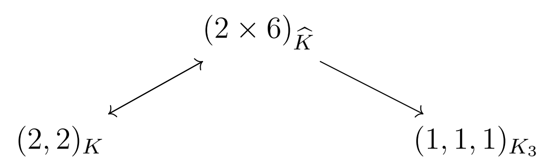
All densities are computed with Proposition 2.2. These data immediately show that if K/F and L/F are locally GCD equivalent quartic extensions, then they must have the same Galois closure.

5.2 Locally GCD equivalent quartic fields

Just like for the previous degree, searching for Galois companions will be enough to study the equivalence between extensions of degree 4.

As mentioned before, we only study locally GCD equivalent quartic extensions K/F and L/F with same Galois group. This immediately implies that whenever one of the extensions is Galois, then the equivalence is actually an equality.

• $G = A_4$: Consider the cubic Galois companions K_3/F and L_3/F associated to K and L respectively. Proposition 2.2 yields the following behaviour on the splitting types:



Thus one gets the identity

$$\begin{aligned}&\{\mathfrak{p}\colon f_{K_3}(\mathfrak{p})=(1,1,1), f_K(\mathfrak{p})=(2,2)\}\\ =\ &\{\mathfrak{p}\colon f_{L_3}(\mathfrak{p})=(1,1,1), f_L(\mathfrak{p})=(2,2)\}.\end{aligned} \tag{5.2}$$

The sets above have prime density $1/4$, and this forces $K_3 = L_3$; if this was not true, the composite Galois extension KL/F would have degree 9. But being

$$\begin{aligned}&\{\mathfrak{p}\colon f_{K_3L_3}(\mathfrak{p})=(1\times 9)\}\\ =\ &\{\mathfrak{p}\colon f_{K_3}(\mathfrak{p})=f_{L_3}(\mathfrak{p})=(1,1,1)\},\end{aligned}$$

the left hand side would have prime density equal to $1/9$, which is in contradiction with Equality (5.2).

The remaining splitting primes in K_3 have density $1/3-1/4=1/12$ and are precisely the splitting primes in the Galois closure $\widehat{K}$. Thus, equality (5.2) and $K_3 = L_3$ force $\widehat{K}$ and $\widehat{L}$ to have the same splitting primes, i.e. $\widehat{K}=\widehat{L}$, which implies $K\simeq L$.

• The case $G = S_4$ is completely similar: one associates to K the unique Galois sextic extension K_6/F contained in $\widehat{K}$, and using the densities of primes $\mathfrak{p}$ with $f_K(\mathfrak{p}) = (2,2)$ one forces $K_6 = L_6$ and from that $\widehat{K}=\widehat{L}$, which in turn gives $K\simeq L$.

• $G = D_4$: Let us take K/F and L/F locally GCD equivalent quartic extensions with Galois closures $\widehat{K}$ and $\widehat{L}$ and Galois group D_4. We follow the notations of diagram (5.1) for the sub-extensions of $\widehat{K}$ and $\widehat{L}$.

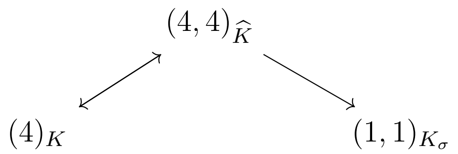
Consider the subfield $K_2\subset K$: using Proposition 2.2, it is immediate to see that, if $f_K(\mathfrak{p}) = (4)$, then $f_{K_2}(\mathfrak{p}) = (2)$; in the same way, a prime ideal $\mathfrak{p}$ such that $f_K(\mathfrak{p})\in\{(1,1,1,1),(1,1,2)\}$ has splitting type $f_{K_2}(\mathfrak{p}) = (1,1)$. These facts, together with the local GCD equivalence between K and L, yield the equalities:

$$\begin{aligned}&\{\mathfrak{p}\colon f_{K_2}(\mathfrak{p})=(2), f_K(\mathfrak{p})=(4)\}\\ &=\{\mathfrak{p}\colon f_{L_2}(\mathfrak{p})=(2), f_L(\mathfrak{p})=(4)\},\end{aligned} \tag{5.3}$$

$$\begin{aligned}&\{\mathfrak{p}\colon f_{K_2}(\mathfrak{p})=(1,1), f_K(\mathfrak{p})\in\{(1,1,1,1),(1,1,2)\}\}\\ &=\{\mathfrak{p}\colon f_{L_2}(\mathfrak{p})=(1,1), f_L(\mathfrak{p})\in\{(1,1,1,1),(1,1,2)\}\}.\end{aligned} \tag{5.4}$$

The sets in Equality (5.3) have prime density equal to $1/4$, while the ones in Equality (5.4) have prime density equal to $3/8$. This shows that K_2 and L_2 have the same splitting type on at least $5/8$ of the primes, and so $K_2 = L_2$ by Proposition 2.6.

Let us consider now the field K_σ. Using Proposition 2.2, it is possible to show the following behaviour:



Thus one obtains the equality

$$\begin{aligned}&\{\mathfrak{p}\colon f_{K_\sigma}(\mathfrak{p})=(1,1), f_K(\mathfrak{p})=(4)\}\\ =\ &\{\mathfrak{p}\colon f_{L_\sigma}(\mathfrak{p})=(1,1), f_L(\mathfrak{p})=(4)\}\end{aligned} \tag{5.5}$$

and the sets above have prime density equal to $1/4$.

Furthermore, the set of primes $\{\mathfrak{p}\colon f_K(\mathfrak{p})=f_L(\mathfrak{p})=(1,1,1,1)\}$ has positive density $\varepsilon>0$ (because it corresponds to the set of splitting primes in the composite extension KL) and, thanks to the fact that these primes split completely also in $\widehat{K}$ and $\widehat{L}$, it is clear that for each one of these primes we have $f_{K_\sigma}(\mathfrak{p}) = f_{L_\sigma}(\mathfrak{p}) = (1,1)$. This result, together with Equality (5.5), implies that K_σ and L_σ share a set of splitting primes of density $1/4+\varepsilon>1/4$, and this yields $K_\sigma = L_\sigma$ by Proposition 2.6. From $K_\sigma = L_\sigma$ and $K_2 = L_2$ we get the equality of composite fields $K_{\sigma^2} = L_{\sigma^2}$.

Now, we show that $\widehat{K}=\widehat{L}$: one has the equalities

$$\{\mathfrak{p}\colon f_K(\mathfrak{p})=(2,2)\}=\{\mathfrak{p}\colon f_L(\mathfrak{p})=(2,2)\},$$

$$\{\mathfrak{p}\colon f_{K_{\sigma^2}}(\mathfrak{p})=(1,1,1,1)\}=f_{L_{\sigma^2}}(\mathfrak{p})=(1,1,1,1)\}$$

and the intersection of these sets gives

$$\begin{aligned}&\{\mathfrak{p}\colon f_{K_{\sigma^2}}(\mathfrak{p})=(1,1,1,1), f_K(\mathfrak{p})=(2,2)\}\\ =\ &\{\mathfrak{p}\colon f_{L_{\sigma^2}}(\mathfrak{p})=(1,1,1,1), f_L(\mathfrak{p})=(2,2)\}.\end{aligned}$$

The sets above have prime density exactly equal to $1/8$, because they are the primes having $\{\sigma^2\}$ as Frobenius symbol. This means that the remaining splitting primes in K_{σ^2}, which have prime density equal to $1/4-1/8=1/8$, identify $\widehat{K}$; but being $K_{\sigma^2}=L_{\sigma^2}$, this means that $\widehat{K}$ and $\widehat{L}$ have the same splitting primes, i.e. $\widehat{K}=\widehat{L}$.

Finally, we show that $K\simeq L$: if they were not, it would be $L\simeq K'$; but then K and L could not be locally GCD equivalent, because a prime with Frobenius symbol $\langle\tau\rangle$ would have splitting type $(2,2)$ in one field but $(1,1,2)$ in the other.

6 Equivalence in degree 5

6.1 Galois groups for quintic fields

Let K be a field of degree 5 over F. The following are the possibilities for the Galois group G_K of its Galois closure $\widehat{K}$. We shall focus mainly on the set of inert primes and its density.

(i) $G_K = C_5$, the cyclic group of order 5. Then $\widehat{K}=K$ and

$$\begin{aligned}\delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(\mathfrak{p})=(1,1,1,1,1)\} &= 1/5,\\ \delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(\mathfrak{p})=(5)\} &= 4/5.\end{aligned}$$

(ii) $G_K = D_5 := \langle\sigma,\tau\,|\,\sigma^5=\tau^2=1,\tau\sigma\tau=\sigma^{-1}\rangle$. Then $\widehat{K}$ has degree 10 over F, contains 5 isomorphic quintic extensions over F and a unique quadratic extension

K_2/F. Moreover:

$$\begin{aligned} \delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(\mathfrak{p}) = (1,1,1,1,1)\} &= 1/10, \\ \delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(\mathfrak{p}) = (1,2,2)\} &= 1/2, \\ \delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(\mathfrak{p}) = (5)\} &= 2/5. \end{aligned}$$

(iii) $G_K = F_5 := \langle \sigma, \mu | \sigma^4 = \mu^5 = 1, \mu\sigma = \sigma\mu^2 \rangle$. Then $\widehat{K}$ has degree 20 over F, contains 5 isomorphic quintic extensions over F and a unique Galois, cyclic quartic extension K_4/F, and furthermore:

$$\begin{aligned} \delta_{\mathcal{P}}\{p\colon f_K(p) = (1,1,1,1,1)\} &= 1/20, \\ \delta_{\mathcal{P}}\{p\colon f_K(p) = (1,4)\} &= 3/4, \\ \delta_{\mathcal{P}}\{p\colon f_K(p) = (5)\} &= 1/5. \end{aligned}$$

(iv) $G_K = A_5$, the alternating group with 60 elements. Then $\widehat{K}$ has degree 60 over F and, most importantly, there are no non-trivial Galois F-extensions in it. The quintic fields in $\widehat{K}$ are all isomorphic, and by Corollary 2.1 every non-trivial subfield has the same splitting primes of K, implying that $\widehat{K}$ is uniquely determined by one of its non-trivial F-sub-extensions. Looking only at the inert primes, one gets:

$$\delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(\mathfrak{p}) = (5)\} = 2/5.$$

(v) $G_K = S_5$, the symmetric group with 120 elements. Then $\widehat{K}$ has degree 120 over F, its only Galois subfields over F being F/F and a quadratic extension K_2/F. Every other sub-extension over F is not Galois and shares with $\widehat{K}$ the set of splitting primes. The quintic subfields are isomorphic. The inert primes satisfy:

$$\delta_{\mathcal{P}}\{\mathfrak{p}\colon f_K(\mathfrak{p}) = (5)\} = 1/5.$$

6.2 Locally GCD equivalent quintic fields

Degree 5 extensions are the first ones which present cases of primitive, non Galois extensions. Whenever one of these extensions occur, we will use the Big Galois Closure approach instead of the Galois companions.

Let K and L be locally GCD equivalent fields of degree 5 over F. It is immediate from the density of the inert primes that, if one of them is Galois over F, then the two fields are actually isomorphic. Moreover, if $\widehat{K}$ has group $G_K = D_5$, then $\widehat{L}$ has group G_L equal to either D_5 or A_5; if $\widehat{K}$ has $G_K = F_5$, then $\widehat{L}$ has group G_L equal to either F_5 or S_5.

• $G_K = D_5$ and $G_L = D_5$: let K_2/F and L_2/F be the quadratic Galois companions of K and L respectively. Proposition 2.2 yields the following behaviour on inert primes:

$$\begin{array}{ccc} & (5\times 2)_{\widehat{K}} & \\ \swarrow\!\!\nearrow & & \searrow \\ (5)_K & & (1,1)_{K_2} \end{array}$$

Thus one has the identity

$$\begin{aligned} &\{\mathfrak{p}\colon f_{K_2}(\mathfrak{p}) = (1,1), f_K(\mathfrak{p}) = (5)\} \\ = \ &\{\mathfrak{p}\colon f_{L_2}(\mathfrak{p}) = (1,1), f_L(\mathfrak{p}) = (5)\}. \qquad (6.1) \end{aligned}$$

The above set has prime density equal to $2/5 > 1/4$, and this implies $K_2 = L_2$ by Proposition 2.6.

The remaining splitting primes in K_2 (which have density $1/2 - 2/5 = 1/10$) are precisely the splitting primes in $\widehat{K}$. Thus Equality (6.1) and $K_2 = L_2$ force $\widehat{K}$ and $\widehat{L}$ to have the same splitting primes, i.e. $\widehat{K} = \widehat{L}$. This yields $K \simeq L$.

• $G_K = F_5$ and $G_L = F_5$: this case is completely simlar to the previous one: just consider the quartic Galois companions K_4 and L_4 of K and L respectively. The inert primes of K become splitting primes of K_4: this forces $K_4 = L_4$ which in turn gives $\widehat{K} = \widehat{L}$, which in turn gives $K \simeq L$.

(**) $G_K = A_5$ and $G_L = A_5$: consider the Galois closures $\widehat{K}$ and $\widehat{L}$ and let us study their intersection.

If $\widehat{K} \cap \widehat{L}$ is different from F, then there is a common non-trivial subfield, which identifies the same splitting primes for both the fields, implying $\widehat{K} = \widehat{L}$ and $K \simeq L$.

So assume the intersection is equal to F: the composite Galois extension $\widehat{KL}$ has degree 3600 and Galois group $A_5 \times A_5$. A prime $\mathfrak{p}$ which is inert in both K and L has a Frobenius symbol formed by elements of order 5 in $A_5 \times A_5$. These elements have the form (g, h) with $g^5 = h^5 = 1_{A_5}$, with the only exception of $g = h = 1_{A_5}$.

But by local GCD equivalence, the set of such primes has prime density 2/5, while the density of the primes having elements of order 5 in $A_5 \times A_5$ as Frobenius symbols is $(25 \cdot 25 - 1)/3600 = 624/3600 < 1/4 < 2/5$, which is a contradiction.

(**) We are left with the cases $G_K = S_5$ and $G_L = S_5$, $G_K = D_5$ and $G_L = A_5$ and the case $G_K = F_5$ and $G_K = S_5$. These cases are solved by using the Big Galois Closure technique: one studies the intersection between $\widehat{K}$ and $\widehat{L}$ and must distinguish between two cases: if $\widehat{K} \cap \widehat{L}$ has degree greater or equal than 5, then the intersection is a field which uniquely detects both $\widehat{K}$ and $\widehat{L}$, forcing $\widehat{K} = \widehat{L}$ and thus the isomorphism between K and L. If $[\widehat{K} \cap \widehat{L} : F] \leq 2$ instead (no degree

3 or 4 intersection occurs) then one imitates the proof of the case $G_K = A_5, G_L = A_5$ in order to get a composite field $\widehat{KL}$ with a degree so large that the density of order 5 Frobenius elements in $G_K \times G_L$ results strictly less then the the product of the densities of inert primes in K and L, while the two things should be equal.

7 Final Remarks

7.1 Comparing equivalent fields of different degree

The proofs in the previous sections showed that any two number field extensions having same degree $n \leq 5$ which are locally GCD equivalent are in fact isomorphic. In order to complete the proof of Theorem 1.1.b, one needs to see what happens when equivalent fields of different degrees are compared.

The prime densities computations of the previous sections show that this possibility cannot happen for locally GCD equivalent fields of degree $n \leq 5$: among the field extensions with these degrees, cubic fields can be equivalent (and thus isomorphic) only to cubic fields, because the inert primes have greatest common divisor of their splitting type equal to 3, a number which is not obtained in any other low degree. For the same reason, quintic fields can be equivalent only to quintic fields.

We are left only with the comparison between quartic and quadratic extensions; but in any quadratic extension the inert primes have density 1/2, while in quartic fields such a density value is not attained by primes with splitting type $(2, 2)$.

7.2 A counterexample in degree 6

Theorem 1.1 proves that the local GCD equivalence reduces to isomorphism on equivalent fields of degree $n \leq 5$. It can be proven that there are counterexamples already in degree 6 : in fact, for every Galois cubic extension K/F, it is possible to present two non isomorphic quadratic extensions L/K and M/K such that L/F and M/F are F-locally GCD equivalent extensions of degree 6.

The construction relies on two concepts: first, local GCD equivalence can be proved to be equivalent to the fact that the norm groups of the fractional ideals are the same for the two extensions (see [4], Chapter VI, Section 1.b for the details). Then, using this different formulation, Stern [10] proved the existence of the sextic extensions L/F and M/F as above.

Moreover, being the much stronger relation given by arithmetic equivalence not reducible to the isomorphism for degrees $n \geq 7$, we can finally state that 5 is the maximum degree n for which the claim of Theorem 1.1 holds for every number field extension of degree n.

7.3 Inert primes are not enough in quartic fields

The previous sections showed explicitly the equivalence between the statements of Theorem 1.1 and Theorem 1.2: in particular, number fields extensions of prime degree $p \leq 5$ are uniquely characterized by their inert primes.

One could wonder if also quartic fields are uniquely determined by their inert primes, in the cases for which they actually exist. This request is weaker than local GCD equivalence, and, as we show below, it is not enough in order to have an isomorphism.

In fact, there are easy counterexamples: consider a quartic field K with Galois closure $\widehat{K}$ having Galois group D_4 and consider the non-conjugated non-Galois field K' contained in $\widehat{K}$ (refer to diagram 5.1 for notations). Then a prime $\mathfrak{p} \subset \mathcal{O}_F$ is inert in K if and only if its Frobenius symbol in D_4 is formed by elements of order 4: but the computations given by Proposition 2.2 show that the very same property holds also for K', and so we have two non-isomorphic quartic field extensions with same inert primes.

As an explicit example, consider $K := \mathbb{Q}[x]/(x^4 - 3x^2 - 3)$ and $K' := \mathbb{Q}[x]/(x^4 - 3x + 3)$: these quartic fields are not Galois over $\mathbb{Q}$ and share the same Galois closure over $\mathbb{Q}$, which is the octic field $\widehat{K} := \mathbb{Q}[x]/(x^8 + x^6 - 3x^4 + x^2 + 1)$ with Galois group D_4; so they share the inert primes, but in fact K and K' are not isomorphic.

7.4 Similar results in higher degree

Although 5 is the maximum degree for which Theorem 1.1.b holds, it is still possible to get a similar rigidity result for large families of field extensions in arbitrary prime degree by a simple adaptation of the Big Galois Closure technique used previously.

Let p be a prime number. Let K/F be a number field extension of degree p, and assume that its Galois closure has group equal to either A_p or S_p. Applying Proposition 2.2 it is easy to prove that this field has inert primes. If one mimics the procedure used to reduce the equivalence of quintic fields having group A_5 or S_5 to isomorphism, then it is possible to get the following theorem.

Theorem 7.1. *Let K and L be number fields of prime degree p over F which are F-locally GCD Equivalent and such that their Galois closures share the same Galois group G. Assume G equal either to A_p or S_p Then K and L are F-isomorphic.*

Theorem 7.1 is actually very strong, because a "random" number field extension of prime degree tends to have Galois group of its closure equal to the symmetric group S_p: from this one can conclude that, for these degrees, the local GCD equivalence reduces very often to isomorphism.

A stronger result, by Lochter again, proves Theorem 7.1 for every degree n and Galois groups S_n and A_n. At the moment, it seems not reachable without his original approach, or by means of the Big Galois Closure technique alone.

References

[1] G. J. Janusz. *Algebraic number fields*, volume 7 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, second edition, 1996.

[2] W. Jehne. Kronecker classes of algebraic number fields. *J. Number Theory*, 9(3):279–320, 1977.

[3] N. Klingen. Zahlkörper mit gleicher primzerlegung. *Journal für die reine und angewandte Mathematik*, 299:342–384, 1978.

[4] N. Klingen. *Arithmetical similarities*. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1998. Prime decomposition and finite group theory, Oxford Science Publications.

[5] J. Klüners and G. Malle. A database for number fields. Available at `http://galoisdb.math.upb.de/home`.

[6] S. Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[7] B. Linowitz, D. B. McReynolds, and N. Miller. Locally equivalent correspondences. *Ann. Inst. Fourier (Grenoble)*, 67(2):451–482, 2017.

[8] M. Lochter. Weakly Kronecker equivalent number fields. *Acta Arith.*, 67(4):295–312, 1994.

[9] R. Perlis. On the equation $\zeta_K(s) = \zeta_{K'}(s)$. *J. Number Theory*, 9(3):342–360, 1977.

[10] L. Stern. On the equality of norm groups of global fields. *J. Number Theory*, 36(1):108–126, 1990.

Francesco Battistoni
Dipartimento di Matematica
Università di Milano,
via Saldini 50, 20133 Milano, Italy.
E-mail address: `francesco.battistoni@unimi.it`