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, using an equivalent relation called Weak Kronecker Equivalence. Among the many results he got, Lochter discovered that number fields extensions of degree \( \leq 5 \) 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.

1. Introduction

1.1. Notation and Definitions. Given a number field \( F \), we will denote with \( \mathcal{P}(F) \) the set of non zero prime ideals of \( F \). The rational primes \( \mathcal{P}(\mathbb{Q}) \) will be denoted also with \( \mathcal{P} \).

Given a number field extension \( L/F \) and an unramified prime \( p \in \mathcal{P}(F) \), its splitting type is the \( t \)-ple \( f_{L}(p) := (f_{1,L}(p), \ldots, f_{t,L}(p)) \) given by the inertia degrees of the prime factors \( q_{1}, \ldots, q_{t} \) of \( \mathcal{O}_{L} \) lying over \( p \).

Given a set of primes \( A \subset \mathcal{P}(F) \), its prime density is the number (if it exists)

\[
\delta_{p}(A) := \lim_{x \to +\infty} \frac{\# \{ p \in A : \text{Nm}(p) \leq x \}}{\# \{ p \in \mathcal{P}(F) : \text{Nm}(p) \leq x \}} = \lim_{x \to +\infty} \frac{\# \{ p \in A : \text{Nm}(p) \leq x \}}{x \log x}.
\]

As usual, 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 \( p \in \mathcal{P}(F) \), the residue field of \( p \) is the finite field \( \mathbb{F}_{p} := \mathcal{O}_{F}/p \).

Given a finite Galois extension \( L/F \) with Galois group \( G \), an unramified prime \( p \in \mathcal{P}(F) \) and the prime factors \( q_{1}, \ldots, q_{t} \in \mathcal{P}(L) \) lying over \( p \), the decomposition group of \( q_{i} \) is the set \( G_{q_{i}} := \{ \sigma \in G : \sigma(q_{i}) = q_{i} \} \). The \( G_{q_{i}} \)'s are cyclic subgroups of \( G \) and are conjugated between them.

For every \( i = 1, \ldots, t \) there is a group isomorphism

\[
\Psi_{i} : G_{q_{i}} \to \text{Gal}(F_{q_{i}}/\mathbb{F}_{p}) = \langle \phi_{i} \rangle
\]

where \( \phi_{i} : F_{q_{i}} \to \mathbb{F}_{p} \) is the Frobenius automorphism of the finite field \( F_{q_{i}} \).

The Frobenius symbol of \( p \) is the conjugation class \( (L/F, p) := \{ \Psi_{i}^{-1}(\phi_{i}) : i = 1, \ldots, t \} \).

Remark 1. In a finite Galois extension \( L/F \), the splitting type of a prime \( p \in \mathcal{P}(F) \) has equal entries, and \( p \) has splitting type \( (f, \ldots, f) \) if and only if its Frobenius symbol is formed by elements of order \( f \) in the Galois group.

2010 Mathematics Subject Classification. 11R16, 11R44, 11R45.

Key words and phrases. Equivalence of number fields, density of primes.
Remark 2. From here until the end of the note, every prime ideal taken into account has to be considered unramified in the extensions we deal with.

1.2. Number fields characterized by sets of primes with given density. Given a number field $F$ and its ring of integers $\mathcal{O}_F$, it is a main topic in Algebraic Number Theory to study the factorization and the splitting type of a rational prime number $p$ in $\mathcal{O}_F$. Some classical questions dealing with this problem are the following: are number fields uniquely determined by the splitting types of rational primes? Is it true that if two number fields share a common set of primes with given splitting type, then the fields are isomorphic?

There are plenty of results concerning these questions, especially in the setting of arithmetic equivalence. Two number fields extensions $K/F$ and $L/F$ are said to be arithmetically equivalent over $F$ if for almost every prime ideal $p \in \mathcal{P}(F)$ the splitting types are the same (i.e. $f_{K}(p) = f_{L}(p)$ for a.e. $p$).

The following facts, proved by Perlis [6] and independent of the base number field $F$, give a strong characterization of arithmetically equivalent extensions:

- If two extensions $K/F$ and $L/F$ of degree $\leq 6$ are arithmetically equivalent, then the two fields are $F$-isomorphic.
- There exist arithmetically equivalent extensions $K/F$ and $L/F$ of degree 7 which are not $F$-isomorphic.
- If $K/F$ and $L/F$ are arithmetically equivalent extensions and one of them is Galois, then they are $F$-isomorphic.

This note focuses on a relation which is weaker than arithmetic equivalence: two number fields $K$ and $L$ are Locally GCD equivalent over a number field $F$ if for every prime $p \in \mathcal{P}(F)$ which is unramified in both $K$ and $L$ holds

$$\gcd(f_{1,K}(p), \ldots, f_{t,K}(p)) = \gcd(f_{1,L}(p), \ldots, f_{t,L}(p)).$$

This relation, which is weaker than arithmetic equivalence, forces the number fields involved to have some constraints on their splitting types, and one naturally asks whether the occurring of this equivalence implies the isomorphism or not.

This relation has been called Local GCD Equivalence by Linowitz, McReynolds and Miller [1]. Nonetheless, it was not a new concept: Lochter [5] already introduced this equivalence (although without giving it a name) and showed that is equivalent to a different relation, called Weak Kronecker Equivalence, which was his object of investigation. Lochter’s work [5] exploited an approach which consistently relied on Group Theory and representation Theory, and that allowed him to get the following rigidity result.

Theorem 1. Let $K/F$ and $L/F$ be locally GCD equivalent over $F$ and such that $[K : F], [L : F] \leq 5$. Then $K$ and $L$ are $F$-isomorphic.

Actually it is possible to translate this statement into a simpler one: in fact, Theorem 1 is equivalent to say that number fields extensions of degree 2, 3 and 5 are uniquely determined by their inert primes, while number fields extensions of degree 4 are uniquely determined by their inert primes plus the primes with splitting type $(2,2)$.

This alternative expression for Theorem 1 suggests that there could be a way to prove it which is different from Lochter’s proof: an idea could be to notice that, if $K$ and $L$ are locally GCD equivalent over $F$, then they have the same splitting types over “too many primes of a certain kind”. Thus one could wonder if it is possible to recover Theorem 1 by means of some results concerning the density of sets of prime numbers: this would be interesting because it would allow to explain an interesting result concerning rigidity properties of number fields by means of simpler tools.
In fact, the aim of this note is to show that it is indeed possible to prove Theorem 1 using only density theorems, like the famous Chebotarev’s Theorem, and basic Group and Galois Theory: in fact, basic characterizations of the subgroups of symmetric groups $S_n$ (with $n \leq 5$) and well known lemmas of Galois Theory are enough for our purpose.

Moreover, although there are many distinct cases to consider for the proof, they can be all solved using mainly two techniques. We specify which technique is used by means of the following notations:

- $\bullet$ : this symbol denotes the first approach, which consists in reducing the study of two equivalent extensions $K/F$ and $L/F$ at looking for an equivalence of some Galois companions of $K$ and $L$, i.e. some Galois extensions over $F$ which are naturally related to the original fields and have small degree (e.g. if $K/F$ has degree 3 and is not Galois, its Galois closure contains a unique quadratic extension $K_2/F$, which is the companion of $K$).

- $\star$ : this symbol denotes a different approach, which we call big Galois closure: instead of looking for some Galois extension of low degree, one considers a big Galois extension containing both the equivalent extensions $K/F$ and $L/F$, and proves the isomorphism working in this larger setting. We use this technique to deal with the cases where one of the extensions involved is primitive, i.e. has only $F$ and itself as $F$-sub-extensions.

Here is a brief sketch of the note.

In Section 2 we present the lemmas and tools which will be used throughout the note, and we recall how locally GCD equivalence for quadratic number fields provides the isomorphism.

In sections 3, 4 and 5 we study locally GCD equivalence between number fields of degree 3, 4 and 5 respectively: again, we will show that it is possible to recover the isomorphism using this simple density setting.

Finally, in Section 6 we give some remarks.

1.3. Acknowledgements. The author thanks Harry Smit from 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. Key Lemmas and first characterizations

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

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

**Corollary 1** (Frobenius). Let $L/F$ be a finite Galois extension of number fields. Then, the set of primes which split completely in $L$ has prime density equal to $1/[L:F]$.

**Proof.** Immediate consequence of Chebotarev’s theorem: a prime splits completely in a Galois extension of number fields if and only if its Frobenius symbol is the identity element of $G$. 

The following is a technical proposition, which is crucial in determining the splitting types of primes in generic number field extensions.
Proposition 1. Let $E/F$ be a finite Galois number field extension with Galois group $G$, and let $L/F$ be an intermediate extension. Let $H := \text{Gal}(E/L)$.

Let $X := \{ H, g_1H, \ldots, g_rH \}$ be the set of left cosets of $H$. Let $p \in \mathcal{P}(F)$ and let $g \in G$ be an element of the Frobenius symbol of $p$ in $G$. Consider the action of the group generated by $g$ on $X$ given by left multiplication.

Then there is a bijection

$$ \{ \text{orbits of the action} \} \leftrightarrow \{ \text{primes of } \mathcal{P}(L) \text{ dividing } p \}.$$ 

Moreover, if $(f_1, \ldots, f_t)$ is the $t$-ple representing the size of the orbits, then $f_L(p) = (f_1, \ldots, f_t)$.

Proof. See Chapter III, Prop. 2.8 of [2].

A prime with splitting type $(1, \ldots, 1)$ is said to split completely or, equivalently, to be a splitting prime.

Corollary 2. Let $K/F$ be a finite number field extension and let $\hat{K}/F$ be its Galois closure with group $G$. Then a prime $p \in \mathcal{P}(F)$ splits completely in $K$ if and only if it splits completely in $\hat{K}$.

Proof. While the complete splitting in $\hat{K}$ obviously forces the complete splitting in $F$, the converse implication is true because of Proposition 1 if there were other elements of $g$, different from $1_G$, which are Frobenius symbols for primes $p \in \mathcal{P}(F)$ with $f_K(p) = (1, \ldots, 1)$, it would be $g \cdot g_iH = g_iH$, which would force $H$ to be normal, i.e. $K = \hat{K}$ and $g = 1_G$.

Let us briefly recall a key lemma from Algebraic Number Theory.

Lemma 1. Let $K/F$ and $L/F$ be finite number field extensions and let $KL/F$ be its composite extension. Then $p \in \mathcal{P}(F)$ splits completely in $KL$ if and only if it splits completely in both $K$ and $L$.

Proof. One needs to prove the lemma only for Galois extensions, because Corollary 1 and the following diagram of sub-extensions permit to consider splitting primes in the intermediate fields as splitting primes in the Galois closures.

\begin{center}
\begin{tikzcd}
\hat{K} \arrow[r] \arrow[d] & KL \arrow[d] \arrow[r] & \hat{L} \\
K \arrow[r] \arrow[d] & F \arrow[r] & L \arrow[d] \\
F
\end{tikzcd}
\end{center}

Assume that $K/F$ and $L/F$ are both Galois: the claim then follows from Chapter III, Prop. 2.5, 2.6 of [2].

Corollary 3. 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.
ON LOCALLY GCD EQUIVALENT NUMBER FIELDS

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

$$\{p \in \mathcal{P}(F) : f_{KL}(p) = (1, \ldots, 1)\} = \{p \in \mathcal{P}(F) : f_K(p) = (1, \ldots, 1) \text{ and } f_L(p) = (1, \ldots, 1)\}.$$ 

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 $K = KL = L$. □

2.2. Equivalence in degree 2. We look now at the (easy) study of local GCD equivalence between quadratic fields, and we give also some density result concerning these fields.

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

Proposition 2. Let $K$ and $L$ be two quadratic fields over $F$.

1) If $K$ and $L$ are Locally GCD Equivalent over $F$, then they are $F$-isomorphic.
2) If $\{p \in \mathcal{P}(F) : f_K(p) = f_L(p) = (1, 1)\}$ has prime density strictly greater than $1/4$, then $K$ and $L$ are $F$-isomorphic.
3) The set $\{p \in \mathcal{P}(F) : f_K(p) = f_L(p)\}$ has prime density $\geq 1/2$. $K$ and $L$ are equal if and only if $> >$ holds.

Proof. 1) Quadratic extensions over $F$ are Galois extensions: if they are Locally GCD Equivalent, then they have the same set of splitting primes, and thus they are isomorphic by Corollary 3.

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

$$\{p \in \mathcal{P}(F) : f_{KL}(p) = (1, 1, 1, 1)\} = \{p \in \mathcal{P}(F) : f_K(p) = f_L(p) = (1, 1)\}.$$ 

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 $\{p \in \mathcal{P}(F) : f_K(p) = f_L(p)\}$ is identified with the set of splitting primes in $F[x]/(x^2 - \alpha \beta)$. The claim follows immediately. □

3. Equivalence in degree 3

3.1. Galois Groups for cubic fields. Let $K$ be a field of degree 3 over $F$, and let $\hat{K}$ be its Galois closure with Galois group $G$. The group $G$ can be one of the following:

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

$$\delta_P \{p : f_K(p) = (1, 1, 1)\} = 1/3,$$

$$\delta_P \{p : f_K(p) = (3)\} = 2/3.$$ 

$G = S_3$, the symmetric group with 6 elements. Then $\hat{K}$ has degree 6 over $F$, it contains three $F$-conjugated cubic fields 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 the densities in detail, it is:
\[
\delta_p \{ p : f_K(p) = (1,1,1) \} = \frac{1}{6},
\]
\[
\delta_p \{ p : f_K(p) = (1,2) \} = \frac{1}{2},
\]
\[
\delta_p \{ p : f_K(p) = (3) \} = \frac{1}{3}.
\]
All density computations are derived from Chebotarev’s Theorem and Proposition [1].

3.2. **Locally GCD equivalent cubic fields.** The equivalence problem in this degree can be solved by means of the sole Galois 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 if $K/F$ and $L/F$ are Galois cubic extensions and are locally GCD equivalent, they have the same splitting primes, and thus $K = L$.
- Let us assume that both $K$ and $L$ are not Galois. Consider their Galois closures $\hat{K}$ and $\hat{L}$, and the quadratic Galois companions $K_2$ and $L_2$.
Using Proposition [1] it is easy to show the following correspondence among the splitting types of the fields involved:

\[
\begin{align*}
(3,3)_{\hat{K}} & \quad \rightarrow \quad (3)_{K_2} \\
(3)_{K} & \quad \rightarrow \quad (1,1)_{K_2}
\end{align*}
\]

One gets the following identity:
\[
\{ p : f_{K_2}(p) = (1,1), f_K(p) = (3) \} = \{ p : f_{L_2}(p) = (1,1), f_L(p) = (3) \}.
\]
This implies that $\{ p : f_{K_2}(p) = (1,1), f_K(p) = (3) \}$ has prime density greater than $1/3$, and by Proposition [2] 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 ones that split completely in $\hat{K}$. But this fact, together with $K_2 = L_2$ and Equality [2], force $\hat{K}$ and $\hat{L}$ to have the same splitting primes, i.e. $\hat{K} = \hat{L}$, which in turn implies $K \simeq L$ (because the cubic extensions in $\hat{K}/F$ are $F$-conjugated between them).

4. **Equivalence in degree 4**

4.1. **Galois groups for quartic fields.** Let $K$ be a field of degree 4 over $F$, and let $\hat{K}$ be its Galois closure with Galois group $G$. The group $G$ can be one of the following:
$G = C_4$, the cyclic group of order 4. Then $K = \hat{K}$ is Galois over $F$ and the splitting types and densities are as follows:
\[
\delta_p \{ p : f_K(p) = (1,1,1,1) \} = \frac{1}{4},
\]
\[
\delta_p \{ p : f_K(p) = (2,2) \} = \frac{1}{4},
\]
\[
\delta_p \{ p : f_K(p) = (4) \} = \frac{1}{2}.
\]
\(G = C_2 \times C_2:\) then \(K = \hat{K}\) is Galois over \(F\) and
\[
\delta_{\mathfrak{p}}\{\mathfrak{p}: f_K(\mathfrak{p}) = (1, 1, 1, 1)\} = 1/4,
\]
\[
\delta_{\mathfrak{p}}\{\mathfrak{p}: f_K(\mathfrak{p}) = (2, 2)\} = 3/4.
\]
\(G = D_4 := \langle \sigma, \tau | \sigma^4 = \tau^2 = 1, \tau \sigma \tau = \sigma^3 \rangle.\) Then \(\hat{K}\) has degree 8 over \(F\), it contains 5 quartic fields and 3 quadratic fields, the lattice of sub-extensions being as follows:

\[
\begin{array}{c}
\hat{K} \\
\uparrow \\
K \\
\uparrow \\
K_\sigma \\
\uparrow \\
K_2 \\
\uparrow \\
F \\
\end{array}
\]

The quartic fields form 3 distinct classes of \(F\)-isomorphism: \(\{K, \hat{K}\}, \{K', \hat{K}'\}\) and \(\{K_\sigma^2\}\). The extension \(K_\sigma^2/F\) is Galois with Galois group \(C_2 \times C_2\).
Assuming that \(\text{Gal}(\hat{K}/K) = \langle \tau \rangle\), Proposition \(1\) yields
\[
\delta_{\mathfrak{p}}\{\mathfrak{p}: f_K(\mathfrak{p}) = (1, 1, 1, 1)\} = \delta_{\mathfrak{p}}\{\mathfrak{p}: (\hat{K}/F, \mathfrak{p}) = 1_{D_4}\} = 1/8,
\]
\[
\delta_{\mathfrak{p}}\{\mathfrak{p}: f_K(\mathfrak{p}) = (1, 1, 2)\} = \delta_{\mathfrak{p}}\{\mathfrak{p}: (\hat{K}/F, \mathfrak{p}) = \{\tau, \sigma^2\tau\}\} = 1/4,
\]
\[
\delta_{\mathfrak{p}}\{\mathfrak{p}: f_K(\mathfrak{p}) = (2, 2), (\hat{K}/F, \mathfrak{p}) = \sigma^2\} = 1/8,
\]
\[
\delta_{\mathfrak{p}}\{\mathfrak{p}: f_K(\mathfrak{p}) = (2, 2), (\hat{K}/F, \mathfrak{p}) = \{\sigma\tau, \tau\sigma\}\} = 1/4,
\]
\[
\delta_{\mathfrak{p}}\{\mathfrak{p}: f_K(\mathfrak{p}) = (4)\} = \delta_{\mathfrak{p}}\{\mathfrak{p}: (\hat{K}/F, \mathfrak{p}) = \{\sigma, \sigma^3\}\} = 1/4.
\]
If \(\text{Gal}(\hat{K}/K) = \langle \sigma \tau \rangle\), simply reverse the roles of \(\tau\) and \(\sigma \tau\) in the description above.

\(G = A_4,\) the alternating group with 12 elements. Then \(\hat{K}\) has degree 12 over \(F\), it contains 4 quartic fields (each one \(F\)-conjugated 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:
\[
\delta_{\mathfrak{p}}\{\mathfrak{p}: f_K(\mathfrak{p}) = (1, 1, 1, 1)\} = 1/12,
\]
\[
\delta_{\mathfrak{p}}\{\mathfrak{p}: f_K(\mathfrak{p}) = (1, 3)\} = 2/3,
\]
\[
\delta_{\mathfrak{p}}\{\mathfrak{p}: f_K(\mathfrak{p}) = (2, 2)\} = 1/4.
\]

\(G = S_4:\) then \(\hat{K}\) 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 \(\hat{K}\) are \(F\)-conjugated. The splitting types and decomposition are as follows:
\[
\begin{align*}
\delta_P\{p : f_K(p) = (1,1,1,1)\} &= 1/24, \\
\delta_P\{p : f_K(p) = (1,1,2)\} &= 1/4, \\
\delta_P\{p : f_K(p) = (1,3)\} &= 1/3, \\
\delta_P\{p : f_K(p) = (2,2)\} &= 1/8, \\
\delta_P\{p : f_K(p) = (4)\} &= 1/4.
\end{align*}
\]

All densities are computed with Chebotarev’s Theorem and Proposition \[\text{Proposition 1}\].

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.

### 4.2. 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 isomorphism.

- **\(G = D_4\):** Let us take \(K/F\) and \(L/F\) locally GCD equivalent quartic extensions with Galois closures \(\hat{K}\) and \(\hat{L}\) and Galois group \(D_4\). We follow the notations of diagram \[\text{Diagram 3}\] for the sub-extensions of \(\hat{K}\) and \(\hat{L}\).

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

\[
\begin{align*}
\{p : f_{K_2}(p) = (2), f_K(p) = (4)\} &= \{p : f_{L_2}(p) = (2), f_L(p) = (4)\}, \\
\{p : f_{K_2}(p) = (1,1), f_K(p) \in \{(1,1,1,1),(1,1,2)\}\} &= \\
\{p : f_{L_2}(p) = (1,1), f_L(p) \in \{(1,1,1,1),(1,1,2)\}\}.
\end{align*}
\]

The sets in Equality \[\text{Equality 4}\] have prime density equal to 1/4, while the ones in Equality \[\text{Equality 5}\] have positive density equal to 3/8. This tells us 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 \[\text{Proposition 2}\].

Let us consider now the field \(K_\sigma\). Using Proposition \[\text{Proposition 1}\] it is possible to show the following behaviour:

\[
\begin{array}{c}
(4,4)_{\hat{K}} \\
(4)_{\hat{K}} \\
(1,1)_{K_\sigma}
\end{array}
\]

Thus one obtains the equality

\[
\{p : f_{K_\sigma}(p) = (1,1), f_K(p) = (4)\} = \{p : f_{L_\sigma}(p) = (1,1), f_L(p) = (4)\}
\]

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

Furthermore, the set of primes \(\{p : f_K(p) = f_L(p) = (1,1,1,1)\}\) 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 \( \hat{K} \) and \( \hat{L} \), it is clear that for any of these primes holds \( f_{K, \sigma}(p) = f_{L, \sigma} (p) = (1, 1) \). This result, together with Equality \( (6) \), yields \( K_{\sigma} = L_{\sigma} \), and together with \( K_2 = L_2 \) provides \( K_{\sigma^2} = L_{\sigma^2} \).

Now, we show that \( K = L \): one has the equalities

\[ \{ p : f_K(p) = (2, 2) \} = \{ p : f_L(p) = (2, 2) \} \]

and the intersection of these sets gives

\[ \{ p : f_{K, \sigma^2}(p) = (1, 1, 1, 1), f_K(p) = (2, 2) \} = \{ p : f_{L, \sigma^2}(p) = (1, 1, 1, 1), f_L(p) = (2, 2) \} \]

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

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 Chebotarev symbol \( \tau \) would have splitting type \((2, 2)\) in one field but \((1, 1, 2)\) in the other.

- **\( G = A_4 \)**: Consider the cubic Galois companions \( K_3/F \) and \( L_3/F \) associated to \( K \) and \( L \) respectively. Proposition \( \text{[11]} \) yields the following behaviour on the splitting types:

\[
\begin{align*}
(2 \times 6)_{\hat{K}} & \quad \searrow \quad (1, 1, 1)_{K_3} \\
(2, 2)_K & \quad \swarrow \quad (1, 1, 1)_{K_3}
\end{align*}
\]

Thus one gets the identity

\[ \{ p : f_{K_3}(p) = (1, 1, 1), f_K(p) = (2, 2) \} = \{ p : f_{L_3}(p) = (1, 1, 1), f_L(p) = (2, 2) \} \]  

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

\[ \{ p : f_{K_3L_3}(p) = (1 \times 9) \} = \{ p : f_{K_3}(p) = f_{L_3}(p) = (1, 1, 1) \} \]

the left hand side would have prime density equal to 1/9, which is in contradiction with Equality \( (7) \).

The remaining splitting primes in \( K_3 \) have density \( 1/3 - 1/4 = 1/12 \) and are precisely the primes which split completely in the Galois closure \( \hat{K} \). Thus, equality \( (7) \) and \( K_3 = L_3 \) force \( \hat{K} \) and \( \hat{L} \) to have the same splitting primes, i.e. \( \hat{K} = \hat{L} \), which implies \( K \simeq L \).

- **\( G = S_4 \)**: Let \( K_6/F \) be the Galois companion of degree 6 associated to \( K \). Proposition \( \text{[11]} \) together with the correspondence between \( K \) and any subgroup of order 6 of \( S_4 \) and the one between \( K_6 \) and the normal subgroup of order 4 of \( S_4 \), gives the following relations between the splitting types:
This immediately shows that, if $K/F$ and $L/F$ have Galois closure with group $S_4$ and are locally GCD equivalent, there is the equality

$$\{p: f_{K_6}(p) = (1 \times 6), f_K(p) = (2, 2)\} = \{p: f_{L_6}(p) = (1 \times 6), f_L(p) = (2, 2)\}$$

and the prime density of these sets (which is equal to the one of primes with splitting type $(2, 2)$ in $K$) is equal to $1/8$.

Assuming $K_6 \neq L_6$, it would be that the Galois composite $K_6L_6$ would have degree $n \geq 12$. But then the equality

$$\{p: f_{K_6L_6}(p) = (1 \times n)\} = \{p: f_{L_6}(p) = (1 \times 6) = f_{L_6}(p)\}$$

would be a contradiction with respect to the previous computation, because the sets of Equality (8) would be contained in a set of prime density $1/n \leq 1/12$.

Being $K_6 = L_6$, let us look now the Galois closures $\hat{K}$ and $\hat{L}$. From the locally GCD equivalence between $K$ and $L$, one already has

$$\{p: f_{\hat{K}}(p) = (4 \times 6)\} = \{p: f_{\hat{L}}(p) = (4 \times 6)\},$$

$$\{p: f_{\hat{K}}(p) = (2 \times 12), f_K(p) = (2, 2)\} = \{p: f_{\hat{L}}(p) = (2 \times 12), f_L(p) = (2, 2)\}.$$  

Moreover, the equality $K_6 = L_6$ yields

$$\{p: f_{\hat{K}}(p) = (3 \times 8)\} = \{p: f_{\hat{L}}(p) = (3 \times 8)\}$$

and the primes with splitting type $(2, 2, 2)$ in $K_6$ which do not come from inert ideals of $K$ have necessarily splitting type $(2 \times 12)$ in $\hat{K}$: this allows us to conclude that

$$\{p: f_{\hat{K}}(p) = (2 \times 12)\} = \{p: f_{\hat{L}}(p) = (2 \times 12)\},$$

which in turn yields that $K$ and $L$ share the same splitting primes, i.e. $\hat{K} = \hat{L}$, and from this it follows $K \simeq L$. 

---

(8)
5. Equivalence in degree 5

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

$G = C_5$, the cyclic group of order 5. Then $\hat{K} = K$ and

$$\delta_P \{ p : f_K(p) = (1,1,1,1,1) \} = \frac{1}{5},$$

$$\delta_P \{ p : f_K(p) = (5) \} = \frac{4}{5}.$$

$G = D_5 := \langle \sigma, \tau | \sigma^5 = \tau^2 = 1, \tau \sigma \tau = \sigma^{-1} \rangle$. Then $\hat{K}$ has degree 10 over $F$, contains 5 $F$-conjugated quintic fields and a unique quadratic extension $K_2/F$. Moreover:

$$\delta_P \{ p : f_K(p) = (1,1,1,1,1) \} = \frac{1}{10},$$

$$\delta_P \{ p : f_K(p) = (1,2,2) \} = \frac{1}{2},$$

$$\delta_P \{ p : f_K(p) = (5) \} = \frac{2}{5}.$$

$G = F_5 := \langle \sigma, \mu | \sigma^4 = \mu^5 = 1, \mu \sigma = \sigma \mu^2 \rangle$. Then $\hat{K}$ has degree 20 over $F$, contains 5 $F$-conjugated quintic fields and a unique Galois, cyclic quartic extension $K_4/F$, and furthermore:

$$\delta_P \{ p : f_K(p) = (1,1,1,1,1) \} = \frac{1}{20},$$

$$\delta_P \{ p : f_K(p) = (1,4) \} = \frac{3}{4},$$

$$\delta_P \{ p : f_K(p) = (5) \} = \frac{1}{5}.$$

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

$$\delta_P \{ p : f_K(p) = (5) \} = \frac{2}{5}.$$

$G = S_5$, the symmetric group with 120 elements. Then $\hat{K}$ has degree 120 over $F$, its only Galois $F$-subfields being $F/F$ and a quadratic extension $K_2/F$. Every other $F$-sub-extension is non-Galois and shares with $\hat{K}$ the set of splitting primes. The inert primes satisfy:

$$\delta_P \{ p : f_K(p) = (5) \} = \frac{1}{5}.$$

5.2. Locally GCD equivalent quintic fields. Degree 5 extensions are the first one 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 $\hat{K}$ has group $G_K = D_5$, then $\hat{L}$ has group $G_L$ equal to either $D_5$ or $A_5$; if $\hat{K}$ has $G_K = F_5$, then $\hat{L}$ 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 1 yield the following behaviour on inert primes:

\[
\begin{array}{c}
(5 \times 2)_{\hat{K}} \\
(5)_K \\
(1, 1)_{K_2}
\end{array}
\]

Thus one has the identity

\[
\{p: f_{K_2}(p) = (1, 1), f_K(p) = (5)\} = \{p: f_{L_2}(p) = (1, 1), f_L(p) = (5)\}.
\]

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

The remaining splitting primes in $K_2$ (which have density $1/2 - 2/5 = 1/10$) are precisely the primes which split completely in $\hat{K}$. Thus Equality (9) and $K_2 = L_2$ force $\hat{K}$ and $\hat{L}$ to have the same splitting primes, i.e. $\hat{K} = \hat{L}$. This yields $K \simeq L$.

- $G_K = F_5$ and $G_L = F_5$: Let $K_4$ and $L_4$ be the quartic Galois companions of $K$ and $L$ respectively. There is the following correspondence on splitting types:

\[
\begin{array}{c}
(5 \times 4)_{\hat{K}} \\
(5)_K \\
(1, 1, 1, 1)_{K_4}
\end{array}
\]

which yields the identity

\[
\{p: f_{K_4}(p) = (1, 1, 1, 1), f_K(p) = (5)\} = \{p: f_{L_4}(p) = (1, 1, 1, 1), f_L(p) = (5)\}.
\]

The above sets have prime density equal to $1/5$. If $K_4$ and $L_4$ were not equal, their Galois composite $K_4L_4$ would be a field of degree $n \geq 8$ over $F$; but then one would have the identity

\[
\{p: f_{K_4L_4}(p) = (1 \times n)\} = \{p: f_{K_4}(p) = f_{L_4}(p) = (1, 1, 1, 1)\},
\]

and the left hand side would have prime density $1/n \leq 1/8$, which is in contradiction with our assumption. Thus $K_4 = L_4$.

The remaining splitting primes (which have density $1/4 - 1/5 = 1/20$) are precisely the primes which split completely in $\hat{K}$: then Equality (10) and $K_4 = L_4$ force $\hat{K}$ and $\hat{L}$ to have the same splitting primes, i.e. $\hat{K} = \hat{L}$.

This immediately implies $K \simeq L$.

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

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

So assume the intersection is equal to $F$: the composite Galois extension $\hat{K}\hat{L}$ has degree...
3600 and Galois group $A_5 \times A_5$. A prime $p$ 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.

** $G_K = D_5$ and $G_L = A_5$:** Just like in the previous case, consider the intersection between the Galois closures $\hat{K}$ (with group $D_5$) and $\hat{L}$ (with group $A_5$). The intersection can be either a quintic field or $F$.

In the first case a field isomorphic to $K$ would be contained in $\hat{L}$, which would yield $K \cong L$.

Otherwise, if the intersection is trivial, consider the composite Galois field $\hat{K}\hat{L}$. It has degree $10 \cdot 60 = 600$ and has group $D_5 \times A_5$.

A prime which is inert in both $K$ and $L$ has an element of order 5 in the new group as Frobenius symbol. But such inert primes form a set of prime density equal to $2/5$, while the density of the primes having these symbols is $(5 \cdot 25 - 1)/600 = 124/600 < 1/10$, and this is a contradiction.

** $G_K = F_5$ and $G_L = S_5$:** Let us consider the closures $\hat{K}$ (with group $F_5$) and $\hat{L}$ (with group $S_5$).

Because of the group structure of $S_5$, which does not admit subgroups of index 4, there are only two possibilities for $\hat{K} \cap \hat{L}$: it is either a quintic field or $F$. In the first case the two Galois fields share a common quintic field, which implies $K \cong L$.

Assume instead that the intersection is equal to $F$: then the composite Galois extension $\hat{K}\hat{L}$ has degree $20 \cdot 120 = 2400$ and Galois group $F_5 \times S_5$. A prime $p$ which is inert in both $K$ and $L$ has a conjugacy class of elements of order 5 as Frobenius symbol in $F_5 \times S_5$. But this kind of primes forms a set with prime density $1/5$, while the density of order 5 Frobenius symbols in $F_5 \times S_5$ is equal to $(5 \cdot 25 - 1)/2400 = 124/2400 < 1/10$, and this is a contradiction.

** $G_K = S_5$ and $G_L = S_5$:** the Galois closure $\hat{K}$ is uniquely determined by any subfield which is neither $F$ or the quadratic extension $K_2/F$.

Let us consider $\hat{K} \cap \hat{L}$: whenever this intersection is a field of degree $> 2$, then the two fields share a common subfield which uniquely determines them, and this yields $\hat{K} = \hat{L}$, i.e. $K \cong L$.

If $\hat{K} \cap \hat{L} = F$, the composite extension $\hat{K}\hat{L}$ has degree $120 \cdot 120 = 14400$ and Galois group $S_5 \times S_5$. A prime $p$ which is inert in both $K$ and $L$ necessarily as an element of order 5 as Frobenius symbol.

But again, the set of common inert primes of $K$ and $L$ has prime density equal to $1/5$, while the Frobenius symbols of order 5 have density $(25 \cdot 25 - 1)/14400 = 624/14400 < 1440/14400 = 1/10$.

If instead $\hat{K} \cap \hat{L} = K_2$, the composite extension $\hat{K}\hat{L}$ has degree 7200 and its Galois group is a quotient of $S_5 \times S_5$ with a normal subgroup of order 2. This quotient preserves the elements of order 5.

Thus, following the sketch of the previous case, one obtains a contradiction, because the density of the primes which are inert in both $K$ and $L$ is $1/5$, while the Frobenius symbols of order 5 in this new Galois group have density $(25 \cdot 25 - 1)/7200 = 624/7200 < 720/7200 = 1/10$. 


6. Final Remarks

We have shown that locally GCD equivalent extensions with same degree $\leq 5$ are isomorphic. In order to complete the proof of Theorem 1, one needs to show that locally GCD equivalent number fields of degree $\leq 5$ have actually the same degree over $F$.

This is immediate from the computations of densities and splitting types done in the previous sections: number fields of degree 3 and 5 always have inert primes, so they must be locally GCD equivalent to number fields of the same degree. Number fields of degree 2 have half of the primes which have splitting type $(2)$, while in number fields of degree 4 the primes with splitting type $(2, 2)$ form a set with density always different from $1/2$.

It is known, thanks to Lochter [5], that 5 is the highest degree for which the local GCD equivalence implies the isomorphism: in fact, for any base number field $F$ there exist two field extensions of degree 6 over $F$ which are locally GCD equivalent but not $F$-isomorphic. For more details, see Chapter VI of [3].

One could wonder why the maximum degree for arithmetic equivalence that always provide an isomorphism is 6, while for local GCD equivalence is 5. These bounds become clearer if one deals with these relations in the original group theoretic setting (see Theorem 2 of [6] and the aforementioned Chapter VI of [3]). Surely, one could expect that this upper bound was lower for local GCD equivalence, being a weaker relation than arithmetic equivalence.

As mentioned in the introduction, Theorem 1 can be stated, for number fields extensions of prime degree $\leq 5$, saying that these fields are uniquely determined by their inert primes, which appears to be a not so obvious rigidity characterization.

It is quite curious that, searching through the literature and Internet, there are no direct references to the fact that inert primes are enough for uniquely determining number fields extensions of degree 3 and 5, and the only proof of this fact was hidden among the papers related to Weak Kronecker Equivalence.

One could ask if also quartic fields are uniquely determined by their inert primes (if they exist). This request is in fact much weaker than local GCD equivalence, and, as one expects, it is not enough in order to have an isomorphism. In fact, there are easy counterexamples: take a quartic field $K$ with Galois closure $\hat{K}$ having group $D_4$ and consider the non-conjugated non-Galois field $K'$ contained in $\hat{K}$ (refer to diagram 3 for notations, with $F = \mathbb{Q}$.) Then, looking at the computations provided by the Proposition 1, if a prime $p$ has some elements of order 4 in $D_4$ as Frobenius symbols, then $p$ is inert in both $K$ and $K'$.

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 1 it is easy to prove that this field has inert primes.

If one mimics the Big Galois Closure technique used for the equivalence of quintic fields having group $A_5$ or $S_5$, then it is possible to get the following, more general, proposition:

**Proposition 3.** Let $K$ and $L$ be number fields of prime degree $p$ over $F$ which are locally GCD Equivalent over $F$ and have same Galois Group $G$ of the closure. Assume $G$ is equal either to $A_p$ or $S_p$ Then $K$ and $L$ are $F$-isomorphic.
REFERENCES

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

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

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

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

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

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

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