

## Galois Extensions with Predefined Disintegrating Groups

Sheetal Kumari, Research Scholar, Department of Mathematics, OPJS University, Churu, Rajasthan.  
 Dr. Ashwini Kumar Nagpal, Associate Professor, Department of Mathematics, OPJS University, Churu, Rajasthan.

### ABSTRACT

Worked on a solution to the inverse Galois issue in the context of a specific location all of  $\mathbb{Q}$  disintegration groups are cyclic if every finite group is a Galois extension of  $\mathbb{Q}$ , and this is what we're looking for (resp., abelian). All solvable groups have this property, thanks to Shafarevich's solution to the inverse Galois problem for particular sets. Though, nonsolvable groupings are unrestrained. As a result, we provide the first endless descendants of Galois realisations utilising solely recurring disintegrated groups and the nonsolvable Galois group to overcome these issues.... As an added bonus, we investigate universal functional areas.

**Keywords:** *Inverse Galois theory; Locally cyclic extensions; Local and global fields; Unramified extensions; Galois covers; Specialization*

### Introduction

Each predetermined group  $G$  appears as a Galois group over  $K$  in inverse Galois problem (a number field  $K$ ). A heuristic approach has been offered that suggests the answer should be "yes, and for systematic reasons" rather than "yes, but out of reach at this point" for the problem. Restrictive Galois additions are defined at a specified set of  $K$ 's key ideals  $S$  and then asked if there are any Galois extensions of  $K$  with group  $G$  (short for Galois extensions)  $F/K$  that meet these local requirements. These systematic arguments arise from this process. For instance, the Grunwald issue is a well-known example of a "Inverse Galois problem with local constraints," and it corresponds perfectly to the scenario in where  $S$  is a fixed finite collection of prime numbers. In this case,  $S$  is exactly the set of  $F/K$  ramified  $K$ 's primes. [1] This leads to inverse Galois issues with specific inertia and/or disintegration groups. The following question attempts to express this issue in everyday language: **Question 1** "A finite group,  $K$  is a number field and an assortment of cyclic subgroups of  $G$  are given, such that  $G$  equals the normal closure for  $I_1, \dots, I_r$ . In other words, let  $D_i$  be a subgroup of  $G$  such

that  $I_i \leq D_i$ , and  $D_i/I_i$  is cyclic for all integers  $i=1, \dots, r$ . What  $G$ -extensions  $L/K$  exist that have the

inertia/decomposition group pair at  $p$  conjugate to  $(I_i, D_i)$  for  $i \in \{1, \dots, r\}$  for each prime  $p$  of  $K$  ramified in  $L$ ?

**Question 1** is examined in **Questions 2** and **3** below. The purpose of this article is to look into a few particularly intriguing cases." [2]

**Definition 1.1** "The number  $K$  should be treated as a field of numbers. As long as there are cyclic completions of the Galois extension  $L \cdot K_p/K_p$ , it is said to be locally cyclic."

"Definition 1.1 is about the disintegration groups at ramified primes of  $L/K$  because unramified extensions of  $K_p$  are naturally cyclic, hence as a specific instance of Question 1, we are led to the following:"

**Question 2** "Let  $G$  be a finite group and  $K$  a number field. Are there infinitely many, pairwise linearly disjoint, locally cyclic Galois extensions of  $K$  with Galois group  $G$ ?"

**Question 2** requires linear disjointness, which we provide to avoid making the solution too easy for some subsets of students. Because it's feasible to build an endless number of  $G \times C_2$ -extensions of  $K$  that are each locally cyclic and contain the sub extension  $L/K$  by altering the quadratic extension, those extensions aren't considered basically novel. [3] In comparison to the locally cyclic property, the following feature is less strong, but more adaptable."

**Definition 1.2** "The number  $K$  should be treated as a field of numbers. It is local abelian to call a Galois extension for  $L/K$ , if all completions  $L \cdot K_p/K_p$  are abelian for prime  $p$  of  $K$

Consider the case of locally abelian extensions, in which the compositum is again locally abelian. Because of this,  $K^{\text{loc-ab}}$  of  $K$  maximal locally abelian extension (for locally cyclic, this does not hold)."

**Question 3** "We'll use  $G$  as a finite group and  $K$  as a number field for this discussion. How many locally abelian Galois extensions to  $K$  with Galois group  $G$  are there in the infinite pairwise linearly disjoint space? In specifically, does  $G$  have the same sign as  $G_{\text{al}}(K^{\text{loc-ab}}/K)$ ?"

a yes to Question 2 is known for all finitely solvable groups because of the nature of Shafarevich's solution of the inverse Galois problem for those groups. We are not aware of any nonsolvable group where Question 2 has previously been addressed. a no to question 3 is known."

### 1.1. Locally cyclic and abelian Galois application.

As one-of-a-kind examples of an inverse Galois problem with specified local behaviour, issues relating to the existence of locally cyclic or locally abelian Galois extensions with prescribed Galois groups are important. They can be used in other areas of number theory. Some of our favourite are listed here.[5]

#### 1.1.1. Embedding problems

"Locally cyclic extensions" can be a lifesaver if you're experiencing difficulties with central embedding. [6] Even stronger notion of a Scholz extension is required to guarantee the solvability of such embedding difficulties, which isn't expressed in this assertion. These extensions will be used as an entrance point into embedding challenges for specific non-split central extensions of the Galois group  $S_5$  [7]

#### 1.1.2. Extensions with no logic over a limited number of fields

Even though it may appear complex at first, when no restrictions are imposed, creating unramified  $K/k$  extensions of number fields using supplied  $K/k$  Galois groups is actually quite simple. However, if we need that the degree of  $k$  be "small," the problem becomes difficult for "big" given the Galois group  $\text{Gal}(K/k)$ . When " $G$  is the Galois group" of a simple local "abelian extension  $F/\mathbb{Q}$ ", you'll obtain a modest base field as an added bonus. Unramified  $G$ -extensions are said to exist in folklore even in correct quadratic number fields, but this has never been confirmed [9].

#### 1.1.3. Weak calculation

"Let  $V$  represent a selection over the range of values in the number field  $K$ . It's worth recalling that  $V$  is said to satisfy weak approximation if the set  $V(K)$  of  $K$ -rational points is dense within the set

$\prod_{p \in S} V(K_p)$ , where  $K_p$  is completed at  $p$  for any finite set  $S$  of  $K$  primes. Known naturally occurring locally cyclic extensions relate to weak approximation concerns on specific varieties. If  $K/k$  is an abelian extension of number fields, the reverse inference applies as well for  $\mathbf{R}^1_{K/k}(G_m)$  if it is a locally cyclic Galois extension of number fields. This is demonstrated in [7], where it is shown that for abelian extensions of number fields, the converse implication holds." [10]

#### 1.1.4. Polynomials with spectral approximation

"There is another specific use for locally cyclic extensions in the study of so-called Polynomials with spectral approximation, which are polynomials  $f \in \mathbf{O}_K[X]$  (necessarily reducible!) with Galois group  $G$  that have a root in every completion of  $K$  but not in  $K$ . This is a difficult problem. With the exception of cyclic groups of prime power order, where a trivial group-theoretical barrier exists, it is easy to see that intersective polynomials exist for all groups that arise as Galois groups. Group theory does have an upper limit on the number of such irreducible polynomials, though, specifically the least number

such that proper subgroups  $U_1, \dots, U_m$  of  $G$  with  $\bigcap_{\infty \in G, 1 \leq i \leq m} U_i^\infty = \{1\}$ . In general, obtaining this lower bound is an open question. This approach has been used successfully to obtain optimally intersective realizations for several classes of groups. For example, see [12] for solvable groups for some constructions of families of minimally intersecting polynomials with non-solvable Galois groups despite the fact that our work does not produce any new  $\bigcap_{\infty \in G, 1 \leq i \leq m} U_i^\infty = G$ h optimally intersecting realizations, our criteria could be applied in the future to create such families."

## 2. Configuration and results

The treatment discussed here is broken down into four phases. There are a number of requirements for function fields and their specialisation in Section 3, such as Beckman-result n's on the ramification of specialisation, Ziegler's on the simultaneous prime values of certain polynomials, and embedded difficulties. These will be examined in Section 3.  $\mathbb{Q}$  extensions

that are locally abelian will be discussed in Section 4. We suggest a generic approach to the problem based on the specialisation of function field extensions. A number of novel locally abelian extensions will then be created, including nonsolvable Galois groups.

**Theorem 2.1** "There exist infinitely many primes  $p$  such that for each  $k \in \mathbb{N}$ , the group

$\text{PGL}_2(p)^k$  possesses locally abelian realizations over  $\mathbb{Q}$ "

"In particular, theorem 2.1, we obtain many small cyclic number fields with unramified  $\text{PGL}_2(p)$ -extensions it deals with the case of locally cyclic extensions of  $\mathbb{Q}$ . Here our main goal is to provide the first examples of non-solvable finite groups with a positive answer to Question 2.

Theorem 2.1, which deals with locally cyclic extensions of  $\mathbb{Q}$ , yields a large number of small cyclic number fields with unramified  $\text{PGL}_2(p)$ -extensions. Our major objective is to answer Question 2 with the first examples of non-solvable finite groups."

**Theorem 2.2** "For any  $n \leq 10$  and  $k \in \mathbb{N}$ , there exist infinitely many linearly disjoint locally cyclic extensions of  $\mathbb{Q}$  with Galois group  $S^k$ ."

"The objective is to show that, local cyclic realisations and embedding difficulties are compatible. Further nontrivial examples of locally cyclic realisations with a nonsolvable Galois group are given in Theorem 5.6, where they are identical to a central extension of  $S_5$  or  $\text{PGL}_2$ . Finally, we present an analogue over global function fields to support a general positive answer to Question 2 (and a fortiori to the weaker Question 3)."

### 3. Conditions

3.1. Function field extensions "Let  $K$  be a field. A finite Galois extension  $F/K(t)$  is called  $K$ -regular (or simply regular, if the base field is clear), if  $F \cap \overline{K} = K$ . For any and any place  $p$  of  $F$  extending the  $K$ -rational place  $t \rightarrow t_0$ , we have a residue field extension  $F_{t_0}/K$ . This is a Galois extension, not depending on the choice of place  $p$ . We call it the specialization of  $F/K(t)$  at  $t_0$ . Now let  $K$  be of characteristic zero, and let  $F/K(t)$  be a  $K$ -regular extension. Let  $t_i \in K \cup \{\infty\}$  be a branch point of  $F/K(t)$ . The ramification index of  $F/K(t)$  at  $t_i$  is the minimal positive integer  $e_i$  such that  $F$  embeds into  $\overline{K}(((t - t_i)^{1/e_i}))$ . If the ramification index is larger than 1, then  $t_0$  is called a branch point of  $F/K(t)$ . The set of branch points is always a finite set. If  $K$  is of characteristic 0, then associated to each branch point  $t_i$  (of ramification index  $e_i$ ) is a unique conjugacy class  $C_i$  of  $G$ , corresponding to the automorphism where  $\zeta_i$  is a primitive  $e_i$ -th root of unity. The ramification index then equals the order of elements in the class  $C_i$ ."

3.2 Specialty groups for inertia and decomposition Based on previously published findings, we investigate the behaviour of inertia and decomposition groups in functional field specialisations. As a result, we can draw the following conclusion: Function field extensions have inertia groups associated to their branch points, according to Theorem 2.

**Theorem 3.1** "Let  $K$  be a number field and  $N/K(t)$  a  $K$ -regular Galois extension with Galois group  $G$ . Then with the exception of finitely many primes, depending only on  $N/K(t)$ , the following holds for every prime  $p$  of  $K$ .

If  $t_0 \in K$  is not a branch point of  $N/K(t)$ , then the following condition is necessary for  $p$  to be ramified in the specialization  $N_{t_0}/K$ :"

"Here  $I_p(t_0, t_i)$  is the intersection multiplicity of  $t_0$  and  $t_i$  at the prime  $p$ . Furthermore,  $v_i > 0$  implies that the inertia group of a prime extending  $p$  in  $N_{t_0}/K$  is conjugate in  $G$  to  $\langle \tau^{v_i} \rangle$  where  $\tau$  is a generator of an inertia subgroup over the branch point  $t \rightarrow t_i$  of  $N/K(t)$ "

"Regarding the definition of intersection multiplicity  $I_p$  occurring in Theorem 3.1, note that in the special case  $K = \mathbb{Q}$  this may be defined conveniently in the following way: Let  $f(X) \in \mathbb{Z}[X]$  be the irreducible polynomial of  $t_i$  over  $\mathbb{Z}$  and  $f(X, Y)$  its homogenization (with  $f := Y$  in the special case  $t_i = \infty$ ). Let  $t_0 = a/b$  with  $a, b \in \mathbb{Z}$  co-prime, and let  $p$  be a prime number. Then  $I_p(t_0, t_i)$  is the multiplicity of  $p$  in  $f(a, b)$ ."

There is a distinct structure to the decomposition groups at ramified primes in function field extensions. To put it another way, the decomposition group's properties at  $p$  are determined by

## Reference

- [1]S. Beckmann, On extensions of number fields obtained by specializing branched coverings, J. Reine Angew. Math. 419 (1991) 27–53.
- [2]D. Bubboloni, J. Sonn, Intersective Snpolynomials with few irreducible factors, Manuscr. Math. 151 (2016) 477–492.
- [3]L. Caputo, S. Vinatier, Gauss sums, Jacobi sum and cyclotomic units related to torsion Galois modules, preprint, <https://arxiv.org/pdf/1402.3795>, 2014.
- [4]P. Dèbes, M.D. Fried, Nonrigid constructions in Galois theory, Pac. J. Math. 163(1) (1994) 81–122.
- [5]P. Dèbes, N. Ghazi, Galois covers and the Hilbert-Grunwald property, Ann. Inst. Fourier 62(3) (2012) 989–1013.
- [6]C. Frei, D. Loughran, R. Newton, The Hasse norm principle for abelian extensions, Am. J. Math. 140(6) (2018) 1639–1685.
- [7]M.D. Fried, H. Völklein, The inverse Galois problem and rational points on moduli spaces, Math. Ann. 290(4) (1991) 771–800.
- [8]B. Green, T. Tao, Linear equations in primes, Ann. Math. 171 (2010) 1753–1850. [9]M. Jarden, Algebraic Patching, Springer Verlag, 2011.
- [10]C. Jordan, Recherches sur les substitutions, J. Liouville 17 (1872) 351–367.
- [11]K. Kedlaya, A construction of polynomials with squarefree discriminants, Proc. Am. Math. Soc. 140 (2012) 3025–3033.
- [12]J. König, On intersective polynomials with non-solvable Galois group, Commun. Algebra 46(6) (2018) 2405–2416.

