# ON CLASS FIELD THEORY FROM A GROUP THEORETICAL VIEWPOINT

LUCIAN M. IONESCU

Abstract. The main goal of Class Field Theory, of characterizing abelian field extensions in terms of the arithmetic of the rationals, is achieved via the correspondence between Arithmetic Galois Theory and classical (algebraic) Galois Theory, as formulated in its traditional form by Artin.

The analysis of field extensions, primarily of the way rational primes decompose in field extensions, is done in terms of an invariant of the Galois group encoding its structure.

Prospects of the non-abelian case are given in terms of Grothendieck's Anabelian Theory.

Contents



## 1. Introduction

One of the main goals of Class Field Theory is describing field extensions of $k = \mathbf{Q}$ in terms of the arithmetic of the integers [2], and in particular characterizing how rational primes decompose in field extensions.

In the non-abelian case, regarding field extensions *arithmetically similar* if almost of the rational primes decompose in the same way, was already studied in terms of group theory in [1].

In this article we develop this direction of research for the case of abelian extensions, towards a functorial correspondence between what we call *Arithmetic Galois Theory* and the traditional Galois Theory we will refer to as "algebraic".

*Date*: May 5, 2022.

The umbrella framework of Anabelian Geometry, as envisioned by Grothendieck in the 1970s, include these two "good examples", together with the *Topological Galois Theory* of covering spaces and Theory of Ramified Covers of Riemann Surfaces.

Weber-Kronecker Theorem places abelian field theory in the context of cyclotomic extensions. As explained in the background section §2, the corresponding well known facts of CFT can be mapped (traced back) to group theoretical facts about finite abelian group $Z/n$ and its symmetry group of automorphisms $(Z/n^\times, \cdot)$. The correspondence between its subgroups and correspondence quotients is set into correspondence with the Galois Theory of the cyclotomic extension. The decomposition of primes there corresponds to the orbit structure of multiplication by primes etc..

The long-term goal is to systematically study:

1) The functoriality between Arithmetic and Algebraic Galois Theory and correspondences;

2) The decoposition of primes in field extensions, as corresponding to the orbit decomposition in the arithmetic side;

3) Applications of the above correspondence to Reciprocity Laws;

4) The Ramification Theory in interpretation in terms of Anabelian Geometry.

## 2. Arithmetic Galois Theory

The main point is to make precise what "arithmetic of **Q**" means, by considering the "reflection" of Galois Theory in the Klein Geometry of $(Z/n, +)$, as an abelian group.

We will consider first Abelian field extensions $BQ \to L \to Q(\zeta_n)$ over the rationals as a base field, with conductor $n$, i.e. the minimal root of unity allowing for an embedding in a cyclotomic extension. Its Galois group is $(Z/n^\times, \cdot)$.

### 2.1. A few examples.

Let us build the theory starting from examples.

2.1.1. *Gaussian integers.* Consider the familiar case of Gaussian integers $Z[i] = Q(\zeta_4)$. In this case the degree is $[Q(\zeta_n) : Q] = 2$ and the genus-degree-ramification equation yields $2 = e \cdot f \cdot g$, with the well known case: ramified, inert and split.

Let us look at the "arithmetic side". Given a prime $p$, multiplication by $p$, denoted $M_p : Z/p^t imes \to Z_p^\times$ determines the decomposition of primes as follows:

**Ramified case**. If $p\ modn$ is a zero divisor, then the prime ramifies. In our case, with $n = 4$, $gcd(p, 4) \neq 1$ implies $p = 2$. Then the index of $ker M_2$ gives the ramification index $e = 2$, and the short exact sequence $ker(M_2) \to Z/4 \to Z/2$ can be viewed as a *ramified cover* ...

**Unramified case**. If $p\ modn$ is in $Z/n^\times$, then it is unramified ($e = 1$) and the *arithmetic degree* is as follows:

a) $p \cong 1$ and $f = ord(p) = 1$, hence $g = 2$ the prime splits completely; e.g. $5 = (2 + i)(2 - i)$;

b) $p \cong 3$ and $f = ord(p) = 2$, hence $g = 1$ and the prime is inert; e.g. $p = 3$.

2.1.2. *Prime cyclotomic extensions.* Consider $n = 7$. Then the only ramified prime is $p = 7$ itself, with $e = ker(M_7) = p$ as well known.

If $gcd(q, p) = 1$ then the orders of $[p] = p \ mod\ 7$, divisors of $|G| = p - 1 = 6$, are as follows:

$$Table : [p] = 1, 2, 3, 4, 5, 6; \quad f = ord(p) = 1, 3, 6, 3, 6, 2$$

and, since $g = |G|/f$ is the index of the *arithmetic Frobenius subgroup* $C_f$, generated by $p$. The *arithmetic decomposition* short exact sequence is:

$$1 \to I = \{1\} \to D \to C_f,$$

where we insist to view the quotient $D = G/C_f$ as a "bundle" over the "Frobenius cycle" $C_f$, in anticipation of the non-split / non-abelian case.

For other example see [4] (see Galois Theory Examples)

## 3. Conclusions

Arithmetic Galois Theory aims to make precise what "arithmetic of **Q** means by considering the category $Z$ of finite abelian groups (see also [5].

Further developments are in view:

- Study the cyclotomic case and its subextensions (via KW-Theorem).

- Hint to ACFT Hurwitz Theorem about absolute Galois group, in the context of Anabelian geometry.

Furthermore:

I) Study $Z \to Q[Z]$ group ring correspondence and its quotients;

II) Study Artin functor and interpret in the context of Anabelian geometry; look for the Algebraic de Rham Cohomology and Periods ($\pi_1 = H_1$ here): derived functors of Group Ring? [adic completion, abeliantization]

III) What corresponds to $Q[Z]/f(x)$ in the arithmetic-Geometric side? [If not abelian then homotopy is more than homology]

IV) Study the Abelian Polynomial Th.: Split(f(x)) corresponds to congruences [i.e. corresponds to Spec(Z) covering maps] iff Gal(f(x)) is Abelian [by KW-Th. subgroup of Z/n].

Our overall goal is to bridge with Anabelian Geometry and Periods, or at least aim-and-shoot (even if missing big!); just to make the "typical Alg. NT reader" aware of the "Everests base camp" (Anabelian Geometry, Langlands programme, Motives and Periods).

V) Study Primes and Decompositions in quotients: Arithmetic (primes in field extensions), Algebraic (polynomials over finite fields), and the Correspondence (Reciprocity Laws; explaining what are these)

III) Determine the Group Invariant (see [6]) for the analysis of Galois Group Decompositions.

The author hopes that the various ideas only sketched will lead the reader to detailed works on the subjects mentioned.

## References

[1] Norbert Klingen, "Arithmetical Similarities: Prime decomposition and finite group theory", Oxford Mathematical Monographs, Clarendon Press, Oxford, 1998.
[2] Shemanske, Overview of Class field theory,
[3] Garbanati, Class Field Theory Summarized,
[4] Morandi, Field and Galois Theory
[5] L. M. Ionescu, On Galois Theory with an invitation to Category Theory, https://vixra.org/abs/2204.0104
[6] Fusun Akman, Graph Invariants of Finite Groups via a Theorem of Lagarias, https://arxiv.org/abs/math/0612618.

Department of Mathematics, Illinois State University, IL 61790-4520
*E-mail address*: lmiones@ilstu.edu,akmanf@ilstu.edu