ON GALOIS THEORY WITH AN INVITATION TO CATEGORY THEORY

LUCIAN M. IONESCU

ABSTRACT. Galois theory in the category of cyclic groups studies the automorphism groups of the cyclic group extensions and the corresponding Galois connection. The theory can be rephrased in dual terms of quotients, corresponding to extensions, when viewed as covering maps.

The computation of Galois groups and stating the associated Galois connection are based on already existing work regarding the automorphism groups of finite p-adic groups.

The initial goals for developing such a theory were: pedagogical, to introduce the basic language of Category Theory, while exposing the student to core ideas of Galois Theory, but also targeting applications to the Galois Theory of cyclotomic extensions, towards investigating some aspects of *Abelian Class Field Theory* and *Anabelian Geometry.*

CONTENTS

Date: April 18, 2022.

1. Introduction

Galois Theory had a long evolution from its foundations set by Evariste Galois in the 1800s and its Field Theory formulation by Artin in the 1940s, to its modern days "descendents", which includes Grothendieck's *Anabelian Geometry* [2], Chasse and Sweedler's Hopf-Galois Theory [3] as well as work by G. C. Rota in the 1970s [26, 27, 28] in the G-sets framework, as well as more recent investigations of lattices of periods of group actions [29, 30].

In this article we will define the Galois Theory in the Category of cyclic groups, as a stepping stone for relating cyclotomic extensions and primes (Galois group) decomposition within the arithmetic realm, part of the theory of group acting on sets and corresponding theory of periods.

While the emphasis is to generalize the scope of Galois Theory point of view, the corresponding computations and results are based on prior work on automorphisms of finite abelian groups [4, 5, 6, 7, 9, 8].

Part of the motivation for this work comes from the need to blend the use of Category Theory with the usual set-oriented presentations of Abstract Algebra, covering the transition from undergraduate to graduate studies in Mathematics.

An "invitation to Category Theory" is included, by introducing the category $|CZ$ of cyclic groups, and actual use of some foundational terms, in such a way that a quick consultation of Wikipedia by the non-specialist would suffice in providing the additional details.

Defining extensions in this category and the corresponding Galois groups, is followed by an exposition of the associated Galois connection. Incidentally, this work build on, and generalizes, the recent articles documenting the automorphism group of finite abelian groups (refs here) ...

The dual picture of quotients associated to embedding, as a nice feature of this abelian category, allows to put the two Galois Theories together, in the framework of groups extensions (short exact sequences).

The action of Z on cyclic groups allows to present the theory of decomposition of primes in this context belonging to Elementary Number Theory, as a preparation with the more advanced treatment as part of Algebraic Number Theory.

Applications to cyclotomic extensions and prime decomposition are only sketched, as a preview, to be documented in a follow-up article. The relation between Arithmetic Galois Theory in category Z and classical Galois Theory, is provided by the group ring and group of units functorial adjunction. It is only "announced", being left to the follow-up article.

2. The Diophantine Line as the "Toy" Category $\mathcal{Z}$

The two main examples of Galois connections occur in the original Galois Theory, within the classical context of field theory, and more recently after Poincare's development of Topology, in the Theory of Covering Spaces.

The two points of view are dual, representing in categorical parlance the case of *monomorphisms* and that of *epimorphisms* [23][1].

2.1. Objects and Morphisms in $\mathcal{Z}$.

The objects of the category are the cyclic groups $Ob(Z) = \{Z, Z/n\}$, where Z/nZ is abreviated as Z/n[2]

The morphisms are the (abelian) group homomorphisms, which since the groups are cyclic, are determined by the image of the generator: $M_d : A \to B, M_d(x) = kx$, with $A, B \in Ob(Z)$. For example $M_2 : Z/6 \to Z/4$ has the kernel isomorphisc to $Z/3$ and the image (iso to) $Z/2$. Of course the only morphism from a torsion to a free group is $0 : Z/3 \to Z$; the other direction, from free to torsion, we only have quotients, e.g. $M_6\ mod 3 : Z \to Z/3$.

2.2. Mono, epi and duality.

The *extensions* in this category are the monomorphisms $M_d : Z \to Z$ and $M_d : Z/d \to Z/n, n = d \cdot d'$. They correspond to the subgroups of Z/n, which in turn correspond to the divisors of n. Correspondingly we have a lattice of monomorphisms, subgroups or divisors, depending on the viewpoint chosen.

Since our objects abelian, the *category is abelian*, and each extension is a *Galois extension* ("normal"), representing the *kernel* of the corresponding quotient, of the target group by its image, as a subgroup:

$$Z/d \to Z/n \to Z/d', \quad and \quad Z \to Z \to Z/n.$$

Putting these together yields a short exact sequence, which is an instance of a more general mono-epi duality: *Pontriagin duality.*

3. The Galois Theory in the Category of Abelian Groups

The only *Galois objects* in the sense of [3] considered here are the "tautological ones", where the group of automorphisms of on object acts on the corresponding object.

3.1. Galois Objects and Galois Groups.

Definition 3.1. Given a Galois extension $A \to B$ in $\mathcal{Z}$, the associated *Galois group* is:

$$Gal(A/B) = \{\phi \in Aut_{Ab}(B) | \phi_{|A} = Id_A,$$

[1] For an ample treatment, see [24] or [25].

[2] Z could be assimilated as $Z/0$, but we prefer to distinguish the free case from the torsion case.

consisting of the automorphisms of B (in our category), that preserve A, and restrict to A as identity (fix A, for short).

Remark 3.1. Such a subgroup of automorphisms of finite abelian groups were studied by [4] and subsequent related articles [6] etc., as far back in time as 1969, but the connection with Galois Theory was not made explicitly.

In our case of cyclic groups, where the "prime sectors are distinct, non-interacting (no non-trivial homocyclic groups present), the determination of Galois groups is easy.

In the free case $M_n : Z \to Z$, $Gal(M_n) = 1$ (we prefer to indicate the extension itself), is trivial.

In the torsion case, the Chinese Remainder Theorem reduces it to the case of primary groups Z/p^k.

3.2. **On Abelian Groups and Their Symmetries.** The brief description included below will be accompanied by some suggested mental pictures, with physics-content oriented yet totally optional, in order to facilitate the understanding of the facts.

3.2.1. *The Structure of Abelian Groups.* Finite abelian groups are direct sums $A = \oplus_p A_p$, of $p-sectors$ (p-groups), thought of as capable of fundamental vibrations, harmonics of a fundamental associated to the prime p.

Each $p-sector$ is a product of *homocyclic p-groups* $H_p(k;n) = C^n_{p^k}$, thought of as a "space-time block", of space-width (rank) n, and "time-depth/resolution" k, common to all the "strands" of the discrete space.

Remark 3.2. When there are at least two strands $n > 1$, permutations of the strands may enter the picture, and a version of Cayley's Theorem shows the possible complexity of its automorphism group ([9], Th. 3.2, p.3):

Theorem 3.1. *Let $k > 1$. Then every finite group G (Monster included!), is iso to a subgroup of $Aut(C^n_k)$, for some n.*

Remark 3.3. The presence of different "time-depth" summands in a p-sector of a finite abelian group, adds additional complexity to the structure of the corresponding automorphism group [7, 6, 8].

In fact Z/p^k is a truncation of p-adic numbers, representing a $k-th$ order deformation of its "tangent space", the finite field F_p [32]. Mixing various orders of deformation seams "artificial" anyways, and a full treatment of the p-adic case, in the spirit of Hasse's work, is probably beneficial for clarifying and simplifying the theory.

Given an abelian group A, the following are important *fully invariant subgroups*:

$$A[p^n] = \{x \in A | p^n x = 0\}, \qquad p^n A = \{p^n x | xinA\}.$$

Multiplication by p acts as a shift on each C_{p^e} summand in A_p, hence p^nA results in "shifting the coefficients" of x to the "right", towards higher powers (orders) of p. Note that in spite of the apparent "grading" by the power of p, due to the possible carry-over digit under addition or multiplication, the power/exponent is not a grading, but rather defining a *descending filtration* ([4], p.24):

$$A \supseteq pA \supseteq p^2A ... \supseteq p^\lambda A = 0,$$

where λ is the maximum order of deformation / length of the cyclic p-summands ${C_p}^e$[3].

Similarly, $A[p^n]$ form an ascending filtration, "orthogonal" under multiplication to the above one, where n can be visualized as the index of the leading non-zero p-adic digit of one of its elements.

Example 3.1. For our cyclic case $A = Z/p^k$, the two filtrations coincide are correspond to lattice of its subgroups, which in turn correspond to the divisors of p^k. This can be also viewed as a tower, as follows:

$$0 \to Z/p \to Z/p^2 \to ... \to Z/p^k = A,$$

where at each step the image is the maximal non-trivial subgroup.

3.2.2. *On the Structure of Automorphisms of Abelian groups.* For our purpose in this article, we will present the known results on automorphism groups presented in [8], recast in the framework of Galois Theory introduced above.

To exemplify the main concepts and avoid technicalities, we will focus on the primary groups Z/p^k, leaving the homocyclic group case to the interested reader to document (see also [8], §4, p.564).

For a homocyclic group H, each "step" in the filtration determines the following short exact sequence structure of the corresponding Galois group ([8], Lemma 3.1, p.561):

$$0 \to Hom(H, pH) \overset{\sigma}{\to} Aut(H) \overset{\rho}{\to} Aut(H[p]) \to 0,$$

where the first map $\sigma(\phi) = 1 + \phi$[4], and the second map ρ, is the restriction to the fully invariant subgroup $H[p]$.

Example 3.2. Apply the result to $A = Z/p^k$. Since $Hom(A, pA) \cong Z/p^{k-1}$ and $H[p] \cong Z/p$, hence $Aut(A[p]) \cong Z/p - 1$, applying the Chinese Remainder Theorem to show the sequence splits, yields the well known fact [9], p.1:

$$Aut(Z/p^k) = Z/(p-1)p^{k-1}.$$

[3] For a homocyclic summand $H_p(k;n)$, $\lambda = k$.

[4] $Hom(H, pH)$ plays the role of a Lie generator of the group element, the corresponding automorphism.

3.3. **Galois Groups of Primary Abelian Groups Z/p^k.** "Dissecting" the full Galois group $Aut(G)$ [8], §4, proceeds by "peeling" layer-by-layer, from the top, and yielding the corresponding Galois connection.

For example, $Aut_{pG}(G)$ is, with our notation, $Gal(pG \to G)$. Its structure results from the following (loc. cit. Proposition 4.3, Lemma 4.4 and Proposition 4.5):

Proposition 3.1. *Given A a finite abelian p-group, there is a short exact sequence:*

$$0 \to Gal(pG \to G) \to Aut(G) \to Aut(pG) \to 0,$$

where by the previous result:

$$0 \to Hom(G/pG, pG) \to Gal(pG \to G) \to Aut(G/pG) \to 0.$$

If $G[p] \subset pG$ then $\phi : G \to pG$ is epi, and:

$$Gal(pG \to G) = \{1 + \xi\phi | \xi \in Hom(G/pG, pG)\} \cong Hom(G/pG, pG).$$

The restriction $G[p] \subset pG$ excludes the "too short case" F_p summand of a homocyclic group; this would require a separate study of $G = G_1 \oplus H$, with $G_1 = F_p^n$ (loc. cit. p.565; Proposition 4.6).

The primary p-groups can be viewed as k-th order truncions of p-adic integers: $Z/p^k = \{a_0 + ... + a_{k-1}p^{k-1} | a_i \in F_p$ [5].

In this case, iteration of the above "peeling procedure" of the Galois groups yields a chain of fully invariant subgroups in $Aut(G)$. Together with the sequence of fully invariant subgroups of G, allows to define a correspondence, called a Galois connection, and explained next.

3.4. **The Galois Connection.** Recall that the Galois correspondence between subgroups of the Galois group and subextensions is called the *Galois (antitone) connection* [15], and constitutes the central result of Galois Theory [22].

Reinterpreting Remark 4.7 from [8], p.567, we have the following *instance* of an antitonal Galois connection in the category of finite abelian groups.

Let G be a finite abelian p-group.

Definition 3.2. Let $(\mathcal{N}, <)$ the lattice of fully invariant subgroups p^nG of G. Correspondingly let $(\mathcal{G} = \{Gal(p^nG \to G) = Aut_{p^nG}(G)\}, <)$ be the lattice of Galois groups of the corresponding extensions.

Define the following two maps $Gal : (\mathcal{N}, <) < - > (\mathcal{G}, <) : Fix$:

$$Gal(K) = Gal(K \to G), \quad Fix(H) = \{x \in G | \phi(x) = x, \forall \phi \in H\}.$$

A partial version of the main theorem of the *Arithmetic Galois Theory* in the category of finite abelian groups $\mathcal{A}b_{fin}$, is the following.

Theorem 3.2. *The two maps Fix and Gal form an antitonal Galois connection for the chains of fully invariant subgroups p^nG and corresponding Galois groups.*

[5] These are in fact k-th order deformations of the finite field [32]; but we will not need this here.

Remark 3.4. Note that the Galois connection between the two chains of subobjects and subgroups of automorphisms (Galois groups) involves only the fully invariant subgroups of a finite abelian p-group G.

3.5. **The Cyclotomic Case.** In view of our goals to relate Arithmetic Galois Theory and field theory Galois Theory, including the understanding of prime decompositions, we are particularly interested in the case where G is cyclic.

The above partial result on Galois connection in the category of abelian groups specializes to the full Galois Theory in the category $\mathcal{Z}$ of cyclic groups, to be adressed elsewhere.

4. Conclusions

Recall briefly our goals: pedagogical, to relate Category Theory, Abelian groups and to present the foundations of Algebraic Class Field Theory.

The Categorical Theory framework emphasises mono vs. epi duality, objects and their symmetries.

The novelty consists in showing why (and how) the Arithmetic / Algebraic Galois Theories correspond: this is due to the group ring / group of units adjunction. This adjunction will be documented elsewhere.

References

[1] Emil Artin, "Galois Theory", 1944; Dover Publications, 1998.

[2] Wikipedia, Anabelian geometry, https://en.wikipedia.org/wiki/Anabelian_geometry

[3] S. U. Chasse and M. E. Sweedler, Hopf algebras and Galois Theory, LNM 97, Springer-Verlag Berlin, 1969.

[4] Paul Hill, "The automorphisms of primary abelian groups", ..., 1969.

[5] Hans Lieback, "The automorphism group of finite p-groups", Journal of Algebra **4**, 426-432 (1966).

[6] C. J. Hillar and D. L. Rhea, "Automorphisms of finite abelian groups", ...

[7] Marek Golasinski and Daciberg Lima Gonsalves, "On automorphisms of finite abelian p-groups", Mathematica Slovaca, **58** (2008), No.4, 405-412.

[8] A. Mader, "The automorphism group of finite abelian p-groups", ..., 2012.

[9] Bill Semus and Sam Smith, "On the structure of the automorphism group of some finite groups", ...

[10] Wikipedia, Category Theory, https://en.wikipedia.org/wiki/Category_theory

[11] H. Simmons, "An introduction to Category Theory", http://www.cs.man.ac.uk/˜hsimmons/zCATS.pdf

[12] Wikipedia, "Group ring:Adjoint", https://en.wikipedia.org/wiki/Group_ring#Adjoint

[13] Norbert Klingen, "Arithmetical Similarities: Prime decomposition and finite group theory", Oxford Mathematical Monographs, Clarendon Press, Oxford, 1998.

[14] Fusun Akman, Graph invariants of finte groups via a theorem of Lagarias, JP JANTA, Vol. 8, No.2, 2007, pp. 227-258

[15] Wikipedia, Galois Connection, https://en.wikipedia.org/wiki/Galois_connection

[16] T. Schemanske, An overview of Class Field Theory, https://math.dartmouth.edu/t̃rs/expository-papers/tex/CFT.pdf

[17] Garbanati, Class Field Theory Summarized, Rocky Mountain Journal of Mathematics, Vol. 11, No.2, p. 195-225, Spring 1981.

[18] Chris Hillman, An outline of the theory of G-sets, 1996.
https://www.researchgate.net/publication/2651486_An_Outline_Of_The_Theory_Of_G-Sets

[19] Oystein Ore, Galois connections, Trans. Amer. Math. Soc. 55 (1944), 493-513.

[20] M. Erne, J. Koslovski, A. Melton, G. E. Strecker, "A Primer on Galois Connections", Annals of the New York Academy of Sciences, Papers on General Topology and Applications, Volume 704, Issue 1, December 1993, Pages 103-125.

[21] Patrick Morandi, Galois connections, http://sierra.nmsu.edu/morandi/oldwebpages/Math683Fall2013/GaloisConne

[22] Jean-Pierre Tignol, "Galois' Theory of Algebraic Equations", . World Scientific, 2001.

[23] Dennis Eriksson, "Galois Theory and Coverings", Normat 59:3, 18 (2011), http://www.math.chalmers.se/ dener/Galois-theory-of-Covers.pdf

[24] Harold Stark, "Galois Theory, Algebraic Number Theory, and Zeta Functions", *From Number Theory to Physics*, pp 313-393, Springer-Verlag Berlin Heidelberg 1992.

[25] Askold Khovanskii, "Galois Theory, Coverings, and Riemann Surfaces", Springer, 2013.

[26] G.-C. Rota, "Baxter Algebras and Combinatorial Identities I and II, Bull. of Amer. Math. Soc. 75 (1969), 325-329 and 330-344.

[27] G.-C. Rota and D. A. Smith, "Enumaration under group action", Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 4e series, tome 4, no.4 (1977), p.637-646.

[28] G.-C. Rota and B. Sagan, "Congruences derived from group action", Europ. J. Combinatorics (1980) **1**. 67-76.

[29] Huseyin Acan, "The Lattice of Periods of a group action and its topology", Thesis Bilkent University, 2006, http://www.thesis.bilkent.edu.tr/0003103.pdf

[30] W. F. Doran, "The Lattice of Periods of a Group Action", Adv. in Math., **110**, 88-108, (1995).

[31] L. M. Ionescu, A discrete analog of de Rham cohomology on finite abelian groups as manifolds, JP Journal of Algebra, Number Theory and Applications Volume 39, Issue 6, Pages 891 - 906 (December 2017).

[32] L. M. Ionescu, "On p-adic Frobenius lifts and p-adic periods, from a Deformation Theory viewpoint", https://arxiv.org/abs/1801.07570

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