Arithmetic Galois Theory

Part II

Slides

Lucian M. Ionescu
Illinois State University

Sept. 26, 2019

Evariste Galois (1811-1832)

Abstract

• History of Galois Theory has several important stages of development: Galois, Artin, Grothendieck, Chasse and Swedler, and many others recently.

• A goal in Algebraic Number Theory is to precisely formulate what is the "arithmetic of a field extension".

• Category Theory provides a coherent viewpoint to develop Arithmetic Galois Theory.

• Besides the pedagogical role of Arithmetic Galois Theory, a nice application is understanding the decomposition of primes in field extensions, in terms of the arithmetic of Galois group (Abelian case).

From Galois to Artin

• 1800s Galois Theory as sketched by Galois, had some roots in the work of Lagrange (group theory and resolvents). Galois had other less know contributions shared with Chevalley, concerning finite fields and finite groups of symmetry $PSL_n(F_q)$.

• The classical facts of Algebraic Number Theory developed by Kummer, Dedekind and Eisenstein in the 1800s, were recast in the "modern" language of field extensions and Galois groups by Artin around 1920s, after considerable progress done by Hilbert (Class Field Theory).

• The present form of presenting Galois Theory in most (all?) Abstract Algebra textbooks consists in restating Dedekind version (UG), and in more advanced texts, following Artin.

Update: Category Theory and Grothendieck

• 1940s: a new math language was formulated by Eilenberg and MacLane. Grothendieck embraces it, and, among other things, formulates an algebraic version of *homology* and *homotopy*: *Abelian and Anabelian Geometry*.

• Anabelian geometry is a theory of the algebraic fundamental group. Galois group is a prominent example.

• The prototype is the fundamental group in TOPOLOGY. A simpler, well understood case is that of the Category of *covering spaces and deck transformations*.

• The abstract case of Galois Objects and Connections provide the guidelines for designing *Arithmetic Galois Theory*, as a natural SET counterpart of Galois Theory in VECTOR SPACES.

Galois Objects and Hopf Algebras

• 1970s work by Chase and Sweedler, in a categorical framework: Galois object, Hopf algebras, sheaf theory etc.

• 2000s work by others: from Galois group G to group ring kG, which is a Hopf algebra, then looking at other cocomutative coproducts ...

Galois Objects and Connections

• In a category, and object A has "symmetries" $Aut(A)$, and a Galois connection is an inverse correspondence between its subobjects and subgroups of G.

• let $\mathcal{C}$ be a category with finite products. A Galois object (G, X) is a group object G acting on X, i.e. a *representation*:

$$G \to Aut(X).$$

For more details see Chasse and Sweedler 1970s.

• A *Galois connection* can be defined using various "languages": from combinatorial language of POSets, to Categorical Language of *adjunct functors* (see Wikipedia).

... we skip forward to our examples!

Algebraic Number Theory, Topology and Arithmetic

- **Field extensions** and Galois groups (well known);
- **Covering mappings** and deck transformations (a few pictures!);
- The analogy is well known; see Dennis Errikson, or Harold Stark;
- Our category $\mathcal{Z}$: the discrete affine line Z, and its quotients:

$$Universal\ cover : Z \to Z/n, \quad quotients : Z/n \to Z/m, m|n.$$

This is an algebraic version of covering spaces and deck transformations.

- Cyclic groups are instrumental for Abelian extensions, which can be studied as subextensions of cyclotomic fields $Q(\zeta_n)$, with their galois Group

$$Gal(Q(\zeta_n)/Q) \cong (Z/nZ^{\times}, \cdot) \cong Aut(Z/nZ, +).$$

LHS "lives" in Alg. NT (k-VECT and FIELDS), while RHS "lives" in Elem. NT (SETS and GROUPS).

Apply Galois Objects Theory to Our Category $\mathcal{Z}$

• Category: extensions and Galois automorphisms, or discrete covering spaces and transformations:

$$n|m \quad : Z/n \hookrightarrow Z/m \qquad Z/mZ \twoheadrightarrow Z/nZ.$$

Short exact sequences or *Pontryagin duality* reveals the duality.

- Galois Objects: $G = Z/nZ^{\times}$ acting on $A = A/nZ$ by multiplication.

- Note that $Aut(A) -> End(A)$ allows to deal with ramification, when considering how primes split, ramify or are inert.

- Everything is "normal" here (Abelian), and the extensions (subgroups) are in 1:1 correspondence with the lattice of divisibility ("category"): for cyclic groups size determines the subgroup.

- The *Galois connection* is the obvious correspondence via the divisibility lattice (TB documented).

The Galois Connection

• Extensions of Z/m in Z/n correspond to the divisibility lattice: $m|d|n$, and the arithmetic Galois groups $Gal(Zn//Zm)$ correspond inversely, to the symmetry group $Zd^{\times}$, of the cofactor d of d in n.

• Example $n = 6$ divisibility lattice vs. Hasse diagram of $Z6$ (label with indexes etc. as in GT).

Note: This is quite trivial (UG Elementary Number Theory: exercise in CRT & Galois Connections), but corresponds functorially to the Abelian Field Theory side, via group ring construction and taking the maximal irreducible summand [TB explained elsewhere].

... what *is* interesting, is how the splitting of a prime q in Abelian extensions, in GT, can be read out of the multiplication by q in Arithmetic Galois Theory.

Recall on Decomposition of Galois Group

Fix an odd rational prime q and a Galois extension $G = Gal(K/Q)$. The prime ideal (q) factors into prime ideals $Q_1^{e_1} ... Q_g^{e_g}$, with ramification multiplicities e_i and "width" (genus) g. Correspondingly the *symmetry group* reflects this decomposition of (q):

$$1 \to Inertial \to Decomposition \to Cyclic_f, \quad |G/D| = g.$$

The type of decomposition can be determined in various ways:
A) By definition of decomposition of Galois group;
B) Using a primitive element $K = Q(\theta) = Q[x]/(f(x))$, and determining how $f(x)$ factors modulo q;
C) In the Abelian / cyclotomic case, using the action of multiplication my q on the "space" Z/n (includes the ramified case), or, if q does not divide n, the *induced automorphism* and its orbit-stabilizer action: *Arithmetic Galois Theory*.

From Rational to Gaussian Primes

- Primitive residues generate the group Zn*, and correspond to automorphisms; think (compare with) Galois symmetry: $\phi \leftrightarrow 1 \rightarrow g$.

- The Z-Mod version is $\phi = M_q$ where $M_q(x) = qx, x \in Zn$. Now the powers of q correspond to the composition iterate of M_q, i.e. $q^k \leftrightarrow \phi^k$.

- Ex. $Z_4* = 1, 3$ will be used to find how rational primes split in Gaussian primes, in the Galois extension $Q \rightarrow Q(z4)$, in the Arithmetic Galois Theory side. We need the multipliers ($n = 4$):

$$M : Z \rightarrow End(Zn), \quad Ker(M) = nZ \ induces \ M : Z4 \rightarrow End(Z4).$$

[Hint: Splitting corresponds to $Spec(Z) = P$ and prime $p \rightarrow Mp$ in $End(Z4)$.]

Note: ramification and splitting/inert behaviour are unified via $Aut(A) \rightarrow End(A)$ ...

Z-Module Viewpoint

- Defining polynomial of the $Q(i)/Q$ extension is $f(x) = x^2 + 1$

- Primes split according to $p = kmod4$:
  $p = 1\ mod\ 4$, e.g. 13: see $x^2 + 1 = (x - a)(x - b)\ mod\ 13$, a and b square roots of -1 in $Z13$.
  $p = 2\ mod\ 4:\ \ p = 2, X^2 + 1 = (x + 1)^2\ mod\ 2$ [Note: $2x = M2(x) = 0$]
  $p = 3\ mod\ 4$: e.g. $p = 7, x^2 + 1$ irreducible $mod\ 7$.

- Remark: These facts "translate" into the Z-Mod language, in terms of $Mp(x) = px$ in $Z4$, and its primary decomposition.

Cyclotomic extensions - prime sector $Q(\zeta_p)$

• Galois group $G = Zp*$, degree $n = |Gal(Q(\zeta_p)/Q)| = p - 1$.

• Odd primes q split according to the structure of Mq(x) on Z/p: it determines the Galois decomposition on the arithmetic side:

$$Ip \to D \to C_p, \quad |Ip| = e,\ |Cp| = p^f,\ |G/D| = g,\ p - 1 = efg.$$

• The only ramified prime is p itself (totally ramified $e = p - 1$):
Algebraic: $p|Disc((x^p - 1)/(x - 1)) = (-1)^{(p-1)/2}p(p - 2)$ ...
Arithmetic: $Mp = 0$, and must look at the covering map $Z- > Z/p$
[Nice geometrically meaningful pictures of "branching covers" ... not now!]

• Non-ramified case $q <> p$, hence $Mq(x)$ is an automorphism. Its multiplicative order determines the decomposition of the *arithmetic Galois group* $Z_p^\times$, hence allows to determine the type of decomposition of the prime q in the p-cyclotomic extension.

Prime Power Cyclotomic Extensions $Q(\zeta_{p^m})$

The well-known "facts" stated in the context of Galois Theory, can be traced back to the arithmetic setup, *to clarify its origin*:

[Ciurca], p.50: **Theorem 2.3.2.** *We have the following classification of prime decomposition in a prime power cyclotomic field* $Q(\zeta_{p^m})$ ... etc.
The inertial degree is $f = ord_{Z/(p^m)} = \phi(p^m)/d$;
The genus (number of factors) is d.

[Conrad], p.5: **Theorem 2.8.** *When n is not divisible by p, the image of* $Gal(F_p(\zeta_n)/F_p)$ *in* $Z/nZ^\times$ *is* $< p \bmod n >$. *In particular* $[F_p(\zeta_n) : F_p]$ *is the order of p mod n.*

• The analysis of the *Klein Geometry* Z/nZ and $Z/nZ^\times$ and the various *finite dynamics* M_q is worth studying *per se*; math applications: decomposition of primes!

Actions and Decompositions

• The decomposition of a prime number / ideal is in fact the decomposition of the Z-action on a SET (Arithmetic GT) or MODULE (Algebraic GT).

• Such a decomposition of the *target space* due to the *image*, leads to a *decomposition of the group* via *Orbit-Stabilizer Theorem*: essentially division partitions of $G/Stab$ (compare with [Akman-2006]).

• In our arithmetic case $M_q = M_{ram} \times Aut$ (typical of endomorphisms of p-adic numbers), has a ramified part due to a "derivative" (shifts/projections in p-sectors of Frobenius type), and the split-inertia phenomenon is the usual *Extension vs. Deformation Alternative* (e.g. p-adic numbers and their extensions).
• The "Global-Functorial Picture" is interesting, involving *Spec* of the coefficients Z, which correspond to irreducible polynomials in a deformation $Z[p]$ via Cohen's Th., and prime quotients (extensions): *Reciprocity Laws* and decompositions of spectra.

"Reducing" the Galois Group Action

• While the theory of decomposition of primes is classical and well documented, the *idea* of *reduction modulo a prime* was not noticed to be realizable by **reducing / remapping the action of the Galois group** on the "source" of the group ring functor, which yields a decomposition of fields corresponding to the factorization of $x^n - 1$ in cyclotomic polynomials.

• Plainly put, the group ring functor $Q[]$ or $Z[]$ is compatible with automorphisms $Aut()$; hence the Galois group of an irreducible piece (field extension) is the same $Gal(Q(\zeta_n)/Q) = Z_n^\times = Aut(Z/nZ)$, and the decomposition of Z-actions on the algebraic side corresponds to the decomposition on the arithmetic side ...

Conclusions and Further Developments

- A bit of Category Theory helps;
- The Arithmetic in Z, the *discrete number line* (before we teach the "Real" Number Line), relates to DIVISIBILITY so-so nice and easely, that is a playing graund for learning some TOPOLOGY and Galois Theory, without even knowing it! (Select your keywords carefully; no need to define the full version).
- Arithmetic Galois Theory exhibits the decomposition theory in *Module Theory*, as well as the *Topology* framework. Claim: it corresponds functorially with Abelian Galois Theory.
- There is much more to it: discrete de Rham cohomology (LI), as algebraic de Rham cohomology (Grothendieck) relates to Anabelian Geometry and Motives (Grothendieck, Ayoub, Yves Andre etc.), clarifying what Periods are all about (LI: NSF GP 2019).

The End

Outline

Bibliography

• L.M. Ionescu, Arithmetic Galois Theory - Part I, www.ilstu.edu/ lmiones

• S. U. Chasse and M. E. Sweedler, "Hopf Algebras and Galois Theory", LNM 97, 1969.

• T. Crespo, A. Rio and M. Vela, "From Galois to Hopf Galois: Theory and Practice", Contemporary Mathematics, Vol. 649, 2015.

• Tudor Ciuca, "Arithmetic of cyclotomic fields", 2018.

• Keith Conrad, "Cyclotomic extensions", https://kconrad.math.uconn.edu/blurbs/galoistheory/cyclotomic.pdf

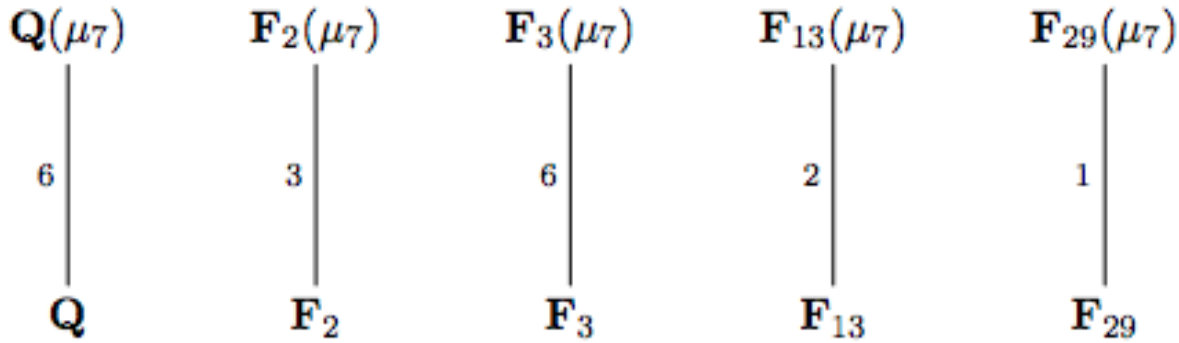
• Fusun Akman, "Graph Invariants of Finite Groups via a Theorem of Lagarias", math/0612618, 2006

• Harold Stark, "Galois Theory, Algebraic Number Theory and Zeta Functions".

• Dennis Errikson, "Galois Theory and Coverings", http://www.math.chalmers.se/ dener/Galois-theory-of-Covers.pdf

Additional Examples of Primes Splitting in $Q(\zeta_7)$

Example 2.9. The degree $[\mathbf{F}_p(\mu_7) : \mathbf{F}_p]$ is the order of p mod 7 that is 1, 2, 3, or 6 (if $p \neq 7$). The field diagram below gives some examples.



These are all consistent with how $(T^7-1)/(T-1) = T^6+T^5+\cdots+T+1$ factors modulo each of the primes: into irreducibles of common degree $[\mathbf{F}_p(\mu_7) : \mathbf{F}_p]$.

$$\begin{aligned} T^6+T^5+T^4+T^3+T^2+T+1 &\equiv (T^3+T+1)(T^3+T^2+1) \bmod 2 \\ &\equiv \text{irreducible mod } 3 \\ &\equiv (T^2+3T+1)(T^2+5T+1)(T^2+6T+1) \bmod 13 \\ &\equiv (T-7)(T-16)(T-20)(T-23)(T-24)(T-25) \bmod 29. \end{aligned}$$