ISSN 1464-8997 (on line) 1464-8989 (printed)

Geometry & Topology Monographs
Volume 3: Invitation to higher local fields
Part II, section 10, pages 299–304

10. Galois modules and class field theory

Boas Erez

In this section we shall try to present the reader with a sample of several significant instances where, on the way to proving results in Galois module theory, one is lead to use class field theory. Conversely, some contributions of Galois module theory to class fields theory are hinted at. We shall also single out some problems that in our opinion deserve further attention.

10.1. Normal basis theorem

The Normal Basis Theorem is one of the basic results in the Galois theory of fields. In fact one can use it to obtain a proof of the fundamental theorem of the theory, which sets up a correspondence between subgroups of the Galois group and subfields. Let us recall its statement and give a version of its proof following E. Noether and M. Deuring (a very modern proof!).

Theorem (Noether, Deuring)**.** *Let K be a finite extension of $\mathbb{Q}$. Let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. Then L is isomorphic to $K[G]$ as a $K[G]$-module. That is: there is an $a \in L$ such that $\{\sigma(a)\}_{\sigma\in G}$ is a K-basis of L. Such an a is called a normal basis generator of L over K.*

Proof. Use the isomorphism

$$\varphi\colon L \otimes_K L \to L[G], \quad \varphi(x \otimes y) = \sum_{\sigma\in G} \sigma(x)y\sigma^{-1} ,$$

then apply the Krull–Schmidt theorem to deduce that this isomorphism descends to K. Note that an element a in L generates a normal basis of L over K if and only if $\varphi(a) \in L[G]^*$.

Published 10 December 2000:

10.1.1. Normal integral bases and ramification.

Let us now move from dimension 0 (fields) to dimension 1, and consider rings of algebraic integers.

Let p be a prime number congruent to 1 modulo an (odd) prime l. Let $L_1 = \mathbb{Q}(\mu_p)$, and let K be the unique subfield of L_1 of degree l over $\mathbb{Q}$. Then $G = \mathrm{Gal}(K/\mathbb{Q})$ is cyclic of order l and K is tamely ramified over $\mathbb{Q}$. One can construct a normal basis for the ring $\mathcal{O}_K$ of integers in K over $\mathbb{Z}$: indeed if ζ denotes a primitive p-th root of unity, then ζ is a normal basis generator for $L_1/\mathbb{Q}$ and the trace of ζ to K gives the desired normal integral basis generator. Let now $L_2 = \mathbb{Q}(\mu_{l^2})$. It is easy to see that there is no integral normal basis for L_2 over $\mathbb{Q}$. As noticed by Noether, this is related to the fact that L_2 is a wildly ramified extension of the rationals. However there is the following structure result, which gives a complete and explicit description of the Galois module structure of rings of algebraic integers in absolute abelian extensions.

Theorem (Leopoldt 1959)**.** *Let K be an abelian extension of $\mathbb{Q}$. Let $G = \mathrm{Gal}(K/\mathbb{Q})$. Define*

$$\Lambda = \{\lambda \in \mathbb{Q}[G] : \lambda\mathcal{O}_K \subset \mathcal{O}_K\}$$

where $\mathcal{O}_K$ is the ring of integers of K. Then $\mathcal{O}_K$ is isomorphic to Λ as a Λ-module.

Note that the statement is not true for an arbitrary global field, nor for general relative extensions of number fields. The way to prove this theorem is by first dealing with the case of cyclotomic fields, for which one constructs explicit normal basis generators in terms of roots of unity. In this step one uses the criterion involving the resolvent map φ which we mentioned in the previous theorem. Then, for a general absolute abelian field K, one embeds K into the cyclotomic field $\mathbb{Q}(f_K)$ with smallest possible conductor by using the Kronecker–Weber theorem, and one "traces the result down" to K. Here it is essential that the extension $\mathbb{Q}(f_K)/K$ is essentially tame. Explicit class field theory is an important ingredient of the proof of this theorem; and, of course, this approach has been generalized to other settings: abelian extensions of imaginary quadratic fields (complex multiplication), extensions of Lubin–Tate type, etc.

10.1.2. Factorizability.

While Leopoldt's result is very satisfactory, one would still like to know a way to express the relation there as a relation between the Galois structure of rings of integers in general Galois extensions and the most natural integral representation of the Galois group, namely that given by the group algebra. There is a very neat description of this which uses the notion of factorizability, introduced by A. Fröhlich and A. Nelson. This leads to an equivalence relation on modules which is weaker than local equivalence (genus), but which is non-trivial.

Let G be a finite group, and let $S = \{H : H \leqslant G\}$. Let T be an abelian group.

Definition. A map $f: S \to T$ is called *factorizable* if every relation of the form

$$\sum_{H \in S} a_H \operatorname{ind}_H^G 1 = 0$$

with integral coefficients a_H, implies the relation

$$\prod_{H \in S} f(H)^{a_H} = 1 .$$

Example. Let $G = \mathrm{Gal}(L/K)$, then the discriminant of L/K defines a factorizable function (conductor-discriminant formula).

Definition. Let $i: M \to N$ be a morphism of $\mathcal{O}_K[G]$-lattices. The lattices M and N are said to be *factor-equivalent* if the map $H \to |L^H : i(M)^H|$ is factorizable.

Theorem (Fröhlich, de Smit)**.** *If $G = \mathrm{Gal}(L/K)$ and K is a global field, then $\mathcal{O}_L$ is factor-equivalent to $\mathcal{O}_K[G]$.*

Again this result is based on the isomorphism induced by the resolvent map φ and the fact that the discriminant defines a factorizable function.

10.1.3. Admissible structures.

Ideas related to factorizability have very recently been used to describe the Galois module structure of ideals in local field extensions. Here is a sample of the results.

Theorem (Vostokov, Bondarko)**.** *Let K be a local field of mixed characteristic with finite residue field. Let L be a finite Galois extension of K with Galois group G.*

(1) *Let I_1 and I_2 be indecomposable $\mathcal{O}_K[G]$-submodules of $\mathcal{O}_L$. Then I_1 is isomorphic to I_2 as $\mathcal{O}_K[G]$-modules if and only if there is an a in K^* such that $I_1 = aI_2$.*
(2) *$\mathcal{O}_L$ contains decomposable ideals if and only if there is a subextension E/L of L/K such that $|L : E|\mathcal{O}_L$ contains the different $\mathcal{D}_{L/E}$.*
(3) *If L is a totally ramified Galois p-extension of K and $\mathcal{O}_L$ contains decomposable ideals, then L/K is cyclic and $|L : K|\mathcal{O}_L$ contains the different $\mathcal{D}_{L/K}$.*

In fact what is remarkable with these results is that they do *not* involve class field theory.

10.2. Galois module theory in geometry

Let X be a smooth projective curve over an algebraically closed field k. Let a finite group G act on X. Put $Y = X/G$.

Theorem (Nakajima 1975)**.** *The covering X/Y is tame if and only if for every line bundle $\mathcal{L}$ of sufficiently large degree which is stable under the G-action $H^0(X,\mathcal{L})$ is a projective $k[G]$-module.*

This is the precise analogue of Ullom's version of Noether's Criterion for the existence of a normal integral basis for ideals in a Galois extension of discrete valuation rings. In fact if (X,G) is a *tame* action of a finite group G on any reasonable proper scheme over a ring A like $\mathbb{Z}$ or $\mathbb{F}_p$, then for any coherent G-sheaf $\mathcal{F}$ on X one can define an equivariant Euler–Poincaré characteristic $\chi(\mathcal{F},G)$ in the Grothendieck group $K_0(A[G])$ of finitely generated *projective* $A[G]$-modules. It is an outstanding problem to compute these equivariant Euler characteristics. One of the most important results in this area is the following. Interestingly it relies heavily on results from class field theory.

Theorem (Pappas 1998)**.** *Let G be an abelian group and let $\mathcal{X}$ be an arithmetic surface over $\mathbb{Z}$ with a free G-action. Then $2\chi(\mathcal{O}_{\mathcal{X}},G) = 0$ in $K_0(\mathbb{Z}[G])/\langle\mathbb{Z}[G]\rangle$.*

10.3. Galois modules and L-functions

Let a finite group G act on a projective, regular scheme X of dimension n defined over the finite field $\mathbb{F}_q$ and let $Y = X/G$. Let $\zeta(X,t)$ be the zeta-function of X. Let e_X be the l-adic Euler characteristic of X. Recall that

$$\zeta(X,t) = \pm(q^n t^2)^{-e_X/2}\zeta(X,q^{-n}t^{-1}), \quad e_X \cdot n = 2\sum_{0\leqslant i\leqslant n}(-1)^i(n-i)\chi(\Omega^i_{X/\mathbb{F}_q})$$

the latter being a consequence of the Hirzebruch–Riemann–Roch theorem and Serre duality. It is well known that the zeta-function of X decomposes into product of L-functions, which also satisfy functional equations. One can describe the constants in these functional equations by "taking isotypic components" in the analogue of the above expression for $e_X \cdot n/2$ in terms of equivariant Euler-Poincaré characteristics. The results that have been obtained so far do *not* use class field theory in any important way. So we are lead to formulate the following problem:

Problem. Using Parshin's adelic approach (sections 1 and 2 of Part II) find another proof of these results.

Let us note that one of the main ingredients in the work on these matters is a formula on ε-factors of T. Saito, which generalizes one by S. Saito inspired by Parshin's results.

10.4. Galois structure of class formations

Let K be a number field and let L be a finite Galois extension of K, with Galois group $G = \mathrm{Gal}(L/K)$. Let S be a finite set of primes including those which ramify in L/K and the archimedean primes. Assume that S is stable under the G-action. Put $\Delta S = \ker(\mathbb{Z}S \to \mathbb{Z})$. Let U_S be the group of S-units of L. Recall that $U_S \otimes \mathbb{Q}$ is isomorphic to $\Delta S \otimes \mathbb{Q}$ as $\mathbb{Q}[G]$-modules. There is a well known exact sequence

$$0 \to U_S \to A \to B \to \Delta S \to 0$$

with finitely generated A, B such that A has finite projective dimension and B is projective. The latter sequence is closely related to the fundamental class in global class field theory and the class $\Omega = (A) - (B)$ in the projective class group $\mathrm{Cl}\,(\mathbb{Z}[G]$ is clearly related to the Galois structure of S-units. There are local analogues of the above sequence, and there are analogous sequences relating (bits) of higher K-theory groups (the idea is to replace the pair $(U_S,\ \Delta S)$ by a pair $(K_i'(\mathcal{O}),\ K_{i-1}'(\mathcal{O}))$).

Problem. Using complexes of G-modules (as in section 11 of part I) can one generalize the local sequences to higher dimensional fields?

For more details see [E].

References

[E] B. Erez, Geometric trends in Galois module theory, Galois Representations in Arithmetic Algebraic Geometry, eds. A. Scholl and R. Taylor, Cambridge Univ. Press 1998, p. 115–145.

[F] A. Fröhlich, L-values at zero and multiplicative Galois module structure (also Galois Gauss sums and additive Galois module structure), J. reine angew. Math. 397 (1989), 42–99.

[Leo] H.-W. Leopoldt, Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers, J. reine angew. Math. 201(1959), 119–149.

[Let] G. Lettl, The ring of integers of an abelian number field, J. reine angew. Math. 404 (1990), 162–170.

[P] G. Pappas, Galois modules and the theorem of the cube, Invent. Math. 133 (1998), no. 1, 193–225.

[S] B. De Smit, Factor equivalence results for integers and units, Enseign. Math. (2) 42 (1996), no. 3-4, 383–394.

[U] S. Ullom, Integral representations afforded by ambiguous ideals in some abelian extensions, J. Number Theory 6 (1974), 32–49.

[VB] S.V. Vostokov and M. V. Bondarko, Isomorphisms of ideals as Galois modules in complete discrete valuation fields with residue field of positive characteristic, preprint, 1999.

Université Bordeaux 1, Institut de Mathématiques
351 Cours de la Libération, 33405 Talence, France
E-mail: erez@math.u-bordeaux.fr