BOOK REVIEWS

BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 34, Number 2, April 1997, Pages 173–176
S 0273-0979(97)00718-0

Multiplicative Galois module structure, by Alfred Weiss, Fields Inst. Monographs, vol. 5, Amer. Math. Soc., Providence, RI, 1996, vii+95 pp., \$39.00, ISBN 0-8218-0265-8

Given an algebraic number field K, the main objects of study are the ring of integers $\mathcal{O}_K$, the class group $Cl(K)$, and the unit group $E(K) = \mathcal{O}_K^*$. All these arithmetical objects are classical. Instances of both $Cl(K)$ and $E(K)$ played prominent roles in Kummer's groundbreaking progress on Fermat's Last Theorem. Kummer took K to be the p-th cyclotomic field $\mathbb{Q}(\zeta_p)$ with $\zeta_p = \exp(2\pi i/p)$ and p (an odd prime) the exponent in the Fermat equation, and he proceeded to prove that FLT holds for the exponent p if the class number $h(K)$ (i.e. the order of $Cl(K)$) is prime to p. The prime p is called *regular* in this case. Here already one can profitably use Galois module structure. Let G be the Galois group (that is, the group of automorphisms) of K over $\mathbb{Q}$. It is easy to describe G: in fact $G = \{\sigma_1, \dots, \sigma_{p-1}\}$ where σ_i is characterized by $\sigma_i(\zeta_p) = \zeta_p^i$. All the arithmetical objects attached to K which we have seen so far are acted on by G, so K, $\mathcal{O}_K$, $Cl(K)$, and $E(K)$ are $\mathbb{Z}[G]$-modules, the first two being written additively, and the other two multiplicatively. Consider now D, the p-primary part of the finite abelian group $Cl(K)$. Kummer's regularity condition we just mentioned says that D is zero. Now D is a module over $R = (\mathbb{Z}/(p^N))[G]$ for N appropriately large, and the ring R can be shown to admit $p-1$ orthogonal idempotents $e_0, \dots, e_{p-2}$ which sum to 1. Accordingly, D is the direct sum of $e_0D, \dots, e_{p-2}D$, and one has the following result (due to Brückner, Iwasawa, and Skula independently, using previous work of Eichler):

if $e_iD \neq 0$ for at most $\sqrt{p} - 2$ indices i, then the first case of FLT holds for p.

(Remark: In actual fact, for every p less than four million, $e_iD \neq 0$ happens for at most seven indices i.) The condition $e_iD \neq 0$, which can be called "representation-theoretic", happens to have a simple arithmetic interpretation for odd $i \neq 1$ (but the proof is highly non-trivial): $e_iD \neq 0$ iff p divides the numerator of the Bernoulli number B_{p-i}. The easier direction (only if) is due to Herbrand, and the other to Ribet. The proof uses L-functions and modular forms among other things.

Kummer also had to consider units, and a certain subgroup C of $E(K)$, the so-called cyclotomic units, as well. He proved that the index of C in $E(K)$ equals the class number of K^+, the maximal real subfield of K. Again, the ring R and its decomposition can be used to obtain a more precise conjecture, a special case of

1991 *Mathematics Subject Classification.* Primary 11R33; Secondary 11R23, 11R34, 11R37, 11R42, 11S25, 11S31, 16H05, 19A31, 20C10, 20J06.

the Gras conjecture, proved in this case and more generally by Mazur, Wiles, and Greenberg. It relates the R-module structure of the p-primary parts of the groups $Cl(K^+)$ and $E(K)/C$.

The subject of "multiplicative Galois module structure" is, therefore, the study of class groups, unit groups, and related entities, as modules over suitable group rings of Galois groups. One always starts with a G-Galois extension K/F of number fields, with $F = \mathbb{Q}$ being an important special case. It would probably be too ambitious a goal if one aimed for a precise description of the isomorphism class of $E(K)$ and $Cl(K)$ over $\mathbb{Z}[G]$ in full generality. We hope to explain what one could reasonably ask, and which results one may expect.

Setting aside class groups for the moment, let us begin with the first general result about $E(K)$. This is Dirichlet's theorem, and in its original form no Galois group intervenes at all. The theorem states that $E(K)$ modulo its torsion subgroup μ (the group of all roots of unity in K) is $\mathbb{Z}$-free of rank $r = r_1 + r_2 - 1$, with r_1 (resp. r_2) being the number of real embeddings (resp. half the number of complex embeddings) of the field K. If K is G-Galois over $\mathbb{Q}$, then either all embeddings are real and $r = [K : \mathbb{Q}]-1$, or all embeddings are complex and $r = [K : \mathbb{Q}]/2-1$. In the former case there is a "natural" $\mathbb{Z}[G]$-module of rank r, to wit, the augmentation ideal $I(G)$, generated by all $\sigma - 1$, $\sigma \in G$. It would be unreasonable to expect $E(K)/\mu$ to be isomorphic to $I(G)$ in general, but Artin and Herbrand proved (in this situation) that $E(K)$ always contains a *submodule of finite index* isomorphic to $I(G)$. (In more learned terms: $\mathbb{Q} \otimes_{\mathbb{Z}} E(K) \cong \mathbb{Q} \otimes_{\mathbb{Z}} I(G)$.) In the case where all embeddings are complex, or when F is not $\mathbb{Q}$, $I(G)$ may be suitably replaced, as we shall explain shortly.

One of the goals of the theory is to understand as well as possible the $\mathbb{Z}[G]$-structure of $E(K)$ and of $Cl(K)$. It became apparent early on that one also has to consider certain enlargements $E_S(K)$ which are called S-unit groups; $E_S(K)$ is the group of all $x \in K^*$ which are locally a unit at all v *not in* S. Here S is always supposed to be a finite set of places of K containing S_∞, the set of archimedean (= infinite) places. There are also S-class groups $Cl_S(K)$; if one chooses the set of places S sufficiently large, $Cl_S(K)$ will be trivial, and $E_S(K)$ incorporates in a certain way both $E(K)$ and $Cl(K)$. Most of the theory deals with $E_S(K)$ with certain "largeness" conditions imposed on S which we shall not attempt to explain. Similarly as above, one always has a standard module ΔS, the kernel of the augmentation map $\mathbb{Z}S \to \mathbb{Z}$ which sends $\sum_{s\in S} z_s s$ to $\sum_{s\in S} z_s$, and this module satisfies $\mathbb{Q}\otimes_{\mathbb{Z}} \Delta S \cong \mathbb{Q}\otimes_{\mathbb{Z}} E_S(K)$. For $S = S_\infty$ and $F = \mathbb{Q}$ one recovers $\Delta S = I(G)$.

Before turning to Alfred Weiss' book, let us try to give some further background information on the subject. First of all, there is also the *additive* theory founded by Fröhlich. One of the most prominent results in that theory (and perhaps in algebraic number theory) is Taylor's proof of Fröhlich's conjecture. This essentially describes for tamely ramified extensions K/F the $\mathbb{Z}[G]$-module structure of $\mathcal{O}_K$ in terms of data (root numbers) which come from Artin L-functions. In a certain way, the multiplicative theory is an outgrowth of the additive theory, and there is a lot of interaction between the two.

The theory of L-functions (Dirichlet, Artin) is always in the background. This is perhaps already clear from the historical origins: the Bernoulli numbers mentioned above are linked with special values of Dirichlet L-series, and so are logarithms of cyclotomic units. The latter phenomenon led to the Stark conjectures, a topic also treated in the book under review.

Next we observe that unit groups have local counterparts. For any G-Galois extension K/F *of a p-adic field F,* one can look at the $\mathbb{Z}[G]$-modules K^* and $U(K)$ (local units). The local situation is certainly simpler than the global one. However it is by no means trivial, and there are beautiful results by Borevič, Jannsen, Wingberg, and others. (Perhaps these might have been mentioned in the book under review.) Without entering into the details, let us just say that these results are obtained using a fair amount of homological algebra. In the case $\zeta_p \notin K$, one obtains for example that K^* becomes on p-completion isomorphic to a first syzygy (kernel of a projective resolution) of $I_p(G)$, the augmentation ideal of $\mathbb{Z}_p[G]$.

This brings cohomology into play. Class field theory permits (at least) an analytic approach (L-functions) and a cohomological approach. It comes as no surprise that class field theory also enters the stage. In formulating the multiplicative Chinburg conjecture (which we shall not do here) it is crucial to use the full cohomological machinery of class field theory. This conjecture of Chinburg does not exactly predict the isomorphism class of $E_S(K)$; it makes predictions about certain projective $\mathbb{Z}[G]$-modules associated to it.

As the reader can see, we are talking about a subject with deep roots in classical algebraic number theory. It has many ramifications, and it is partly very technical. There are some very general conjectures (notably of Stark, and of Chinburg, with numerous variations, and they are, again, rather technical to formulate). Then there are some nice results, and a lot of room for future results. Let us just discuss two questions:

1) If one identifies two $\mathbb{Z}[G]$-modules M and N if their p-completions are isomorphic for all prime numbers p ("M and N in the same genus"), does this "unfocussing" allow us to describe $E_S(K)$?

The answer is essentially yes, and this is well explained in the book. One of the invariants used to describe $E_S(K)$ is, however, complicated and probably very hard to get at.

2) (This is intentionally a bit vague.) The identification process in 1) is almost the same as disregarding arbitrary projective direct summands (considering M and N up to "homotopy"). On the other hand, Chinburg's conjecture makes predictions about certain projective modules which come with $E_S(K)$. Thus, given that the answer in 1) is yes, can we say more if we *assume* Chinburg's conjecture to be true?

The answer is: yes, sometimes. If $F = \mathbb{Q}$, G is cyclic of odd order, and Chinburg's conjecture holds for K/F, then if S satisfies a certain technical condition, E_S is $\mathbb{Z}[G]$-isomorphic to $\Delta S \oplus \mu$. (We recall that μ is the group of roots of unity in K, and ΔS was explicitly defined above.) This is in a certain sense the strongest conceivable result.

There is a variety of other results in the book under review, but let us rather try now to describe the book as a whole. The subject is a fairly young one, and the author does a very nice job of explaining the main problems, conjectures, and methods. A reasonable amount of background material (homological algebra, $\mathbb{Z}[G]$-modules, class field theory) is also presented briefly or sketched. Highlights include: the Gruenberg-Weiss theory of envelopes, the multiplicative Chinburg conjecture, Stark's conjecture, and Tate's proof of the latter for $\mathbb{Q}$-valued characters. At the end, the author presents a very instructive example: $K = \mathbb{Q}(\zeta_p)$, which takes us back to the beginning of this review.

Let me say a few words about the presentation. This book was not written with a general audience in mind. It retains to some extent the lively but terse style of the lectures from which it originated, and these lectures were aimed mainly at specialists. Thus one needs a fair amount of prerequisites and experience to read the book. Conscientious reading entails going back and forth incessantly because of the many cross-references. For example, references and comments on the literature are all in the last chapter. Many of the hints and allusions in the first chapter are somewhat hard to follow unless one knows the book already. I also feel that perhaps the proof of the very important Theorem 3 should not have been omitted.

After these minor comments it should be stressed that no comparable work exists in the literature, and that we should be thankful to have this book, which is at the same time an introduction, and a report on the state of the art, written by one of the leading experts. (The recent proof of the so-called Strong Stark Conjecture for $K/\mathbb{Q}$ abelian, by J. Ritter and A. Weiss himself, came too late to be included in the book.) Even non-experts with some background in algebra should be able to profit from browsing in this book, which will be a standard reference for a long time to come.

Cornelius Greither
Université Laval and CICMA
E-mail address: greither@mat.ulaval.ca