Astérisque

OLAF NEUMANN

On maximal p-extensions, class numbers and unit signatures

Astérisque, tome 41-42 (1977), p. 239-246

<http://www.numdam.org/item?id=AST_1977__41-42__239_0>

Société Mathématique de France
Astérisque 41-42 (1977) p.239-246

ON MAXIMAL p-EXTENSIONS, CLASS NUMBERS AND UNIT SIGNATURES

by

Olaf NEUMANN

The main subjects of the present note are assertions on class numbers and unit groups in certain number fields. The classical example is the well-known

Theorem of H. Weber. The subfields of the 2^m-th cyclotomic field $\mathbb{Q}(\zeta_{2^m})$ have odd class numbers and the totally real subfields of $\mathbb{Q}(\zeta_{2^m})$ have units of arbitrarily given signatures.

This theorem was generalized to other types of absolutely abelian fields by H. Hasse [4]. Following the approach given by A. Fröhlich [2] and K. Iwasawa [5b], we are treating questions about class numbers and unit groups by embedding finite number fields in suitable (possibly infinite) extensions with prescribed ramification points. Many results which can be proved in this way are contained in H. Koch's monograph [6a], chap. 12.

In §1 of the present note we formulate a proposition on p-extensions with a fully ramified prime divisor. Applying this proposition in §2 to 2-extensions, we get further generalizations of H. Weber's theorem. In §3 we are led to an interesting statement on the 2-extensions of $\mathbb{Q}$. In more detail, we can formulate the

following

Theorem. Let $L/\mathbb{Q}$ be the maximal 2-extension of $\mathbb{Q}$ and $K/\mathbb{Q}$ the unique $\mathbb{Z}_2$-extension of $\mathbb{Q}$. Then we can attach to each discrete prime $\underline{\underline{p}}$ of K resp. to the real prime $\underline{\underline{r}}$ of $\mathbb{Q}$ a subgroup $T_{\underline{\underline{p}}}$ resp. $T_{\underline{\underline{r}}}$ of $\mathrm{Gal}(L/K)$ such that the canonical morphism of the free pro-2-product $T_{\underline{\underline{r}}} * (\overset{*}{\underline{\underline{p}}}\, T_{\underline{\underline{p}}})$ into $\mathrm{Gal}(L/K)$ is an isomorphism.

The proof rests essentially on the theorem of H. Weber. Our theorem extends a result of J. Neukirch [9] on p-extensions of $\mathbb{Q}$ $(p \neq 2)$ to the case $p = 2$.

Full proofs of all assertions will be published elsewhere. In conclusion I would like to thank the organizers of the "Journées Arithmétiques" for including this paper into the present proceedings.

§1. On p-extensions with a totally ramified prime divisor.

If p is a fixed rational prime then the notion "p-extension" will be used in the sense of "(possibly infinite) normal extension of p-power degree". The symbol ζ_n stands for any primitive n-th root of unity.

1.1 Proposition. Let k be a finite number field, p a fixed rational prime, K/k a p-extension and $\underline{\underline{p}}$ a prime divisor of k which is totally ramified in K/k. Suppose that H/K is a finite p-extension such that all divisors in K lying over $\underline{\underline{p}}$ are unramified. Then the following statements hold :

a) $(H : K) > 1$ if and only if there exists an abelian p-extension L/K with the properties

(I) $(L : k) > 1$;

(II) $L.K \subseteq H$, $L \cap K = k$;

(III) $\underline{\underline{p}}$ is unramified in L/K .

b) Let H/k be normal. Then the Galois group $\mathrm{Gal}(H/K)$, viewed as an $\mathrm{Gal}(H/k)$-operator group, admits at least d generators if and only if there exist d independent cyclic extensions, $L_1/k,\ldots,L_d/k$, of degree p with the properties (I), (II), (III) of statement a).

1.2 Corollary. Suppose that K/k is a finite p-extension with exactly one ramified divisor $\mathfrak{q}$. We assume that $\mathfrak{q}$ is totally ramified in K/k. Then for the class numbers h_k resp. h_K of k resp. K holds : $p|h_K \iff p|h_k$.

For the proof one puts H = the Hilbert p-class field of K and applies proposition 1.1 a) to the extension H/k. The special case $k = \mathbb{Q}(\zeta_p)$, $K = \mathbb{Q}(\zeta_{p^n})$ is just a well-known theorem of K. Iwasawa ([5b], cf. [6a], chap. 12, example 12.5).

1.3 Corollary ([7], Satz 5). Let $K/\mathbb{Q}$ be a cyclic extension of degree p. Then the class number h_K is prime to p if and only if $K/\mathbb{Q}$ has a prime discriminant.

§2. On finite 2-extensions.

For any field F, denote by h_F^+ the class number of F in the narrow sense whereas the usual class number is denoted by h_F.

An immediate consequence of proposition 1.1 is

2.1 Proposition. Let k be a finite number field with odd class number h_k^+. Suppose that K/k is a 2-extension the ramification points of which are at most the real primes and one discrete prime $\mathfrak{p}$. Then $\mathfrak{p}$ is totally ramified in K/k and h_K^+ is odd. The field K has units of arbitrarily given signatures.

This proposition can be applied to some interesting examples and includes the announced generalizations of Weber's theorem.

2.2 First example. $k = \mathbb{Q}$. Let p be a rational prime and $K/\mathbb{Q}$ a 2-extension unramified outside of $\{\infty,p\}$. Possible cases :

a) $p \neq 2$: $K/\mathbb{Q}$ cyclic, $K \subseteq \mathbb{Q}(\zeta_p)$, $p \equiv 1\ (2^m)$;

b) $p = 2$: $K = \mathbb{Q}(\zeta_{2^m})$ or $\mathrm{Gal}(K/\mathbb{Q})$ non-abelian with two generators.

The abelian cases of this example were just treated by H. Hasse [4].

2.3 Second example. $k = \mathbb{Q}(\sqrt{p})$, p a rational prime with $p \equiv 5$ (8). Gauss' theorem on the genera asserts that h_k^+ is odd.

2.4 Third example. Suppose that $k_1 = \mathbb{Q}(\sqrt{d})$ is a real quadratic field with exactly two discriminant divisors and Norm $\varepsilon_0 = -1$ (ε_0 a basic unit). Put k = the 2-class field of k_1 . One can prove that h_k^+ is odd. A series of suitable fields k_1 is given by $k_1 = \mathbb{Q}(\sqrt{2p})$, p a prime with $p \equiv 5$ (8). Here we have $k = \mathbb{Q}(\sqrt{2p},\sqrt{2}) = \mathbb{Q}(\sqrt{p},\sqrt{2})$ (cf. [6c], p. 332).

§3. On some classes of infinite 2-extensions. Results and conjectures.

Let p be a rational prime, k an arbitrary finite number field and S a set of primes of k . By k_S/k we denote the maximal p-extension unramified outside S . The information about the Galois groups $\mathrm{Gal}(k_S/k)$ is quite satisfactory (mostly, on their cohomology) at least in three cases : 1) $p \neq 2$, S contains all divisors of p ; 2) $p = 2$, k has real primes, S contains all divisors of (2) and all real primes ; 3) $p = 2$, k is totally imaginary, S contains all divisors of (2). We suppose that it is possible to reformulate a great part of the known result results for $p \neq 2$ in the case $p = 2$ even if we exclude from S all real primes of k . This is supported by some results which can be deduced, for instance, from §2.

Suppose that S is a set of primes containing all divisors of (2), but no real primes. We put $G_S = \mathrm{Gal}(k_S/k)$. Then G_S is an infinite group since k_S contains the unique $\mathbb{Z}_2$-extension of $\mathbb{Q}$ (the union of all totally real subfields of $\mathbb{Q}(\zeta_{2^m})$, $m \geq 3$).

3.1 Conjecture. The cohomological dimension of G_S is not greater than 2. If S is finite, then G_S has the Euler-Poincaré-characteristic $\chi(G_S) = -r_2$ (r_2 = number of complex places of k).

3.1' Conjecture. The strict cohomological dimension of G_S is not greater than 2.

3.2 Conjecture. Let $\bar{k}_S/k$ be the maximal extension unramified outside S. Then for any finite $\mathrm{Gal}(\bar{k}_S/k)$-module A of exponent 2 the statements of Tate's global duality theorem ([14], [11]) hold.

Conjecture 3.2 makes sense because the dual module of A gets also the structure of a $\mathrm{Gal}(\bar{k}_S/k)$-module.

3.3 Conjecture. Let L/k be any 2-closed extension unramified outside S. Then for any finite 2-primary G_S-module A the inclusion $k_S \hookrightarrow L$ induces isomorphisms

$$H^i(G_S, A) \xrightarrow{\sim} H^i(\mathrm{Gal}(L/k), A) \qquad (i \geq 0)$$

by inflation.

The results of G.N. Markšaitis [8] suggest the following.

3.4 Question. Let S_∞ be the set of real primes of k, $S' = S \cup S_\infty$. To each $\mathfrak{p} \in S_\infty$ we attach the decomposition group, $D_{\mathfrak{p}}$, of some fixed prolongation of $\mathfrak{p}$ to $k_{S'}$. From $\sqrt{-1} \in k_{S'}$ we conclude $D_{\mathfrak{p}} \cong \mathbb{Z}/2\mathbb{Z}$. Does the Galois group $G_{S'} = \mathrm{Gal}(k_{S'}/k)$ admit a free decomposition of the type

$$G_{S'} = H_S * \left(*_{\mathfrak{p} \in S_\infty} \sigma_{\mathfrak{p}} D_{\mathfrak{p}} \sigma_{\mathfrak{p}}^{-1}\right)$$

with suitable elements $\sigma_{\mathfrak{p}} \in G_{S'}$ and a suitable subgroup H_S if S

is sufficiently large ?

3.5 Theorem. Conjecture 3.1 is true if $k = \mathbb{Q}$ or if S contains all but a finite number of primes of k .

The proof rests upon the properties of the Brauer group. In the case $k = \mathbb{Q}$ one needs the theorem of H. Weber.

From Kuroš' subgroup theorem we can deduce the following.

3.6 Proposition. If the answer to question 3.4 is "yes" for some pair (k,S) and if k_1/k is a finite extension with $k_1 = k_S$, then the same is true for the pair (k_1, S_1) where S_1 denotes the set of primes of k_1 lying over S .

Particularly, we get a restatement of Markšaitis' results (s. [8], the formulation of his "theorem 2" was not correct).

3.7 Theorem. Let $L/\mathbb{Q}$ be the maximal 2-extension unramified outside $\{2,\infty\}$. Let $L/\mathbb{Q}$ be a finite extension inside L . Then $\mathrm{Gal}(L/k)$ is isomorphic to the free product of a free pro-2-group F of rank r_2+1 and r_1 copies of the group $\mathbb{Z}/2\mathbb{Z}$ (r_1 = number of real places of k , r_2 = number of complex places of k).

3.8 Proposition. Suppose that k is a finite number field satisfying the following conditions :

a) h_k^+ is odd ; b) over (2) lies exactly one prime divisor $\underline{\mathfrak{d}}$ in k . Then the maximal 2-extension K/k unramified outside $\{\underline{\mathfrak{d}}\}$ has a free pro-2-group of rank r_2+1 (r_2 = number of complex places of k).

In his paper ([9], Satz 11.3) J. Neukirch proves a theorem on the connection between local and global Galois groups which concerns p-extensions of $\mathbb{Q}$ for $p \neq 2$. This theorem can be extended to $p = 2$ by means of our proposition 2.1.

3.9 Theorem. Let k be a totally real number field satisfying the assumptions of proposition 3.8 and let K/k be the unique $\mathbb{Z}_2$-extension. By L/k we denote the maximal totally real 2-extension. To any discrete prime $\underline{\underline{P}}$ of K we attach the inertia group $T_{\underline{\underline{P}}}$ of some fixed prolongation of $\underline{\underline{P}}$ to L . Then we have the following statements :

a) for all $\underline{\underline{P}}$ one has $T_{\underline{\underline{P}}} \cong \mathbb{Z}_2$;

b) the free pro-2-product $\overset{*}{\underline{\underline{P}}} T_{\underline{\underline{P}}}$ is canonically isomorphic to Gal(L/K).

This theorem can be generalized by including all real primes of k . In any case, the proof of theorem 3.9 requires essentially the proposition 2.1.

-:-:-:-

BIBLIOGRAPHY

[1] J.V. ARMITAGE and A. FRÖHLICH.- Class numbers and unit signatures. Mathematika 14 (1967), 94-98.

[2] A. FRÖHLICH.- a) On the absolute class group of abelian fields. (I) J. London Math. Soc. 29 (1954), 211-217 ; (II) ibidem 30 (1955), 72-80.
b) A remark on the class number of abelian fields. J. London Math. Soc. 29 (1954), p. 498.

[3] K. HABERLAND.- Der Tatesche Dualitätzzatz aus der Galois-Cohomologie über Zahlkörpern. Dissertation Berlin 1975.

[4] H. HASSE.- Über die Klassenzahl abelscher Zahlkörper. Berlin 1952.

[5] K. IWASAWA.- a) On $\mathbb{Z}_\ell$-extensions of algebraic number fields. Annals of Math. 98 : 2 (1973), 246-326.
b) A note on class numbers of algebraic number fields. Abh. Math. Sem. Univ. Hamburg 20 (1956), 257-258.
c) A note on the group of units of an algebraic number field. J. Math. pures et appl. 35 (1956), 189-192.

[6] H. KOCH.- a) Galoissche Theorie der p-Erweiterungen. Berlin 1970 (Russian translation Moscow 1973).
b) On fields of class two and Galois cohomology. To appear in : Proceed. Durham Sympos. Number Theory 1975.
c) Und Zink W., Über die 2-Komponente der Klassengruppe quadratischer Zahlkörper mit zwei Diskriminantenteilern. Math. Nachr. 54 (1972), 309-333.

[7] H.W. LEOPOLDT.- Zur Geschlechtertheorie in abelschen Zahlkörper Math. Nachrichten 9 (1953), 351-362.

[8] G.N. MARKŠAITIS.- On p-extensions with a single critical prime (Russ.). Izvest. AN SSSR, ser. mat. 27 : 2 (1963), 463-466.

[9] J. NEUKIRCH.- Einbettungsprobleme mit lokaler Vorgabe und freie Produkte lokaler Galoisgruppen. J. reine u. angew. Math. 259 (1973), 1-47.

[10] O. NEUMANN.- a) On p-closed algebraic number fields with restricted ramification (Russ.). Izvest. AN SSSR, ser. mat. 39 : 2 (1975), 259-271.
b) On p-closed number fields and an analog of Riemann's existence theorem. To appear in : Proceed. Durham Sympos. Number Theory 1975.

[11] G. POITOU.- Cohomologie Galoisienne des modules finis. Paris Dunod (1967).

[12] I.R. ŠAFAREVIČ.- Extensions with given ramification points (Russ.). Publ. Math. I.H.E.S. n° 18 (1964).

[13] J.-P. SERRE.- Cohomologie Galoisienne. Lecture Notes in Mathem. 5, Berlin-Heidelberg-New York (1964).

[14] J. TATE.- Duality theorems in Galois cohomology. Proceed. Intern. Congr. Math. Stockholm 1962, pp. 288-295.

Olaf NEUMANN
Akademie der Wissenschaften der DDR
Zentralinstitut für Mathematik und Mechanik
DDR - 108 BERLIN, Mohrenstrasse 39