数理解析研究所講究録
第 884 巻 1994 年 94-101

On positively ramified extensions of algebraic number fields

BY KAY WINGBERG

By a famous theorem of Grothendieck the structure of the étale fundamental group of a smooth projective curve of genus g over an algebraically closed field k is known for the part prime to the characteristic of k. Precisely there are $2g$ generators with one defining relation

$$\prod_{i=1}^{g} [x_i, y_i] = 1 .$$

The purpose of this note is to introduce an arithmetical site for number fields whose corresponding fundamental group has an analog structure as in the function field case. This approach is due to A. Schmidt [1], [2] generalizing some ideas of the author [4], [5].

1. Algebraic number fields of CM-Type

The starting point for establishing an analogue in the number field case was to define a natural extension $\tilde{K}$ of a number field K of CM-type containing the group μ_p of p-th roots of unity where p is an odd prime number. In order to immediate a geometric situation one considers the cyclotomic $\mathbb{Z}_p$-extension K_∞ of K as a ground field. Since the p-part of the étale fundamental group of K_∞, i.e. the Galois group the maximal unramified p-extension of K_∞, is too small for being an analogue and the Galois group of the maximal p-extension $K_{S_p}(p)$ of K_∞ unramified outside the set S_p of primes of K above p is much too big (not even finitely generated), one looks for something in between. The idea is to restrict the ramification at p using the primes at infinity. In some sence one compactifizes the affine scheme $\mathrm{Spec}(O_K)$. For this approach the following assumptions were needed in the paper [4]:

Let p be an odd prime number,

K is a CM-field containing μ_p,
K^+ is the maximal totally real subfield of K, i.e. $K = K^+(\mu_p)$,
K_∞ is the cyclotomic $\mathbb{Z}_p$-extension of K.

We assume

(i) No prime of K^+ above p splits in K.

(ii) The Iwasawa μ-invariant of K_∞/K is zero.

Theorem 1.1, [4]: *Under the assumptions and notations given above there exists a natural p-extension $\tilde{K}$ of K unramified outside p such that the Galois group $Gal(\tilde{K}/K_\infty)$ is a Poincaré group of dimension 2 and of rank $2g_p$, where g_p is the minus part λ^- of the Iwasawa λ-invariant of K_∞/K. More precisely, there are generators $x_i, y_i, i = 1, \ldots, g_p$, of $Gal(\tilde{K}/K_\infty)$ with one defining relation*

$$\prod_{i=1}^{g_p} [x_i, y_i] = 1 .$$

Corollary 1.2: *The Galois group $Gal(\tilde{K}/K)$ is isomorphic to $\mathbb{Z}_p$ or a Poincaré group of dimension 3.*

The definition of $\tilde{K}$ is as follows. Let $K(p)$ and $K^+(p)$ be the maximal p-extension of K and K^+, respectively. Let $I_v(K(p)/K)$ be the inertia group of $\mathrm{Gal}(K(p)/K)$ with respect to a prime v. Then for a finite set S of primes of K containing S_p we define

$$N_S := (I_v(K(p)/K^+(p)K)v \in S_p;\ \ I_v(K(p)/K),\ \ v \notin S) ,$$

i.e. the normal subgroup of $G(K(p)/K)$ generated by all inertia groups for the primes not in S and the "minus-parts" of the inertia groups for the primes above p. Now

$$\mathrm{Gal}(\tilde{K}/K) := \mathrm{Gal}(K(p)/K)/N_{S_p}$$

and more generally

$$\mathrm{Gal}(\tilde{K}_S/K) := \mathrm{Gal}(K(p)/K)/N_S \quad \text{for} \quad S \geq S_p .$$

Using an analogue of Riemann's existence theorem proved by J. Neukirch and more general by O. Neumann one can show

Theorem 1.3, [4]: *With the assumptions and notations given above let $S \supsetneqq S_p$ be a finite set of primes of K. Then $\mathrm{Gal}(\tilde{K}_S/K_\infty)$ is a free pro-p-group of rank $2g_p + \#S\backslash S_p(K_\infty) - 1$ and there exist generators $x_i, y_i, i = 1, \ldots, g_p$, and $u_v \in I_v(K(p)/K)$, $v \in S\backslash S_p(K_\infty)$ with one relation*

$$\prod_{i=1}^{g_p} [x_i, y_i] \prod_{v \in S\backslash S_p(K_\infty)} u_v = 1 .$$

2. Generalization to admissible number fields and primes

The following approach, due to A. Schmidt, is a part of the content of the paper [1]. This generalization of the situation described in §1 has the disadvantage to that given in §3 that again one needs a CM-field on the bottom and it is not possible to handle all prime numbers. So let

K be a CM-field with maximal totally real subfield K^+ and let
$P^{ns}(K) = \{\text{primes } p \neq 2 \mid \text{primes of } K^+ \text{ above } p \text{ do not split in } K\}$.

Let $F(\text{odd})$ be the maximal Galois extension of a local or global field F of odd degree.

Definition 2.1:

(i) *A number field $L \subseteq K(odd)$ is called* *<u>admissible</u>* *at $p \in P^{ns}(K)$ if $L_\mathfrak{p} \subseteq K_\mathfrak{p}^+(\text{odd})K_\mathfrak{p}$ for all primes $\mathfrak{p}$ of L above p. Furthermore let $P^{ns}(L) := \{p \in P^{ns}(K) \mid L/K$ admissible at $p\}$.*

(ii) *Let L/K be* *<u>admissible</u>* *at $p \in P^{ns}(K)$. Then an extension M of L inside $K(odd)$ is called* positively ramified (p.r.) at $p \in P^{ns}(L)$ *if*

1. *M/L has no tamely ramified part for all $\mathfrak{p}|p$, i.e. the ramification index $e_\mathfrak{p}$ is a power of p.*
2. *$M_\mathfrak{p} \subseteq L_\mathfrak{p}^+(\text{odd})L_\mathfrak{p}$ for all $\mathfrak{p}|p$.*

Of course, in the definition given above the field L need not to be of CM-type but it is in some sense "locally of CM-type at p" and the existence of the field $L_\mathfrak{p}^+$ occuring in (2.1)(ii) is given by the following lemma.

Lemma 2.2: *Let $L \subseteq K(\text{odd})$ be admissible at $p \in P^{ns}(K)$. Then*

(i) For every prime $\mathfrak{p}|p$ of L there exists exactly one field $L_\mathfrak{p} \supseteq K_\mathfrak{p}^+ \supseteq K_\mathfrak{p}^+$ such that $[L_\mathfrak{p} : L_\mathfrak{p}^+] = 2$ and the generator $\rho_\mathfrak{p}$ of $Gal(L_\mathfrak{p}/L_\mathfrak{p}^+) \cong \mathbb{Z}/2$ is induced by the complex conjugation w.r.t. an embedding $L \hookrightarrow \mathbb{C}$.

(ii) Conversely, to every embedding L in $\mathbb{C}$ there exists a prime $\mathfrak{p}$ above p such that $\rho_\mathfrak{p}$ is induced by the complex conjugation.

Remark 2.3.: *The set $P^{ns}(L)$ in (2.1)(i) has positive density (bigger or equal to $1/[\hat{L} : \mathbb{Q}]$, $\hat{L}$ the Galois closure of $L/\mathbb{Q}$).*

Now, for $L \subseteq K(\text{odd})$ and $p \in P^{ns}(L)$ let

$L^{\text{pos},p}$ be the maximal extension of L which is positively ramified at p and
$\tilde{L}^p = L^{\text{pos},p} \cap L_{S_p}(p)$ is the maximal p-extension of L which is unramified outside p and positively ramified at p.

The field $L^{\text{pos},p}$ exists since one can easily see that the compositum of extensions which are p.r at p is again p.r. at p. Obviously $\tilde{L}^p$ contains the cyclotomic $\mathbb{Z}_p$-extension $L_{\infty,p}$ of L.

Theorem 2.4, [1]: *Let $L \subseteq K(odd)$ and $p \in P^{ns}(L)$. Assume that the Iwasawa μ-invariant of $L_{\infty,p}/L$ is zero.*

(i) If $\mu_p \subset L$, then $G(\tilde{L}^p/L_{\infty,p}) = \langle x_i, y_i,\ i = 1, \ldots, g_p \mid \prod_{i=1}^{g_p} [x_i, y_i] = 1 \rangle$.

(ii) If $\mu_p \not\subset L$, then $G(\tilde{L}^p/L_{\infty,p})$ is a free pro-p-group of finite rank.

The non-negative number g_p is called the *p-genus of L* ($g_p = \lambda_p^-$ if L is a CM-field). It would be interesting to know whether the numbers g_p for fixed field L are bounded independently of p as this is the case for function fields.

3. An arithmetic site

In this paragraph we are trying to give a survey of the paper [2]. We start with a new definition of admissibility, now for local number fields. Let K_p be the maximal unramified extension of the local field

$$\mathbb{Q}_p(\zeta_p + \zeta_p^{-1}) \quad \text{where} \quad \zeta_p \quad \text{is a primitive } p\text{-th root of unity.}$$

Definition 3.1:

(i) Let p be an odd prime number. Then a $\mathfrak{p}$-adic number field $k_{\mathfrak{p}}$ over $\mathbb{Q}_p$ is called admissible, if $k_{\mathfrak{p}} \subseteq K_p(\mathrm{odd})(\zeta_p)$.

(ii) Every 2-adic number field is admissible.

We remark that every abelian extension of $\mathbb{Q}_p$ is admissible. Since there is still no reasonable idea of defining admissiblity in the case $p = 2$ we put no restriction for 2-adic number fields.

Definition 3.2: *An extension $L|K$ of number fields is called positively ramified (p.r.) at a prime $\mathfrak{P}|\mathfrak{p}$ if there exists an admissible local field k such that $L_{\mathfrak{P}} = K_{\mathfrak{p}}k$ and the normal closure $\hat{k}$ of the extension $k/k \cap k_{\mathfrak{p}}$ has no tame ramification*

$$\begin{tikzcd}
\hat{k} \arrow[d, dash] & \\
k \arrow[d, dash] \arrow[r, dash] & L_{\mathfrak{P}} = K_{\mathfrak{p}}k \arrow[d, dash] \\
k \cap K_{\mathfrak{p}} \arrow[r, dash] & K_{\mathfrak{p}}
\end{tikzcd}$$

In the case that $L_{\mathfrak{P}}$ itself is admissible (3.2) means that $\hat{L}_{\mathfrak{P}}/K_{\mathfrak{p}}$ has no tame ramification. Furthermore we remark that

the cyclotomic $\hat{\mathbb{Z}}$-extension of a number field,
the maximal p-exension of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ unramified outside p and
unramified extensions

are p.r. everywhere.

Now we are going to define an arithmetic site. The underlying category is denoted by $\mathfrak{C}_0$.

Ob($\mathfrak{C}_0$): finite disjoint unions of spectra Spec($O_{K,S}$) where

K is a (not necessarily finite) global number field with ring of integers O_K and $O_{K,S}$ is the localization of O_K w.r.t. a multiplicatively closed subset S.

Mor($\mathfrak{C}_0$): morphisms of schemes.

If K is a number field and $\mathfrak{p}$ a prime of K then the local field $K_\mathfrak{p}$ and its ring of integers $O_{K_\mathfrak{p}}$ are not in $\mathfrak{C}_0$ but the henselization $(O_K)_\mathfrak{p}$ and its field of fractions. The category $\mathfrak{C}_0$ has fibre products which are the normalizations of the fibre products of schemes.

Definition 3.3:

1) A morphism $\phi : X \to Y$ in $\mathfrak{C}_0$ is p.r. if

(i) ϕ is flat of finite type,

(ii) the field extension $K(X)/K(Y)$ is p.r. at every prime which corresponds to a point of X,

(without loss of generality we assume that X and Y are connected).

2) Let $X \in \mathfrak{C}_0$, then the small site X_{pos} is the category of p.r. morphisms $Y \to X$ with surjective families as coverings.

Thus we defined a Grothendieck topology on $\mathfrak{C}_0$. Now we have to enlarge the category $\mathfrak{C}_0$ to a category $\mathfrak{C}$ by adding "points".

Definition 3.4:

A point is a locally ringed space with a single point as underlying topological space together with a henselian ring A such that $SpecA \in \mathfrak{C}_0$.

Since this note only should give a survey we cannot present all properties of this site in detail and the interested reader is requested to confer the paper [2]. In the following we list some important facts without proof.

Remark 3.5:

1) There exists a morphism of sites $X_{\text{pos}} \to X_{\text{et}}$.

2) For every sheaf F on $X = \text{spec}(R) \in \mathfrak{C}$, R henselian, it holds

   $H^i_{\text{pos}}(X, F) = 0$ for $i \leq 3$, and
   $H^i_{\text{pos}}(X, F) = 0$ for $i \leq 2$ up to 2-torsion, if F is a torsion sheaf.

3) Let $X \in \mathfrak{C}$ and let n be an invertible integer on X. Then for every $F \in \text{Sh}(X_{\text{pos}})$ the canonical homomorphism

$$H^i_{\text{et}}(X, F) \otimes \mathbb{Z}_{(n)} \xrightarrow{\sim} H^i_{\text{pos}}(X, F) \otimes \mathbb{Z}_{(n)}$$

   is an isomorphism for all $i \in \mathbb{Z}$.

4) Let $X \in \mathfrak{C}_0$ and let $Z \subset X$ be a closed subset. For a sheaf F on X_{pos} let

$$\Gamma_Z(X, F) := \ker(\Gamma(X, F) \to \Gamma(X \backslash Z, F)),$$
$$H^i_Z(X, F) := R^i\Gamma_Z(X, \_\,)(F).$$

   Then the relative cohomology sequence exists and the excision theorem is true:

$$H^i_z(X, F) \xrightarrow{\sim} H^i_z(\text{Spec}O^h_{X,z}, F)\ ,$$

   where z is a closed point of X.

5) Let $X = \text{Spec}(R) \in \mathfrak{C}$, R henselian. One can define a sheaf $\hat{\mathbb{G}}_{m,X}$ which plays the role of the multiplicative group for X_{pos}. This sheaf fits in an exact Kummer sequence and up to 2-torsion there exists a local duality theorem with $\hat{\mathbb{G}}_{m,X}$ as dualizing sheaf.

Now we want to present a global duality theorem which is an analogue to Artin/Verdier-duality on the étale site. First we have to define a global sheaf $\hat{\mathbb{G}}_{m,n}$ on $X = \text{Spec}(O_K) \in \mathfrak{C}_0$ which (unfortunately) depends on a natural number $n \in \mathbb{N}$. Let

   K be a finite extension of $\mathbb{Q}$, $X = \text{Spec}(O_K)$,
   $\mathfrak{p}|p$ is a prime of K (for simplicity we assume $p \neq 2$),
   R is the henselization of O_K at $\mathfrak{p}$,
   $k = \text{Quot}(R)/\mathbb{Q}_p$ its field of fractions,
   $k' = k \cap k_p(\text{odd})(\zeta_p)$ is the maximal admissible subfield of k,
   $(k')^+ = k \cap k_p(\text{odd})$.

Then we define

$$U^{\text{pos}}(R) := R \cap (\mu^{(p)} \oplus U^-_{k'})$$

where $\mu^{(p)}$ are the roots of unity of k with order prime to p, $U_{k'}$ is the group of units in $O_{k'}$ and $U^-_{k'} = 0$ if ζ_p is not contained in the maximal unramified extension of k and otherwise $U^-_{k'} = (1 - \rho)U_{k'}$ where $\langle\rho\rangle = \text{Gal}(k'/(k')^+) \cong \mathbb{Z}/2$.

Now let

$$\hat{\mathbb{G}}_{m,n}(X) := \{s \in \mathbb{G}_m(X) \mid s \in U^{\mathrm{pos}}(R) \text{ for every geometric point } \operatorname{Spec}(R) \to X, \text{ whose residue characteristic devides } n\}.$$

Here a geometric point is an object $\operatorname{Spec}(R) \in \mathfrak{C}$ where R is strictly positive, i.e. there is no connected p.r. covering of $\operatorname{Spec}(R)$.

Global duality theorem 3.6: *Let $X = \operatorname{Spec}(O_K)$, K a number field, and let F be a locally constant sheaf of $\mathbb{Z}/n$-modules on X_{pos}. Assume that K is admissible at n. Then the cupproduct*

$$H^i_{\mathrm{pos}}(X,F) \times H^{3-i}_{\mathrm{pos}}(X, \operatorname{Hom}(F, \hat{\mathbb{G}}_{m,n})) \xrightarrow{\cup} H^3_{\mathrm{pos}}(X, \hat{\mathbb{G}}_{m,n}) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z} \otimes \mathbb{Z}_{(n)}$$

defines a pairing of finite abelian groups which is perfect up to 2-torsion.

As an application we consider the fundamental group $\pi_1^{\mathrm{pos}}(X)$ of $X = \operatorname{Spec}(O_K)$ w.r.t. the site X_{pos}. We assume that K is an abelian number field, hence K is admissible everywhere, and let K^+ be the maximal totally real subfield of K. Let p be an odd prime number and suppose that all primes above p ramify in K/K^+. By $C\ell_{S_p}(K)$ we denote that S_p-ideal class group of K, Δ is the Galois group of $K(\mu_p)/K$ and $V_{S_p}(K) = \operatorname{Hom}_\Delta(C\ell_{S_p}(K(\mu_p)), \mu_p)$. Finally let $\pi_1^{\mathrm{pos}}(X)(p)$ be the maximal pro-p factor group of $\pi_1^{\mathrm{pos}}(X)$.

Theorem 3.7: *With the assumptions and notations given above the following is true:*

1) If $K = K^+$, then

$$\pi_1^{\mathrm{pos}}(X)(p) = \begin{cases} \textit{free pro-p group of finite rank, if } V_{S_p}(K) = 0 \\ \textit{duality group of dimension 2. otherwise} \end{cases}$$

2) If $[K : K^+] = 2$, then either $\pi_1^{\mathrm{pos}}(X)(p) \cong \mathbb{Z}_p$ (genus 0-case) or

$$\pi_1^{\mathrm{pos}}(X)(p) = \begin{cases} \textit{Poincaré group of dimension 3, if } \zeta_p \in K \\ \textit{duality group of dimension 2, if } \zeta_p \notin K. \end{cases}$$

For the concept of duality groups see [3]. The assertions of (3.7) are exactly analogue to the function field case. Finally we would like to mention the following corollary: Denoting the normalization of X in the cyclotomic $\mathbb{Z}_p$-extension $K_{\infty,p}$ of K by $X_{\infty,p}$ then we obtain

Corollary 3.8:

i) If $\zeta_p \in K$ the group $\pi_1^{\mathrm{pos}}(X_{\infty,p})(p)$ has $2g_p$ generators x_i, y_i, $i = 1, \ldots, g_p = \lambda_p^-(K)$, with one defining relation

$$\prod_{i=1}^{g_p} [x_i, y_i] = 1 \ .$$

ii) If $\zeta_p \notin K$ the group $\pi_1^{\mathrm{pos}}(X_{\infty,p})(p)$ is a free pro-p group of finite rank.

We remark that the structure of $\pi_1^{\mathrm{pos}}(X_{\infty,p})(p)$ is different to the one given above if the primes of K^+ above p do not ramify in K.

References

[1] A. SCHMIDT: *Positively ramified extensions of algebraic number fields.* To appear.

[2] A. SCHMIDT: *On an arithmetic site.* To appear.

[3] J.-P. VERDIER: *Dualité dans la cohomologie des groupes profinis.* In: J.-P. SERRE. *Cohomologie galoisienne.* Lect. Notes in Math. **5** (1964).

[4] K. WINGBERG: *Ein Analogon zur Fundamentalgruppe einer Riemannschen Fläche im Zahlkörperfall.* Invent. Math. **77** (1984), 557–584.

[5] K. WINGBERG: *Positiv-zerlegte p-Erweiterungen algebraischer Zahlkörper.* J. für reine u. angew. Math. **357** (1985), 193–204.