Available online at www.sciencedirect.com
ScienceDirect
Progress in Natural Science 18 (2008) 323–324
Progress in Natural Science

Short communication

Unramified extensions of quadratic fields

Wei Li *, Dong Yang, Xianke Zhang

Department of Mathematical Sciences, Tsinghua University, Beijing 100084, China

Received 10 January 2007; received in revised form 14 April 2007; accepted 26 November 2007

Abstract

Let K be a global quadratic field, then every unramified abelian extension of K is proved to be absolutely Galois when K is a number field or under some natural conditions when K is a function field. The absolute Galois group is also determined explicitly.

Keywords: Global quadratic fields; Unramified extensions

1. Statement of main theorems

Let K be a quadratic global field. When K is a number field, a finite extension L of K is called unramified if it is unramified at all the primes of K. It is well known that every unramified cyclic cubic extension of K is Galois over $\mathbb{Q}$ with the Galois group isomorphic to S_3, see [3] for example. In this paper, we study general unramified abelian extensions of K. In the number field case, we have the following theorem:

Theorem 1. *Let K be a quadratic number field and L be an unramified abelian extension of K, then L is Galois over $\mathbb{Q}$. Assume that $Gal(K/\mathbb{Q}) = \langle\bar{\sigma}\rangle$, $Gal(L/K) = G_0$, $Gal(L/\mathbb{Q}) = G$ and fix an extension of $\bar{\sigma}$ to G denoted by σ, then G is the semi-direct product of G_0 and $\langle\bar{\sigma}\rangle$ determined by $\sigma^2 = 1$ and $\sigma g \sigma^{-1} = g^{-1}$ for all $g \in G_0$. In particular, when L is cyclic of degree n over K, $Gal(L/\mathbb{Q})$ is isomorphic to the dihedral group D_n.*

When K is a function field with constant field $\mathbb{F}_q$, let $k = \mathbb{F}_q(t)$ be its underlying rational function field and S' a finite set of primes of k. Denote by $d_{S'}$ the greatest common divisor of the elements in $\{\deg P \mid P \in S'\}$. For any finite set S of primes of K, we say a finite extension L of K is unramified with respect to S if it is unramified at all the primes of K and is split completely at S. When S is stable under $Gal(K/k)$, S is the extension of S' in K for some S'. In this case, we also denote d'_S as d_S. Then we have:

Case 1. S is nonempty.

Theorem 2. *Let K be a quadratic function field and S a nonempty finite set of primes of K which is stable under $Gal(K/k)$. If $d_S = 1$, then every abelian extension L of K, which is unramified with respect to S, is Galois over k. Assume furthermore that $Gal(K/k) = \langle\bar{\sigma}\rangle$, $Gal(L/K) = G_0$, $Gal(L/k) = G$ and fix an extension of $\bar{\sigma}$ to G denoted by σ, then G is the semi-direct product of G_0 and $\langle\bar{\sigma}\rangle$ determined by $\sigma^2 = 1$ and $\sigma g \sigma^{-1} = g^{-1}$ for all $g \in G_0$.*

Case 2. S is empty.

Theorem 3. *Notations are the same as above. Denote by J_K the idele group of K and H the subgroup of J_K which contains $K^\times$ corresponding to L, respectively. Let $\alpha \in H$ be an idele whose corresponding divisor has the minimal degree. Then L/k is Galois if and only if $\alpha^{\bar{\sigma}} \in H$. Furthermore, $Gal(L/k)$ is the semi-direct product of G_0 and $\langle\bar{\sigma}\rangle$ determined by $\sigma^2 = 1$ and $\sigma g \sigma^{-1} = g^{-1}$ for all $g \in G_0$.*

* Corresponding author. Tel.: +86 13693564264; fax: +86 10 62785847.
E-mail address: liwei97@mails.tsinghua.edu.cn (W. Li).

1002-0071/$ - see front matter © 2007 National Natural Science Foundation of China and Chinese Academy of Sciences. Published by Elsevier Limited and Science in China Press. All rights reserved.
doi:10.1016/j.pnsc.2007.11.005

2. Proof of the theorems

2.1. Proof of Theorem 1

Proof. Denote by $\mathcal{I}$ and $\mathcal{P}$ the group of fractional ideals and the group of principal ideals of K, respectively. By class field theory (see chapter 7 of [1]), there is a unique subgroup $\mathcal{J}$ of $\mathcal{I}$ containing $\mathcal{P}$ corresponding to L, i.e. L is the class field of $\mathcal{J}$. It is easy to prove that L is absolutely Galois if and only if $\mathcal{J} = \bar{\sigma}\mathcal{J}$ (see Theorem 18.13 of [2]). Note that $\bar{\sigma}\mathcal{I} = \mathcal{I}$ and $\bar{\sigma}\mathcal{P} = \mathcal{P}$, so to prove L is absolutely Galois it suffices to prove that

$$\bar{\sigma}(\mathcal{J}/\mathcal{P}) = \mathcal{J}/\mathcal{P}$$

by the second isomorphism theorem.

Let $\wp$ be a prime ideal of K over a rational prime p. Then

$$\bar{\sigma}\wp = \wp = (p) \quad \text{or} \quad \bar{\sigma}\wp \cdot \wp = (p).$$

so

$$\bar{\sigma}\wp = \wp^{-1} \text{ in } \mathcal{I}/\mathcal{P},$$

i.e. $\bar{\sigma}$ is just the involution which takes an element of $\mathcal{I}/\mathcal{P}$ to its inverse. Then it is obvious

$$\bar{\sigma}(\mathcal{J}/\mathcal{P}) = \mathcal{J}/\mathcal{P}.$$

since $\mathcal{J}/\mathcal{P}$ is a group. Hence L is Galois over $\mathbb{Q}$.

For any $g \in G_0$, assume that $(I, L/K) = g$ for some $I \in \mathcal{J}$. Then $\sigma g \sigma^{-1} = (\bar{\sigma}I, L/K) = (I^{-1}, L/K) = g^{-1}$. So we need only to show that $\sigma^2 = 1$. Let H be the Hilbert class field of K, it is sufficient to show that $\sigma^2 = 1$ in $Gal(H/\mathbb{Q})$.

Let $\sigma^2 = g_0$ in $Gal(H/K)$, then $\sigma^4 = \sigma g_0 \sigma^{-1} \sigma^2 = g_0^{-1}\sigma^2 = 1$. Assume that $g_0 \neq 1$, i.e. g_0 is of order 2, then we can take an unramified cyclic extension L of degree 2^r over K such that $g_0 \neq 1$ in $G_0 = Gal(L/K)$ by the direct sum decomposition of $Gal(H/K)$, here r is some positive integer. For each $g \in G_0$, σg is also an extension of $\bar{\sigma}$ to G_0 and $\sigma g \sigma g = \sigma g \sigma^{-1} \sigma^2 g = \sigma^2 = g_0$. So, g_0 is the unique element of order 2 in $Gal(L/\mathbb{Q})$. For any rational prime p ramified in K, the ramification index of p in $L/\mathbb{Q}$ is 2 obviously. Let $\mathfrak{P}$ be a prime ideal of L over p, then the inertia group of $\mathfrak{P}$ is of order 2, hence must be generated by g_0. This is impossible since K is fixed by g_0. So σ must be of order 2. Thus we complete the proof. □

2.2. Proof of Theorem 2

Proof. Let $\mathcal{O}_S(K)$ be the set of elements of K which are regular outside S. When S is nonempty, $\mathcal{O}_S(K)$ is a Dedekind domain and denote by $Cl_S(K)$ its ideal class group. In [4], Rosen proved there existed a maximal abelian extension H of K which is unramified with respect to S such that $Cl_S(K) \cong Gal(H/K)$ under the reciprocity map. Since S is stable under $Gal(K/k)$, S can be viewed as a set of primes of k. Hence we can define $\mathcal{O}_S(k)$ and $Cl_S(k)$ too. It is easy to see that $\mathcal{O}_S(K)$ is the integral closure of $\mathcal{O}_S(k)$ in K. By Prop. 14.1 in [5], we have the class number of $\mathcal{O}_S(k)$ is d_S, hence is 1 under our assumption. Therefore, the problem is reduced to the same case as in number fields. Since all the left proofs are the same, we omit them here. □

2.3. Proof of Theorem 3

Proof. Let J_K^1 be the group of ideles whose corresponding divisors are of degree 0 and $H^1 = H \cap J_K^1$. For each $\gamma \in H$, $\gamma\alpha^i$ must lie in H^1 for some integer i. Hence $H = H^1 \times \langle\alpha\rangle$. Let $Cl^0(K)$ be the group of divisor classes of degree 0 of K, it is easy to see that $Cl^0(K) \cong J_K^1/K^\times U_K$, where U_K is the group of unit ideles. Since $Cl^0(k)$ is trivial, $Gal(K/k)$ acts on $Cl^0(K)$ as a convolution. Hence H^1 is stable under $Gal(K/k)$ by the same reasoning as in the Proof of Theorem 1. On the other hand, L/k is Galois if and only if $\bar{\sigma}H = H$. Then this is equivalent to require that $\alpha^{\bar{\sigma}} \in H$. If we assume that L/k is Galois, then the determination of $Gal(L/k)$ is the same as above. Thus we finish the proof. □

Remark. Let L be an unramified cyclic extension of degree 2^r over a quadratic number field K. When $r = 1$, it is the direct consequence of genus theory that $Gal(L/\mathbb{Q})$ is the Klein group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. When $r = 2$, one can exclude that $Gal(L/\mathbb{Q})$ is the Hamilton quaternion group by genus theory too, however, not so directly. When $r > 2$, genus theory does not give the information of $Gal(L/\mathbb{Q})$. So, our results are independent of genus theory. It is easy to see that all the results hold for general quadratic extensions K/k of global fields such that $Cl(k)$ or $Cl^0(k)$ is trivial.

Acknowledgement

This work was supported by National Natural Science Foundation of China (Grant No. 10131010).

References

[1] Artin E, Tate J. Class field theory. New York: Benjamin; 1967.
[2] Cohn H. A classical invitation to algebraic numbers and class fields. New York: Springer-Verlag; 1978.
[3] Kishi Y, Miyake K. Parametrization of the quadratic fields whose class numbers are divisible by three. J Number Theory 2000;80:209–17.
[4] Rosen M. The Hilbert class field in function fields. Expos Math 1987;5:365–78.
[5] Rosen M. Number theory in function fields. New York: Springer; 2002.