Tôhoku Math. Journ.
34 (1982), 311-317.

# GALOIS GROUPS OF UNRAMIFIED SOLVABLE EXTENSIONS

KÔJI UCHIDA

(Received September 17, 1981)

Let $\boldsymbol{Q}$ and $\boldsymbol{Z}$ be the rational numbers and the rational integers, respectively. Let $m$ be a positive integer. Let $q$ be a prime number such that $q \equiv 1(\mathrm{mod}\, m)$. Let $\zeta_q$ be a primitive $q$-th root of unity. Then there exists an element $\eta_q$ in $\boldsymbol{Q}(\zeta_q)$ such that $[\boldsymbol{Q}(\zeta_q): \boldsymbol{Q}(\eta_q)] = m$. Let $\boldsymbol{Q}^{(m)}$ be the field generated by $\eta_q$ over $\boldsymbol{Q}$ for all prime numbers $q$ such that $q \equiv 1(\mathrm{mod}\, m)$. Then $\boldsymbol{Q}^{(m)}$ depends only on $m$. We are interested in the structure of the Galois groups of maximal unramified (solvable) extensions of algebraic number fields containing $\boldsymbol{Q}^{(m)}$ for some integer $m$. "Unramified" means every finite or infinite prime is unramified. We will see below that cohomological dimensions of such Galois groups are at most one. We will also see the Galois groups of maximal unramified solvable extensions are free pro-solvable groups under some additional condition on the ground fields. We see $p$-extensions given by Reichardt and Shafarevich are unramified over $\boldsymbol{Q}^{(m)}$, and their methods are essential in the following.

LEMMA 1. *Let $l$ be a prime number and let $\boldsymbol{Q}_l$ be the $l$-adic number field. Then $\boldsymbol{Q}_l^{(m)} = \boldsymbol{Q}^{(m)} \cdot \boldsymbol{Q}_l$ contains the maximal unramified extension of $\boldsymbol{Q}_l$.*

PROOF. Let $p$ be any prime number and $p^d$ be any power of $p$. It suffices to show that $\boldsymbol{Q}_l^{(m)}$ contains an unramified extension of $\boldsymbol{Q}_l$ whose degree is a multiple of $p^d$. We can assume $d$ is sufficiently large. It is easily seen that any common factor of $(l^{mp^d} - 1)/(l^{mp^{d-1}} - 1)$ and $l^{mp^{d-1}} - 1$ is a power of $p$. Hence any prime factor of $m$ except possibly $p$ is not a factor of $(l^{mp^d} - 1)/(l^{mp^{d-1}} - 1)$ for sufficiently large $d$. If $d \geqq 2$ and if $p$ is a factor of $(l^{mp^d} - 1)/(l^{mp^{d-1}} - 1)$, it must be $l^m \equiv 1(\mathrm{mod}\, p)$ and $l^{mp^{d-1}} - 1 = p^s a$, $(a, p) = 1$ for $s \geqq 2$. Then it is easy to see that $(l^{mp^d} - 1)/(l^{mp^{d-1}} - 1)$ is not divisible by $p^2$. Let $\Psi(X)$ be the defining polynomial of the primitive $mp$-th roots of unity over $\boldsymbol{Q}$. Then $\Phi(X) = \Psi(X^{p^{d-1}})$ is the defining polynomial of the primitive $mp^d$-th roots of unity. This shows $|\Phi(l)|$ is arbitrarily large for sufficiently large $d$. As $\Phi(l)$ is a divisor of $(l^{mp^d} - 1)/(l^{mp^{d-1}} - 1)$, $\Phi(l)$ has a prime factor $q$ which is not a divisor of $mpl$. Then $\Phi(l) = \prod_\zeta (l - \zeta)$ shows $(q)$ splits com-