Advanced Studies in Pure Mathematics 13, 1988
Investigations in Number Theory
pp. 1–7

Abundant Central Extensions and Genus Fields

Hiroshi Suzuki

Let k be a finite algebraic number field and K be a Galois extension of k of finite degree. Let L be a central extension of K/k, i.e. $Z(E)\supset A$, where $G=G(K/k)$, $A=G(L/K)$ and $E=G(L/k)$ are Galois groups and $Z(E)$ means the center of E.

The genus field in L is the subfield which corresponds to $A\cap E^c$, E^c being the commutator subgroup of E. Generally this group is a quotient group of the dual $M(G)=H^{-3}(G, \boldsymbol{Z})$ of the Schur multiplier $H^2(G, \boldsymbol{Q}/\boldsymbol{Z})$ of G, and the condition $A\cap E^c=M(G)$ is equivalent to the fact that L is abundant for K/k (i.e. $L\cdot k^{\mathrm{ab}}$ is the maximal central extension of K/k, where k^{ab} is the maximal abelian extension of k). We call the genus field trivial if the genus field coincides with K. In words of group theory, it means that E is a central-commutator extension of $M(G)$ by G.

Miyake [2] treats a problem when K/k has an abundant central extension with trivial genus field. And Miyake [3] gives sufficient conditions, which come from an equivalent condition of this problem, that is

$$\{\alpha\in N_{K/k}J_k \mid \alpha^n\in k^\times\}\subset N_{K/k}J_K\cap k^\times\cdot N_{K/k}\{\alpha\in J_K \mid \alpha^n\in K^\times I_G J_K\}$$

for all any factors n of $\exp M(G)$, where J_K is the idele group of K, I_G is the augmentation ideal of $\boldsymbol{Z}[G]$ and $\exp M(G)$ is the exponent of $M(G)$.

Miyake considered in [4] the problem in local fields in detail, and he gives examples of K/k which has no abundant central extension with trivial genus field for lack of local one at a place where the decomposition group coincides with $G=G(K/k)$.

Even though G is given, in general, the Galois groups of abundant central extensions with the trivial genus fields are not determined uniquely. In this paper we shall consider conditions of the embedding-problem-type that gives the existence of a global abundant central extension with the trivial genus field whose Galois group is a given one, and give several examples of such a case. We give also an example of K/k which has no global abundant central extension with the trivial genus field but has local ones at all places of k.

Received March 20, 1985.

1. We denotes the absolute Galois group of a field M by $\mathfrak{G}_M$. When a central extension of groups $1 \to A \to E \to G \to 1$ with $G = G(K/k)$ is given, we consider the following conditions $(*)$ and $(*)_\mathfrak{p}$. For a prime $\mathfrak{p}$ of k, we take a prime divisor $\mathfrak{P}$ of $\mathfrak{p}$ in K.

$(*)$ There exists a G-epimorphism f: $\mathfrak{G}_K \to A$ such that the following diagram is commutative:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathfrak{G}_K & \longrightarrow & \mathfrak{G}_k & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

This condition is equivalent to the existence of a field L satisfying $G(L/k) = E$ naturally.

$(*)_\mathfrak{p}$ There exists a $G_\mathfrak{p}$-homomorphism $f_\mathfrak{p}$: $G_{K_\mathfrak{P}} \to A$ such that the following diagram is commutative:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathfrak{G}_{K_\mathfrak{P}} & \longrightarrow & \mathfrak{G}_{k_\mathfrak{p}} & \longrightarrow & G_\mathfrak{p} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

Here $G_\mathfrak{p}$ is the decomposition group of G at $\mathfrak{p}$.

This condition does not depend on the choice of $\mathfrak{P}$. If $\mathfrak{p}$ is unramified, then $(*)_\mathfrak{p}$ holds evidently.

2. We put $P(m, k) = |J_k^m \cap k^\times / k^{\times m}|$ $(=1$ or $2)$ for each natural number m. If $m \mid m'$, $P(m, k) = 1$ derives from $P(m', k) = 1$.

Now the following proposition is probably known, but we prove it for the sake of convenience (Cf. Neukirch [5]).

Proposition. *When* $P(\exp A, k) = 1$, *the condition* $(*)$ *is equivalent to the condition that* $(*)_\mathfrak{p}$ *holds for all* $\mathfrak{p}$ *which is ramified in* K/k.

Proof. We denote the condition $(*)$ without the homomorphism f being onto by $(\bar{*})$. Consider the Hochschild-Serre exact sequence

$$0 \longrightarrow H^1(G, A) \xrightarrow{\text{inf}^1} H^1(\mathfrak{G}_k, A) \xrightarrow{\text{res}^1} H^1(\mathfrak{G}_K, A)^G \xrightarrow{\text{trg}} H^2(G, A) \xrightarrow{\text{inf}^2} H^2(\mathfrak{G}_k, A).$$

Let $\xi \in H^2(G, A)$ be the cohomology class for the group extension $1 \to A \to E \to G \to 1$. Then $(\bar{*})$ means that there exists $f \in H^1(\mathfrak{G}_K, A)^G$ such that $\xi = -\text{trg} f$, which is equivalent to $\inf^2 \xi = 0$.

Now assume that the homomorphism f of ($*$) exists. Put $A=\langle a_i; i=1, \cdots, m\rangle$ by taking generators a_i. Let L' be the field corresponding to $\mathrm{Ker} f$, and take m primes $\mathfrak{p}_1, \cdots, \mathfrak{p}_m$ of k which are decomposed completely in L'/k and not dividing 2. (There exist infinitely many such primes.) For each i ($i=1, \cdots, m$), let χ_i be a global character $J_k \twoheadrightarrow \langle a_i\rangle$ which is induced from a family of homomorphisms $k_{\mathfrak{p}_i}=K_{\mathfrak{P}_i} \twoheadrightarrow \langle a_i\rangle$, $k_{\mathfrak{p}_j}\to 0$ ($j\neq i$) with $\mathfrak{P}_i$ being a prime divisor of $\mathfrak{p}_i$ in K (See Artin-Tate [1, Chap. 10]). Then we can consider $\chi_i \in H^1(\mathfrak{G}_k, A)$. $\sum_i \mathrm{res}^1 \chi_i + f$ has the image ξ by $-\mathrm{trg}$ also. And if we restrict it to $\mathfrak{G}_{K_{\mathfrak{P}_i}}=\mathfrak{G}_{k_{\mathfrak{p}_i}}$, all the term are trivial except χ_i. Since $\chi_i(\mathfrak{G}_{k_{\mathfrak{p}_i}})=\langle a_i\rangle$, $\mathrm{Im}(\sum_i \mathrm{res}^1 \chi_i+f) \ni a_i$ ($i=1, \cdots, m$) or $\sum_i \mathrm{res}^1 \chi_i + f$ is G-epimorphism. So ($*$) is satisfied. Now it is shown that ($*$) is equivalent to $\inf^2 \xi=0$.

Consider the following diagram (1).

$$(1)\qquad \begin{array}{ccc} H^2(G, A) & \xrightarrow{\inf^2} & H^2(\mathfrak{G}_k, A) \\ \big\downarrow (\mathrm{res}^2_{\mathfrak{p}})_{\mathfrak{p}} & \circlearrowright & \big\downarrow (\mathrm{res}^2_{\mathfrak{p}})_{\mathfrak{p}} \\ \bigoplus_{\mathfrak{p}} H^2(G_{\mathfrak{p}}, A) & \xrightarrow[\bigoplus_{\mathfrak{p}} \inf^2_{\mathfrak{p}}]{} & \bigoplus_{\mathfrak{p}} H^2(\mathfrak{G}_{k_{\mathfrak{p}}}, A) \end{array}$$

Here $\mathfrak{p}$ runs all the primes of k. Denote by μ_m the group of m-th roots of 1, for $m \in N$. The diagram

$$\begin{array}{ccc} H^1(\mathfrak{G}_k, \mu_m) & \longrightarrow & \prod_{\mathfrak{p}} H^1(\mathfrak{G}_{k_{\mathfrak{p}}}, \mu_m) \\ \wr\| & \circlearrowright & \wr\| \\ k^{\times}/k^{\times m} & \longrightarrow & \prod_{\mathfrak{p}} k_{\mathfrak{p}}^{\times}/k_{\mathfrak{p}}^{\times m} \end{array}$$

implies that $H^1(\mathfrak{G}_k, \mu_m)\to \prod_{\mathfrak{p}} H^1(\mathfrak{G}_{k_{\mathfrak{p}}}, \mu_m)$ is monomorphic if $P(m, k)=1$.

So Tate's duality theorem proves that the right hand vertical map of (1) is a monomorphism if $P(m, k)=1$. Hence, when $P(\exp A, k)=1$, it follows that $\inf^2 \xi=0 \Leftrightarrow \mathrm{res}^2_{\mathfrak{p}} \inf^2 \xi=0$ ($\forall \mathfrak{p}$). Similarly in the beginning of this proof, $\mathrm{res}^2_{\mathfrak{p}} \inf^2 \xi=0$ is equivalent to ($*_{\mathfrak{p}}$). Now the proposition is proved.

Remark. In $k(\mu_{2^\infty})$, take a primitive 2^r-th root ζ_{2^r} of 1 such that $\zeta_{2^{r+1}}=\zeta_{2^r}^2$, and put $\eta_r=\zeta_r+\zeta_r^{-1}$. Let s be the maximal number such that $\eta_s \in k$. Then $P(m, k)=2$ if and only if (m, k) satisfies next three conditions 1, 2 and 3.

1. $-1, 2+\eta_s, -(2+\eta_s) \notin k^2$.
2. $m=2^t m'$ where m' is odd and $t>s$.
3. -1 or $2+\eta_s$ or $-(2+\eta_s) \in k_{\mathfrak{p}}^2$ for every $\mathfrak{p}|2$.

Since $\eta_{s+1}^2=2+\eta_s$, putting $a_{0,m}=(1+\zeta_s)^m=(2+\eta_s)^{m/2}=(-2-\eta_s)^{m/2}$, we can write $k^{\times} \cap J_k^m = a_{0,m} k^{\times m} \cup k^{\times m}$ and $a_{0,m} \notin k^{\times m}$ in this case. (See Artin-Tate [1, Chap. 10])

Take $m_0 \in \boldsymbol{N}$ the minimal number such that $P(m_0, k)=2$ and take $u_0 \in J_k$ such that $u_0^{m_0} = a_{0,m_0}$. Then $a_{0,m} = u_0^m$ for $m \geqq m_0$.

Without any assumption, $(*)$ is equivalent to the condition that $(*)_{\mathfrak{p}}$ holds for all $\mathfrak{p}$ which is ramified in K/k and $\mathrm{inv}(u_0^{\chi \circ \xi})=0$ for any character χ: $A \to \boldsymbol{Z}/\mathrm{ord}\,\chi \cdot \boldsymbol{Z}$ such that $P(\mathrm{ord}\,\chi, k)=2$. Here ξ is the cocycle of the extension $1 \to A \to E \to G \to 1$ and inv is the global invariant, which gives $H^2(G, C_K) \subsetneq \boldsymbol{Q}/\boldsymbol{Z}$.

3. Now we can consider a condition of the existence of an abundant central extension with the trivial genus field by taking a central-commutator extension $1 \to M(G) \to E \to G \to 1$ instead of $1 \to A \to E \to G \to 1$ in $(*)$ or $(*)_{\mathfrak{p}}$.

For example, if K/k is unramified and $P(\exp M(G), k)=1$, there exists an abundant central extension of K/k with the trivial genus field with any central-commutator extension of $M(G)$ by G as its Galois group. Hence there exists an extension K/k which has at least two kinds of abundant central extension with the trivial genus field whose galois groups are not isomorphic.

As an easier example, we consider the following case.

Take a pair of odd prime numbers p and q such that $q \equiv 1 \bmod p^2$. Let k_1 and k_2 be the subfields of $\boldsymbol{Q}(\zeta_{p^2})$ and $\boldsymbol{Q}(\zeta_q)$ over $\boldsymbol{Q}$ of degree p respectively. Then q is unramified in $k_1/\boldsymbol{Q}$. Put $K = k_1 \cdot k_2$ and $k = \boldsymbol{Q}$.

$G = \boldsymbol{Z}/p\boldsymbol{Z} \times \boldsymbol{Z}/p\boldsymbol{Z}$ has two central-commutator extensions of exponent p and of p^2.

At q, $\boldsymbol{Q}_q \ni \zeta_{p^2}$ and $K_{\mathfrak{Q}}$ is a ramified extension of $k_q = \boldsymbol{Q}_q$ of degree p where $\mathfrak{Q}$ is a prime divisor of q in K where $(*)_q$ holds when the exponent is either p or p^2.

At p, since the Galois group of the maximal p-extension of $\boldsymbol{Q}_p$ is free pro-p-group of rank 2, $(*)_p$ holds of course. As the other primes are unramified, K/k has two abundant central extensions with the trivial genus fields with distinct whole Galois groups (which are non-abelian groups of order p^3 with exponent p and p^2).

The existence of an abundant central extension for a local extension $K_{\mathfrak{P}}/k_p$ is not equivalent to $(*)_p$. In fact the following example shows that there is an extension K/k which has local abundant central extensions at every p, but has no global one.

Example. Take odd prime numbers p, p_1, p_2 and p_3 such that $p_i \equiv 1 \bmod p$, $p_i \equiv 1 \bmod p^2$ $(i=1, 2, 3)$,

$$p_2^{(p_1-1)/p} \equiv 1 \bmod p_1, \qquad p_3^{(p_1-1)/p} \equiv 1 \bmod p_1,$$
$$p_1^{(p_2-1)/p} \not\equiv 1 \bmod p_2, \qquad p_3^{(p_2-1)/p} \equiv 1 \bmod p_2,$$
$$p_1^{(p_3-1)/p} \not\equiv 1 \bmod p_3, \qquad p_2^{(p_3-1)/p} \equiv 1 \bmod p_3.$$

Let k_1, k_2 and k_3 be the subfield of degree p over $\boldsymbol{Q}$ of $\boldsymbol{Q}(\zeta_{p_1})$, $\boldsymbol{Q}(\zeta_{p_2})$ and $\boldsymbol{Q}(\zeta_{p_3})$ respectively. Take further a subfield k_4 of $k_1 \cdot k_2$ of degree p to be neither k_1 nor k_2.

By the choice of p, p_1, p_2 and p_3, the decompositions of primes are as follows:

fields \ primes	p_1	p_2	p_3	the others
k_1	ramified	decomposed	dec.	unram. or dec.
k_2	unramified	ram.	dec.	
k_3	unram.	dec.	ram.	
k_4	ram.	ram.	dec.	

Put $k=\boldsymbol{Q}$ and $K=k_3 \cdot k_4$. As in Miyake and Ormerod [4], any abundant central extension of K/k with the trivial genus field must be an abundant central extension of $K_{\mathfrak{P}_1}/\boldsymbol{Q}_{p_1}$ with the trivial genus field where $\mathfrak{P}_1$ is a prime divisor of p_1.

The Galois group of the maximal p-extension of $\boldsymbol{Q}_{p_1}$ is $\langle s, t \mid s^{-1}ts = t^{p_1} \rangle$ as pro-p-group and $\langle t \rangle$ is inertia group. So it is evident that the class of t in the Galois group of a local abundant central extension with the trivial genus field must be of order p^2.

The subgroup of $G(K/k)$ generated by the class of t is the inertia subgroup $G(K/k_3)$ of K/k at p_1, and is also inertia group at p_2. So, when $(*)_{\mathfrak{P}_1}$ holds, the condition $(*)_{p_2}$ implies the existence of a cyclic extension L_{p_2} of degree p^2 over $\boldsymbol{Q}_{p_2}$ containing $K_{\mathfrak{P}_2}$, here P_2 and $\mathfrak{P}_2$ are prime divisors of p_2 in L and K such that $P_2 \mid \mathfrak{P}_2$. Since $K_{\mathfrak{P}_2}/\boldsymbol{Q}_{p_2}$ is ramified, $L_{P_2}/\boldsymbol{Q}_{p_2}$ must be a totally ramified cyclic extension of degree p^2. But it is impossible because $p_2 \not\equiv 1 \bmod p^2$.

Hence $(*)_{p_1}$ and $(*)_{p_2}$ cannot stand together, K/k has no global abundant central extension. By the way, $K_{\mathfrak{P}_1}/\boldsymbol{Q}_{p_1}$ has a local abundant central extension with group $\langle s, t \mid s^p=1,\ t^{p^2}=1,\ s^{-1}ts=t^{p_1} \rangle$, and $K/\boldsymbol{Q}$ is locally cyclic at any other primes.

As the prime numbers satisfying the above condition, there are for instance $p=3$, $p_1=7$, $p_2=13$ and $p_3=6007$.

4. There exists the case that a central-commutator extension of exponent p^2 is possible but those of exponent p are impossible as the Galois group of an abundant central extension with the trivial genus field, and also exists the case that exponent p is possible and p^2 is impossible.

Example. (The case that p^2 is possible but p is impossible.) In the last example, put $K=k_1\cdot k_2$ and $k=\boldsymbol{Q}$. Of course it is impossible to construct any abundant central extension with the trivial genus field with Galois group of exponent p.

In the group $\langle s, t \mid s^p=1,\ t^{p^2}=1,\ s^{-1}ts=t^{p_1}\rangle$, $s^a t^b$ is of order p if a $\in (\boldsymbol{Z}/p\boldsymbol{Z})^\times$ and $b\equiv 0 \bmod p$. Therefore $(*)_{p_1}$ and $(*)_{p_2}$ stand together, and so K/k has an abundant central extension with the trivial genus field with Galois group of exponent p^2.

Example. (The case that p is possible but p^2 is impossible.) Take odd prime numbers $p, p_1, \cdots, p_p$ and p_{p+1} such that $p_i\equiv 1 \bmod p$, $p_i\not\equiv 1 \bmod p^2$ $(i=1, \cdots, p+1)$ and $p_i^{(p_j-1)/p}\equiv 1 \bmod p_j$ for any pair (i, j) of distinct natural numbers $\leqq p+1$. Let k_i be the subfield of degree p of $\boldsymbol{Q}(\zeta_i)$ and take a generator σ_i of

$$G(\prod_j k_j/\prod_{j\neq i} k_j) \quad (\cong G(k_i/\boldsymbol{Q})) \quad \text{for } i=1, \cdots, p+1.$$

$$G(\prod_i k_i/\boldsymbol{Q})=\bigoplus_{i=1}^{p+1} G(\prod_j k_j/\prod_{j\neq i} k_j).$$

On the other hand, $\boldsymbol{Z}/p\boldsymbol{Z}\times\boldsymbol{Z}/p\boldsymbol{Z}$ has $p+1$ subgroups of order p generated by $h_1=(1, 0)$, $h_2=(1, 1), \cdots, h_p=(1, p-1)$ and $h_{p+1}=(0, 1)$. Now $\varphi(\sigma_i)=h_i$ $(i=1, \cdots, p-1)$ determine an epimorphism

$$\varphi\colon G\Big(\prod_{i=1}^{p+1} k_i/\boldsymbol{Q}\Big)\twoheadrightarrow \boldsymbol{Z}/p\boldsymbol{Z}\times\boldsymbol{Z}/p\boldsymbol{Z}.$$

Let k be the subfield corresponding to the kernel of φ. The inertia group of K/k, which is equal to the decomposition group, is the cyclic subgroup of $\boldsymbol{Z}/p\boldsymbol{Z}\times\boldsymbol{Z}/p\boldsymbol{Z}$, generated by h_i.

Since $(*)_{p_i}$ shows that the inverse image of $\langle h_i\rangle$ to the Galois group of an abundant central extension of $K/\boldsymbol{Q}$ with the trivial genus field cannot be cyclic of order p^2, the Galois group must be of exponent p. And it is evident that there exists an abundant central extention with the trivial genus field with Galois group of exponent p, because $K/\boldsymbol{Q}$ is everywhere locally cyclic.

As such primes, we can find

$p=3,\quad p_1=7,\quad p_2=223,\quad p_3=1777,\quad p_4=39199;$

$p=3,\quad p_1=13,\quad p_2=103,\quad p_3=3613,\quad p_4=13417;$

$p=3,\quad p_1=31,\quad p_2=349,\quad p_3=2131,\quad p_4=7968;$

. . . . .

References

[1] E. Artin and J. Tate, Class field theory, Benjamin New York, 1967.

[2] K. Miyake, Central extensions and Schur's multiplicators of Galois groups, Nagoya Math. J., **90** (1983), 137–144.

[3] ——, On central extensions of a Galois extension of algebraic number fields, Nagoya Math. J., **93** (1984), 133–148.

[4] K. Miyake and N. Ormerod, Abundant central extensions of non trivial genera, Nagoya Math. J., **95** (1984), 51–62.

[5] J. Neukirch, Über das Einbettungsproblem der algebraischen Zahlentheorie, Invent. Math., **21** (1973), 59–116.

Department of Mathematics
Tokyo Metropolitan University
Fukasawa, Setagaya-ku
Tokyo 158, Japan