On an Existence Theorem of Grunwald's Type*

JURGEN NEUKIRCH

Let k be a number field, S a finite set of primes of k and $k_{\mathfrak{p}}$ the completions of k at the primes $\mathfrak{p} \in S$. Then the existence theorem of Grunwald-Hasse-Wang asserts:

If $K_{\mathfrak{p}} \mid k_{\mathfrak{p}}$ are given cyclic extensions, $\mathfrak{p} \in S$, then there always exists a global cyclic extension $K \mid k$ having the local extensions $K_{\mathfrak{p}} \mid k_{\mathfrak{p}}$ as completions for $\mathfrak{p} \in S$. In this note we prove.

THEOREM. *If $K_{\mathfrak{p}} \mid k_{\mathfrak{p}}$ are arbitrary (solvable*[1]*) galois extensions, $\mathfrak{p} \in S$, then there always exists a solvable galois extension $K \mid k$ having the given local extensions $K_{\mathfrak{p}} \mid k_{\mathfrak{q}}$ as completions for $\mathfrak{p} \in S$.*

PROOF. It suffices to prove the theorem in the case that $K_{\mathfrak{p}} = k_{\mathfrak{p}}$ for all but one prime $\mathfrak{p}$ of S. The general case is obtained from this in the following way: For every $\mathfrak{q} \in S$ let $K^{(\mathfrak{q})} \mid k$ be a solvable galois extension whose completion is $K_{\mathfrak{q}}$ at $\mathfrak{q}$ and is $k_{\mathfrak{p}}$ at $\mathfrak{p} \neq \mathfrak{q}$. Let K be the composite of the $K^{(\mathfrak{q})}$, $\mathfrak{q} \in S$. The completion of K at $\mathfrak{p}$ is then the composite of the completions of the $K^{(\mathfrak{q})}$ at $\mathfrak{p}$, $\mathfrak{q} \in S$, and this composite is in fact $K_{\mathfrak{p}}$.

Let now $K_{\mathfrak{p}} = k_{\mathfrak{p}}$ for $\mathfrak{p} \neq \mathfrak{q}$. We first prove the theorem in the case that the galois group $A = G(K_{\mathfrak{q}} \mid k_{\mathfrak{q}})$ of $K_{\mathfrak{q}} \mid k_{\mathfrak{q}}$ is cyclic of prime degree p, that there even exists a global cyclic extension $K \mid k$ of degree p. Let G resp. $G_{\mathfrak{p}}$ be the absolute galois group over k resp. $k_{\mathfrak{p}}$, i.e. the galois group of the algebraic closure $\bar{k}$ resp. $\bar{k}_{\mathfrak{p}}$. If we imbed $\bar{k}$ into $\bar{k}_{\mathfrak{p}}$ we obtain $G_{\mathfrak{p}}$ as a subgroup of G by restricting the automorphisms of $\bar{k}_{\mathfrak{p}}$ to $\bar{k}$.

*Recebido pela SBM em 25 de abril de 1974.

[1]Note that every local extension $K_{\mathfrak{p}} \mid k_{\mathfrak{p}}$ is solvable.

We now look at the diagrams

$$\begin{array}{ccc} G & \longrightarrow & G_{\mathfrak{p}} \\ & \psi \searrow \quad \swarrow \psi_{\mathfrak{p}} & \\ & A & \end{array} , \qquad \mathfrak{p} \in S,$$

where $\psi_{\mathfrak{q}} : G_{\mathfrak{q}} \longrightarrow A = G(K_{\mathfrak{q}} \mid k_{\mathfrak{q}})$ is the canonical homomorphism and $\psi_{\mathfrak{p}}$ is the trivial homomorphism for $\mathfrak{p} \neq \mathfrak{q}$. The problem is then to find a homomorphism $\psi : G \longrightarrow A$ with $\psi \mid G_{\mathfrak{p}} = \psi_{\mathfrak{p}}$ for all $\mathfrak{p} \in S$, since the fixed field K of $Ker(\psi)$ then obviously has the required properties. Hence it suffices to prove the surjectivity of the map

$$Hom(G, A) \longrightarrow \prod_{\mathfrak{p} \in S} Hom(G_{\mathfrak{p}}, A)$$

Viewing A as a G-module with trivial G-action, this can be written

(1) $$H^1(G, A) \longrightarrow \prod_{\mathfrak{p} \in S} H^1(G_{\mathfrak{p}}, A).$$

Now by the duality theorem of Tate and Poitou (cf. [3]) we have the exact sequence

$$H^1(G, A) \longrightarrow \prod_{\mathfrak{p} \in S} H^1(G_{\mathfrak{p}}, A) \times \prod_{\mathfrak{p} \in S} H^1(G_{\mathfrak{p}}, A) \longrightarrow H^1(G, A')^*$$

where $A' = Hom(A, \bar{k}^*)$ is the dual G-module of A and X^* denotes the Pontrjagin-dual of X. A moment's reflection shows that the map (1) is surjective if the map

$$\prod_{\mathfrak{p} \in S} H^1(G_{\mathfrak{p}}, A) \longrightarrow H^1(G, A')^*$$

is surjective. Going over to the dual map and identifying $H^1(G_{\mathfrak{p}}, A)^*$ with $H^1(G_{\mathfrak{p}}, A')$ by the local duality theorem we have to prove the injectivity of

$$H^1(G, A') \longrightarrow \prod_{\mathfrak{p} \in S} H^1(G_{\mathfrak{p}}, A').$$

Since $A \cong \mathbb{Z}/p$, A' is isomorphic to the module μ_p of the p-th roots of unity. Furthermore the exact sequence

$$1 \longrightarrow \mu_p \longrightarrow \bar{k}^* \xrightarrow{\ p\ } \bar{k}^* \longrightarrow 1$$

yields the exact cohomology sequence

$$k^* \xrightarrow{\ p\ } k^* \longrightarrow H^1(G, \mu_p) \longrightarrow H^1(G, \bar{k}^*)$$

in which $H^1(G, \bar{k}^*) = 1$ by Hilbert's theorem 90. We therefore have $H^1(G, A') = k^*/k^{*p}$ and analogously $H^1(G_{\mathfrak{p}}, A') = k^*_{\mathfrak{p}}/k^{*p}_{\mathfrak{p}}$, i.e. we have to prove the injectivity of

$$k^*/k^{*p} \longrightarrow \prod_{\mathfrak{p} \in S} k^*_{\mathfrak{p}}/k^{*p}_{\mathfrak{p}}.$$

Let $a \in k^*$ such that $a \in k^{*p}_{\mathfrak{p}}$ for all $\mathfrak{p} \notin S$. Let ζ be a primitive p-th root of unity and $k' = k(\zeta)$. We then look at the extension $k'(\theta) \mid k'$, where θ is a root of $x^p - a = 0$. Since $a \in k^{*p}_{\mathfrak{p}}$ for $\mathfrak{p} \notin S$ this equation splits totally over almost all completions of k', i.e. almost all primes of k' split totally in $k'(\theta)$. By Kronecker's density theorem we obtain $k'(\theta) = k'$, i.e. $\theta \in k'$. Since the degree $[k' : k]$ is prime to p we have moreover $\theta \in k$, i.e. $a \in k^{*p}$ q.e.d.

Now let $K_{\mathfrak{q}} \mid k_{\mathfrak{q}}$ be an arbitrary galois extension. The proof in this general case will be by induction over the degree $[K_{\mathfrak{q}} : k_{\mathfrak{q}}]$. If $K_{\mathfrak{q}} = k_{\mathfrak{q}}$ we can take $K = k$. Otherwise, the solvable extension $K_{\mathfrak{q}} \mid k_{\mathfrak{q}}$ contains a subextension $L_{\mathfrak{q}} \mid k_{\mathfrak{q}}$ which is cyclic of prime degree p. We have already shown that there exists a cyclic extension $L \mid k$ of degree

$$[L : k] = [L_{\mathfrak{q}} : k_{\mathfrak{q}}] = p$$

such that $L_{\mathfrak{Q}} \cong L_{\mathfrak{q}}$ and $L_{\mathfrak{P}} = k_{\mathfrak{p}}$ for $\mathfrak{p} \neq \mathfrak{q}$, $\mathfrak{p} \in S$. Here $\mathfrak{Q}$ denotes the (only) prime of L above $\mathfrak{q}$ and $\mathfrak{P}$ is any prime of L over $\mathfrak{p}$, while $L_{\mathfrak{Q}}$ resp. $L_{\mathfrak{P}}$ means the completion of L with respect to $\mathfrak{Q}$ resp. $\mathfrak{P}$. Let $\bar{S}$ be the set of all primes of L lying above S. Since $[K_{\mathfrak{q}} : L_{\mathfrak{q}}] < [K_{\mathfrak{q}} : k_{\mathfrak{q}}]$ we can assume by induction that there exists a solvable galois extension $K_1 \mid L$ such that

$$K_{1\,\mathfrak{Q}^1} \cong K_{\mathfrak{q}} \text{ and } K_{1\,\mathfrak{P}^1} = L_{\mathfrak{P}} \text{ for } \mathfrak{P} \in \bar{S},\ \mathfrak{P} \neq \mathfrak{Q},$$

where $\mathfrak{Q}_1$ res. $\mathfrak{P}_1$ is any of prime K_1 over $\mathfrak{Q}$ resp. . Now let $K_1, K_2, \dots$, be the conjugates of K_1 over k and K their composite. Then $K \mid k$ is a solvable galois extension. Let $\tilde{\mathfrak{Q}}$ resp. $\tilde{\mathfrak{P}}$ be a prime of K above $\mathfrak{q}$ resp. $\mathfrak{p} \neq \mathfrak{q}$, $\mathfrak{p} \in S$, and let $\mathfrak{Q}_i$ resp. $\mathfrak{P}_i$ be the prime of K_i under $\tilde{\mathfrak{Q}}$ resp. $\tilde{\mathfrak{P}}$, $i = 1, 2, \dots$. Then

$$K_{\tilde{\mathfrak{Q}}} = \prod_i K_{i\mathfrak{Q}_i} \quad \text{and} \quad K_{\tilde{\mathfrak{P}}} = \prod_i K_{i\mathfrak{P}_i}$$

Let σ_i be an automorphism of K such that $\sigma_i K_i = K_i$, $i = 1, 2 \dots$. The isomorphism $\sigma_i^{-1} : K_i \longrightarrow K_1$ maps the prime $\mathfrak{P}_i = \tilde{\mathfrak{P}} \mid \sigma_i K_1$ of $\sigma_i K_1 = K_i$ onto the prime $\mathfrak{P}'_1 = \sigma_i^{-1} \tilde{\mathfrak{P}} \mid K_1$ of K_1. Therefore we have in case $\tilde{\mathfrak{P}}/\mathfrak{p}$, $\mathfrak{p} \neq \mathfrak{q}$,

$$K_{i\mathfrak{P}_i} \cong K_{1\mathfrak{P}_1}$$

and consequently $K_{i\mathfrak{P}_i} \cong K_{1\mathfrak{P}'_1} = L_{\mathfrak{P}'} \quad = k_{\mathfrak{p}}$ where $\mathfrak{P}' = \mathfrak{P}'_1 \mid L$, i.e. $K_{\tilde{\mathfrak{P}}} = k_{\mathfrak{p}}$. Analogously we have

$$K_{i\mathfrak{Q}_i} \cong K_{1\mathfrak{Q}_1}, \quad \text{where} \quad \mathfrak{Q}'_1 = \sigma_i^{-1} \tilde{\mathfrak{Q}} \mid K_1 .$$

Since $\mathfrak{Q}$ is the only prime of L over $\mathfrak{q}$ we have $\mathfrak{Q}'_1 \mid L = \mathfrak{Q}$, i.e. $K_{i\mathfrak{P}_i} \cong K_{1\mathfrak{Q}'_1} \cong K_{\mathfrak{q}}$ for every i, and this yields $K_{\tilde{\mathfrak{Q}}} = \prod K_{i\mathfrak{Q}_i} \cong K_{\mathfrak{q}}$, which proves the theorem.

Remark. Although the above theorem seems to be a very far reaching generalization of Grunwald's version, it is actually not very profound. The original formulation of Grunwald's problem requires the additional condition

$$[K : k] = l.c.m.\ [K_{\mathfrak{p}} : k_{\mathfrak{p}}]$$

for the degree of the cyclic extension $K \mid k$. With this additional requirement the cyclic problem is unsolvable in a special case (which does not occur if the degrees $[K_{\mathfrak{p}} : k_{\mathfrak{p}}]$, $\mathfrak{p} \in S$, are odd). The correct formulation of the general existence problem should be the following:

Let $K_{\mathfrak{p}} \mid k_{\mathfrak{p}}$ galois extensions with galois groups $G_{\mathfrak{p}}$, $\mathfrak{p} \in S$, G a finite group and $G_{\mathfrak{p}} \longrightarrow G$ imbeddings. Does there exist a galois extension $K \mid k$ satisfying the following conditions:

1) $K_{\mathfrak{p}} \mid k_{\mathfrak{p}}$ are the completions of $K \mid k$ at the primes $\mathfrak{p} \in S$.

2) The galois group $G(K \mid k)$ of $K \mid k$ is isomorphic to the given group G in such a way that the image of $G_{\mathfrak{p}}$ in $G(K \mid k)$ is a decomposition group of $K \mid k$ belonging to the prime $\mathfrak{p} \in S$?

It is known that the answer is positive in the case that $k = \mathbb{Q}$ and G is nilpotent of odd order (see [1]).

LITERATURE

[1] J. Neukirch, *Über das Einbettungsproblem der algebraischen Zahlentheorie*, Inventiones math. **21**, 59-116 (1973).

[2] J. Neukirch, *Eine Bemerkung zum Existenzsatz von Grunwald-Hasse-Wang*, J. reine angew. Math. **262/263**. (1973).

[3] G. Poitou, Cohomologie galoisienne des modules finis, Paris, Dunod 1967.

Universität Regensburg
Regensburg Germany