On the embedding problem for global fields

Comments to an old paper of Klaus Hoechsmann.

Peter Roquette (Heidelberg)

August 27, 2003

Abstract

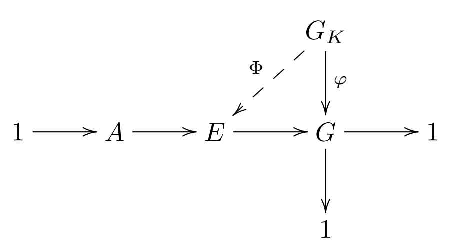
The origin of this note was the attempt to answer a question of Moshe Jarden who had asked me:

> "*Hat jeder Zahlkörper K ein endliches Einbettungsproblem für $Gal(K)$, das lokal lösbar aber global nicht lösbar ist?*"

As a first reaction I referred him to an old paper of Hoechsmann [1] on the embedding problem. But after a second reading of Hoechsmann's paper I found that the answer to Moshe's question – which is affirmative – is not explicitly stated there. Although the answer can be readily derived using Hoechsmann's ideas, it is perhaps not without interest to do this explicitly. This is what I propose in this note.

1 Statement of the result

Let K be a global field and G_K its absolute Galois group. Let A be a finite G_K-module. The action of G_K on A factors through a finite factor group. Let G be such a factor group, i.e. $G = G_K/U$ where U is an open normal subgroup of G_K which acts trivially on A. We consider embedding problems of the form



(1)

where φ is the natural projection, and where E is a group extension of A with G. Such group extensions correspond to the cohomology classes $\varepsilon \in H^2(G, A)$. We are looking for solutions Φ of the embedding problem. We do not require that Φ be surjective. But note that for a global field, it is well known that the existence of any solution, surjective or not, implies the existence of a surjective solution. (A proof can be found in Hoechsmann's paper.)

If $\mathfrak{p}$ is a prime of K then $K_{\mathfrak{p}}$ denotes its completion. The absolute Galois group $G_{K_{\mathfrak{p}}}$ is considered as a subgroup of G_K, viz. the decomposition group of an extension of $\mathfrak{p}$ to the algebraic closure (unique up to conjugation). Let $G_{\mathfrak{p}} = \varphi(G_{K_{\mathfrak{p}}})$ denote the decomposition group of $\mathfrak{p}$ in G.

Given an embedding problem (1) its *localization* at $\mathfrak{p}$ is

$$
\begin{array}{ccccccccc}
 & & & & & & G_{K_{\mathfrak{p}}} & & \\
 & & & & & \swarrow & \downarrow & & \\
1 & \longrightarrow & A & \longrightarrow & E_{\mathfrak{p}} & \longrightarrow & G_{\mathfrak{p}} & \longrightarrow & 1 \\
 & & & & & & \downarrow & & \\
 & & & & & & 1 & &
\end{array}
\qquad (2)
$$

where $E_{\mathfrak{p}}$ is the inverse image of $G_{\mathfrak{p}}$ under the map $E \to G$. The factor system of this localization is the restriction $\mathrm{res}_{G_{\mathfrak{p}}}(\varepsilon)$ of the factor system ε of (1).

The solvability of (1) implies the solvability of (2) for each $\mathfrak{p}$. The "Local-Global-Principle" $\mathsf{LGP}(A, K)$ asserts that conversely, if an embedding problem (1) is locally solvable for each $\mathfrak{p}$ then it is globally solvable. For a given G_K-module A the Local-Global-Principle may hold or may not hold. Our result in this note is

Theorem 1 *For every global field K of characteristic $\neq 2$ and any given $m \geq 3$ there exists a G_K-module A of order 2^m such that the Local-Global-Principle $\mathsf{LGP}(A, K)$ does not hold.*

Remark: The modules A to be constructed will be cyclic groups of order 2^m with the action of G_K defined suitably. If 2 is replaced by a prime number $p > 2$ then the situation is completely different. For, if G_K acts on a cyclic group A of order p^m with $p > 2$ then the Local-Global-Principle $\mathsf{LGP}(A, K)$ does hold (irrespective of the characteristic of the field K). This is a consequence of Gudrun Beyer's theorem. (See Corollary 6 below.) The exceptional role of the prime 2 in this context is a consequence of the difference in the structure of the automorphism group of cyclic groups of p-power order p^m. If $p > 2$ then the automorphism group is cyclic whereas if $p = 2$ this is not the case for $m \geq 3$. In this respect the situation here is similar to the situation of the Grunwald-Wang theorem. (See [2].)

Concerning the characteristic hypothesis in Theorem 1, this is necessary if one wishes to construct counter examples to the Local-Global-Principle by means of cyclic groups A, as we do in this paper. If K is of characteristic 2 and A is a cyclic group of 2-power order with any action of G_K then the $\mathsf{LGP}(A, K)$ holds. This is a consequence of Witt's theorem that for a global field K of characteristic 2 the maximal pro-2-factor group of G_K is free in characteristic 2 (and similarly for any non-zero characteristic). I do not know whether non-cyclic groups A can serve as counter examples to the Local-Global-Principle.

2 The setting

Let me first recall some of the results in Hoechsmann's paper.

The solvable embedding problems (1) form a subgroup of $H^2(G, A)$, and this is precisely the kernel of the inflation map

$$\inf : H^2(G, A) \to H^2(G_K, A)\,. \tag{3}$$

(Note that the inflation map is well defined since the kernel of $G_K \to G$ acts trivially on A.) This holds for any base field K, hence also for the localizations. Now, every element in $H^2(G_K, A)$ is the inflation of some element in $H^2(G, A)$ for a suitable finite factor group G. We conclude:

Proposition 2 *The Local-Global-Principle* $\mathsf{LGP}(A, K)$ *holds if and only if the map*

$$H^2(G_K, A) \xrightarrow{h} \prod\nolimits_{\mathfrak{p}} H^2(G_{K_\mathfrak{p}}, A) \tag{4}$$

is injective.

At this point Hoechsmann cites the duality theorem of Tate-Poitou for global fields. That duality theorem holds if the order of A is relatively prime to the characteristic of K (including the case of characteristic 0) which we assume henceforth. Let $\widehat{A}$ denote the dual G_K-module of A. It consists of the characters χ of A, i.e., the homomorphisms of A into the multiplicative group of the algebraic closure of K. The action of G_K on $\widehat{A}$ is given by

$$\chi^\sigma(a) = \Big(\chi(a^{\sigma^{-1}})\Big)^\sigma \qquad\qquad (a \in A\,, \sigma \in G_K)\,. \tag{5}$$

Note that in this formula σ acts twofold: First σ^{-1} acts on A since A is a G_K-module. Secondly, σ acts on the character values since σ is an automorphism of the algebraic closure of K. In Hasse's terminology, this is a "crossed action" of G_K on $\widehat{A}$.

Now, the Tate-Poitou duality theorem asserts that for a global field K, the map h in (4) is dual to the following map:

$$H^1(G_K, \widehat{A}) \xrightarrow{j} \prod\nolimits_{\mathfrak{p}} H^1(G_{K_\mathfrak{p}}, \widehat{A}) \tag{6}$$

In particular, h is injective if and only if j is injective. We obtain:

Corollary 3 *The Local-Global-Principle* $\mathsf{LGP}(A, K)$ *holds if and only if the map j in* (6) *is injective.*

By this result, the problem is transferred from cohomological dimension 2 to dimension 1. This is the starting point of Hoechsmann. First he reduces the problem to a finite factor group of G_K.

Proposition 4 *Let G be the action group of the G_K-module $\widehat{A}$, i.e., the factor group of G_K modulo the normal subgroup which fixes $\widehat{A}$ elementwise. Then $\mathsf{LGP}(A,K)$ holds if and only if the map*

$$H^1(G,\widehat{A}) \xrightarrow{j_G} \prod_{\mathfrak{p}} H^1(G_{\mathfrak{p}},\widehat{A}) \tag{7}$$

is injective. [1]

Here, $G_{\mathfrak{p}}$ denotes the decomposition group of $\mathfrak{p}$ in G, i.e., the image of $G_{K_{\mathfrak{p}}}$ in G.

Proof:

(i) First we consider the case when $G = 1$, i.e. G_K acts trivially on $\widehat{A}$. In this case it is asserted that the $\mathsf{LGP}(A,K)$ holds, i.e., that the map j in (6) is injective. Now, in case of trivial action we have $H^1(G_K,\widehat{A}) = \mathrm{Hom}(G_K,\widehat{A})$. Every homomorphism $f : G_K \to \widehat{A}$ factors through a finite, abelian factor group $\overline{G}$ of G_K. Let $\overline{\sigma} \in \overline{G}$. Using Chebotarev's density theorem we conclude that there exists a prime $\mathfrak{p}$ of K whose decomposition group contains $\overline{\sigma}$. Hence, if f vanishes on all decomposition groups then $f(\overline{\sigma}) = 0$. Since this holds for all $\overline{\sigma}$ we conclude $f = 0$.

(ii) Now consider the general case. Let L be the finite Galois extension of K corresponding to G, so that G is the Galois group of $L|K$. Consider the commutative diagram:

$$\begin{array}{ccccccc}
0 \longrightarrow & H^1(G,\widehat{A}) & \xrightarrow{\text{inf}} & H^1(G_K,\widehat{A}) & \xrightarrow{\text{res}} & H^1(G_L,\widehat{A}) \\
& \downarrow{\scriptstyle j_G} & & \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle j_L} \\
0 \longrightarrow & \prod_{\mathfrak{p}} H^1(G_{\mathfrak{p}},\widehat{A}) & \longrightarrow & \prod_{\mathfrak{p}} H^1(G_{\mathfrak{p}},\widehat{A}) & \xrightarrow{\text{res}} & \prod_{\mathfrak{p}} H^1(G_{L,\mathfrak{p}},\widehat{A})
\end{array} \tag{8}$$

with self-explaining notations. The rows are exact. The vertical arrow j_L on the right hand side is injective by (i), for G_L acts trivially on $\widehat{A}$. Consequently, if the arrow j_G on the left hand side is injective then j in the middle is injective too, and conversely.

Corollary 5 *As in Proposition 4 let G denote the action group of G_K on $\widehat{A}$. If the group indices $[G : G_{\mathfrak{p}}]$ of the decomposition groups have greatest common divisor 1 then $\mathsf{LG}(A,K)$ holds.*

For, let $c \in H^1(G,\widehat{A})$. If c vanishes at $\mathfrak{p}$, i.e., if $\mathrm{res}_{G_{\mathfrak{p}}}(c) = 0$ then it follows $[G : G_{\mathfrak{p}}] \cdot c = 0$. If this holds for all $\mathfrak{p}$ then $c = 0$, provided the indices $[G : G_{\mathfrak{p}}]$ have greatest common divisor 1.

Corollary 6 *If the action group G of G_K on $\widehat{A}$ is cyclic then $\mathsf{LGP}(A,K)$ holds.*

[1] This proposition and the following corollaries remain valid for any finite factor group G of G_K modulo a normal subgroup which acts trivially on $\widehat{A}$.

For, if G is cyclic then by Chebotarev's density theorem there exists $\mathfrak{p}$ with $G_{\mathfrak{p}} = G$.

Corollary 6 is the theorem of Gudrun Beyer. It is remarkable that the validity of $\mathsf{LGP}(A, K)$ depends on the action of G_K on the dual $\widehat{A}$, not on A itself. This has been discovered by Gudrun Beyer. For corollary 5 Hoechsmann cites Demuškin and Šafarevič.

3 Hoechsmann's theorem

From now on we assume that A is a cyclic group. After decomposing A into its Sylow components we may assume that the order of A is a prime power, $|A| = p^m$. Its dual $\widehat{A}$ is also a cyclic group and $|\widehat{A}| = p^m$ too. If $p > 2$ then the automorphism group of $\widehat{A}$ is cyclic and it follows that G is cyclic, hence $\mathsf{LGP}(A, K)$ holds by Gudrun Beyer's theorem (Corollary 6).

Consequently, in looking for a counter example to $\mathsf{LGP}(A, K)$ we have to take $p = 2$. (This implies that K is of characteristic $\neq 2$ since the order of A is supposed to be relatively prime to the characteristic of K.) The G_K-module A should be a cyclic group such that the action group G on $\widehat{A}$ is non-cyclic. In particular $m \geq 3$. If there exists a prime $\mathfrak{p}$ of K with $G_{\mathfrak{p}} = G$ then by corollary 5 we have that $\mathsf{LGP}(A, K)$ holds. We conclude:

Let A be a G_K-module which is a cyclic group of prime power order p^m. If the Local-Global-Principle $\mathsf{LG}(A, K)$ does not hold then the following conditions are satisfied:

1. $p = 2$.
2. The action group G of G_K on $\widehat{A}$ is non-cyclic, hence $m \geq 3$.
3. For every prime $\mathfrak{p}$ of K, the decomposition group $G_{\mathfrak{p}}$ is a proper subgroup of G.

Now we can formulate Hoechsmann's theorem:

Theorem 7 *The conditions* 1–3 *above are not only necessary but also sufficient for A to be a counter example to* $\mathsf{LGP}(A, K)$.

In view of Proposition 4 this is an immediate consequence of the following group theoretical observation. For simplicity we write X instead of $\widehat{A}$.

Lemma 8 *Let X be a cyclic group of order 2^m $(m \geq 3)$ and G a non-cyclic group of automorphisms of X. Then there exists $0 \neq c \in H^1(G, X)$ such that its restriction $\operatorname{res}_H(c)$ vanishes for every maximal subgroup $H \subsetneqq G$.*

Proof: We identify $X = \mathbb{Z}/2^m$ (additively) and G with a group of units in $(\mathbb{Z}/2^m)^\times$. The action of G on X is given by multiplication. Any element in $H^1(G, X)$ can be represented by a crossed homomorphism $f : G \to X$. The functional equation of a crossed homomorphism is

$$f(\sigma\tau) = \tau f(\sigma) + f(\tau) \qquad \text{for} \qquad \sigma, \tau \in G. \tag{9}$$

In particular, for $\sigma = \tau$ we note that

$$f(\sigma^2) = (\sigma + 1) f(\sigma) \,. \tag{10}$$

We shall prove the lemma by explicitly exhibiting a crossed homomorphism f representing c.

The non-cyclic group G is a direct product

$$G = \langle -1 \rangle \times \langle u \rangle$$

where $u \neq 1$ is a certain unit of X which can be assumed to be $u \equiv 1 \bmod 4$. (If this should not be the case then we replace u by $-u$.) Let k be the exact exponent by which 2 appears in $u - 1$, so that

$$u - 1 = 2^k \lambda$$

where λ is not divisible by 2, hence a unit in X. We have

$$2 \leq k \leq m - 1 \,.$$

(If k would be $\geq m$ then $u \equiv 1 \bmod 2^m$, contradicting the fact that $u \neq 1$ as operator on X.) The group theoretical meaning of k is the following:

The group $2^{m-k}X$ consists precisely of those elements of X which are fixed by u.

For, the relation $ux \equiv x \bmod 2^m$ is equivalent to $(u-1)x \equiv 0 \bmod 2^m$ which, by definition of k, means $x \equiv 0 \bmod 2^{m-k}$.

Every crossed homomorphism $f : G \to X$ is already determined by its values on the generators -1 and u of G. We claim that there is a crossed homomorphism f with the values

$$f(-1) = 2^{m-k} \,, \qquad f(u) = 0 \tag{11}$$

and that its class $c \in H^2(G, X)$ satisfies the requirements of the lemma.

First we consider the subgroup $\langle -1 \rangle$ of G of order two. Consider the function $f_0 : \langle -1 \rangle \to X$ given by the values $f_0(-1) = 2^{m-k}$, $f_0(1) = 0$. This is a crossed homomorphism. To verify this one has to check the validity of (10) for $\sigma = -1$ only. Indeed, we have

$$f_0((-1)^2) = (-1 + 1) 2^{m-k} = 0 = f_0(1) \,.$$

We have the exact sequence

$$1 \to \langle u \rangle \longrightarrow G \longrightarrow \langle -1 \rangle \to 1 \,.$$

As observed above, the value $f_0(-1) = 2^{m-k}$ is fixed by u. Hence we may extend $f_0 : \langle -1 \rangle \to X$ by inflation to a crossed homomorphism $f : G \to X$ such that its values $f(\sigma)$ depend on the residue class of σ modulo $\langle u \rangle$ only. This crossed homomorphism satisfies (11).

Let $c \in H^1(G, X)$ denote the class of f. We claim that the restriction of c to every maximal subgroup of G vanishes. There are three maximal subgroups of G, namely the two cyclic groups $\langle u\rangle$ and $\langle -u\rangle$, and the group $\langle -1, u^2\rangle$ which in general is not cyclic except if $u^2 = 1$ (which means $k = m-1$).

The restriction of c to $\langle u\rangle$ vanishes since $f(u) = 0$ by (11).

As to the restriction of c to $\langle -u\rangle$ we first note that $f(-u) = f(-1) = 2^{m-k}$ does not vanish. But consider a crossed homomorphism $g : G \to X$ belonging to the same class c as f, which means that

$$g(\sigma) = f(\sigma) + (\sigma - 1)x \qquad (\sigma \in G) \tag{12}$$

for some $x \in X$. Can we choose $x \in X$ such that $g(-u) = 0$? This means

$$f(-u) = 2^{m-k} = -(-u-1)x = (u+1)x\,.$$

Since $u \equiv 1 \bmod 4$ we have $u + 1 \equiv 2 \bmod 4$ hence $u + 1 = 2\mu$ with μ a unit in X. Hence by choosing $x = \mu^{-1}2^{m-k-1}$ we indeed have $g(-u) = 0$.

Can we choose x such that g vanishes on the third maximal group $\langle -1, u^2\rangle$? This means, firstly, $g(-1) = 0$ and thus

$$f(-1) = 2^{m-k} = -(-1-1)x = 2x \tag{13}$$

and so we take $x = 2^{m-k-1}$. Secondly, the condition $g(u^2) = 0$ requires that

$$f(u^2) = 0 = -(u^2-1)x = -(u-1)(u+1)x = -\lambda\mu \cdot 2^{k+1} \cdot x\,.$$

The same $x = 2^{m-k-1}$ as above satisfies this condition since $2^m x = 0$.

We have now shown that c vanishes if restricted to any of the three maximal subgroups of G. It remains to verify that $c \neq 0$ in $H^1(G, X)$. In other words: It is *not* possible to choose $x \in X$ such that $g(-1) = g(u) = 0$. Now the condition $g(-1) = 0$ implies by (13) that x is precisely divisible by 2^{m-k-1} (and not by a higher power of 2). On the other hand, the condition $g(u) = 0$ requires that

$$f(u) = 0 = -(u-1)x = -\lambda \cdot 2^k \cdot x$$

and hence x should be divisible by 2^{m-k}. Both these conditions are not compatible, and so $c \neq 0$.

4 Construction of counter examples

In the following we let A be a cyclic group of order 2^m with $m \geq 3$. We try to define a non-cyclic action of G_K on A such that condition 3 of Theorem 7 is satisfied. This will give a counter example to $\mathsf{LGP}(A, K)$. The main tool for this is the following

Lemma 9 *For any global field K there exists an abelian extension $L|K$ of prescribed 2-power degree 2^{r+1} whose Galois group $G = \mathrm{Gal}(L|K)$ has the structure*

$$G \approx \mathbb{Z}/2 \times \mathbb{Z}/2^r\,,$$

and such that for every prime $\mathfrak{p}$ of K its decomposition group $G_{\mathfrak{p}}$ is a proper subgroup of G.

There are many possibilities to construct such a field extension. First assume that K is a number field. Consider the field $K^{(2)}$ of 2-power roots of unity over K. Its Galois group is either a free cyclic pro-2-group (for instance if $\sqrt{-1} \in K$) or else it is the direct product of such a group with a group of order 2. In any case the Galois group of $K^{(2)}|K$ contains finite cyclic factor groups of arbitrary large 2-power order. Accordingly let $L_0|K$ be a cyclic extension of degree 2^r which is contained in $K^{(2)}$. We observe that the only primes $\mathfrak{p}$ of K which are ramified in L_0 (if there are any) are divisors of 2. This follows from the fact that 2 is the only prime number in $\mathbb{Q}$ which is ramified in $\mathbb{Q}^{(2)}$.

Now we take a rational prime number $p > 2$ such that

$$p \equiv 1 \bmod 2^N \tag{14}$$

for sufficiently large N and put

$$L = L_0(\sqrt{p})\,.$$

If N and hence p is sufficiently large then p is unramified in K, i.e., every prime divisor $\mathfrak{p}|p$ appears in p with the exponent 1. We conclude that $\sqrt{p} \notin K$, and that $\mathfrak{p}$ is ramified in the quadratic extension $K(\sqrt{p})$. Therefore $K(\sqrt{p})$ is not contained in L_0, and $K(\sqrt{p})$ is linearly disjoint to L_0 over K. The Galois group G of $L|K$ is the direct product of $\mathrm{Gal}(L_0|K)$ (which is cyclic of order 2^r), with $\mathrm{Gal}(K(\sqrt{p})|K)$ (which is of order 2).

Let $\mathfrak{p}$ be a prime of K and $G_\mathfrak{p}$ its decomposition group in G. If $\mathfrak{p}$ is unramified in L (including the case when $\mathfrak{p}$ is an infinite prime) then its decomposition group is cyclic and hence $G_\mathfrak{p}$ is a proper subgroup of G. If $\mathfrak{p}$ is ramified in L then either $\mathfrak{p}|2$ or $\mathfrak{p}|p$. In the first case, $\mathfrak{p}|2$, if $N \geq 3$ then (14) implies $\sqrt{p} \in \mathbb{Q}_2$, hence $\sqrt{p} \in L_{0,\mathfrak{p}}$, thus $L_\mathfrak{p} = L_{0,\mathfrak{p}}$ is of degree $\leq [L_0 : K] = 2^r$ over $K_\mathfrak{p}$. Hence its Galois group $G_\mathfrak{p}$ is of order $\leq 2^r$ and thus a proper subgroup of G. In the second case, $\mathfrak{p}|p$, let N be large enough such that L_0 is contained in the field of 2^N-th roots of unity over K. The condition (14) implies that $\mathbb{Q}_p$ contains the 2^N-th roots of unity, thus $L_0 \subset \mathbb{Q}_p \subset K_\mathfrak{p}$ and consequently $L_\mathfrak{p} = K_\mathfrak{p}(\sqrt{p})$ is of degree ≤ 2.

Now assume that K is a function field of characteristic $\neq 0$. Let k be its field of constants, and consider the unique extension k_0 of degree 2^r over k. We put $L_0 = Kk_0$; this is the constant field extension of K of degree 2^r. It is cyclic and unramified over K. Now let $t \in K$ be a separating variable. Consider a prime polynomial $p(t) \in k[t]$ with the condition that its residue field contains k_0. This condition is the analogue to condition (14) in the number field case. Since there are infinitely such polynomials we may assume that $p(t)$ is not ramified in K.

If the characteristic of K is $\neq 2$ then we put again

$$L = L_0(\sqrt{p(t)}\,)\,.$$

Quite analogous to the number field case it is seen that L satisfies the requirements of the lemma. The situation here is even easier since $L_0|K$ is unramified, hence it is not necessary here to discuss the prime divisors which are ramified in L_0, as we had to do in the number field case. The only primes $\mathfrak{p}$ of K which are ramified in L are the prime divisors of $p(t)$. For any such $\mathfrak{p}$ its residue field contains k_0 and hence its completion $K_{\mathfrak{p}}$ too contains k_0. It follows that $K_{\mathfrak{p}}$ contains $Kk_0 = L_0$ and therefore $L_{\mathfrak{p}} = K_{\mathfrak{p}}(\sqrt{p(t)})$ is of degree ≤ 2.

If the characteristic of K is 2 then $K(\sqrt{p(t)})$ is inseparabel and useless for our construction. Instead of a square root we have to use a root of the appropriate Artin-Schreier equation:

$$L = L_0(\alpha)\,, \qquad \alpha^2 - \alpha = \frac{1}{p(t)}$$

Again, the only primes of K which are ramified in L are the prime divisors of $p(t)$ and the discussion now proceeds as in the case of characteristic $\neq 2$.

Lemma 9 is proved. In that lemma we have not excluded the case of characteristic 2 because it is not necessary. However, in the following proof we have to assume that $\mathrm{char}(K) \neq 2$ in order to be able to apply Hoechsmann's theorem which is based on the Tate-Poitou duality theorem.

Proof of Theorem 1:

Let us put $X = \mathbb{Z}/2^m$. The automorphism group $\mathrm{Aut}(X)$ consists of the units in $\mathbb{Z}/2^m$ which act by multiplication. $\mathrm{Aut}(X)$ is non-cyclic and has the structure

$$\mathrm{Aut}(X) \approx \mathbb{Z}/2^{\,m-2} \times \mathbb{Z}/2\,.$$

We see that $\mathrm{Aut}(X)$ is isomorphic to the Galois group $G = \mathrm{Gal}(L|K)$ of the field extension of Lemma 9 if in that Lemma we take $r = m - 2$.

Let is fix an isomorphism $G \approx \mathrm{Aut}(X)$. In this way X becomes a G-module. X appears as a G_K-module via the projection $G_K \to G$. The action group of G_K on X is G.

Now we take $A = \widehat{X}$. Then A is a G_K-module of the same order 2^m as X. We have $\widehat{A} = \widehat{\widehat{X}} = X$. Thus the action group of G_K on $\widehat{A}$ is G. The conditions 1–3 of Theorem 7 are satisfied in view of Lemma 9. We conclude that A is a counter example to $\mathsf{LGP}(A, K)$.

Problem: Prove Hoechsmann's theorem directly, without reference to the Tate-Poitou duality theorem. It seems that the reciprocity law for global fields will be sufficient.

References

[1] Klaus Hoechsmann, *Zum Einbettungsproblem.* Journal für die Reine und Angewandte Mathematik 229 (1967) 81–106.

[2] Falko Lorenz, Peter Roquette, *On the theorem of Grunwald-Wang in the setting of valuation theory.* In: Kuhlmann, Franz-Viktor (ed.) et al., Valuation theory and its applications. Volume II. Proceedings of the international conference and workshop, University of Saskatchewan, Saskatoon, Canada, July 28-August 11, 1999. Providence, RI: American Mathematical Society (AMS). Fields Inst. Commun. (to appear)

More literature is cited in these papers.