Mathematical Journal of Okayama University

Volume 3, *Issue* 1 1953 *Article* 2

OCTOBER 1953

Necessary conditions for local class field theory

O. F. G. Schilling*

*University Of Chicago

NECESSARY CONDITIONS FOR LOCAL CLASS FIELD THEORY

(Remarks to a paper of M. Moriya)

O. F. G. SCHILLING

M. Moriya[1] has shown recently that the validity of the limitation theorem (stated briefly as "the norm class group of a normal extension equals the norm class group of its maximal abelian subfield") and of the isomorphism theorem for abelian extensions imply that the residue class field of the underlying field, which is assumed to be complete with respect to a discrete rank one valuation, has for each integer n precisely one extension which must be cyclic.

It is the object of those remarks to show that the full power of the above mentioned theorems of the local class field theory is not needed in order to establish the stated algebraic structure of the residue class field. The methods used here may be viewed as belonging to the *arithmetic decomposition theory of the 2-dimensional cohomology group* of a normal unramified extension of the base field. In order to be able to make direct references to the existing literature the terminology of the theory of algebras is used here, as it was employed in some earlier work[2].

The following theorem will be proved:

Suppose that the field F is complete with respect to a discrete rank one valuation. Then the following assumptions imply that the residue class field of F with respect to the given valuation is perfect and has for every integer n precisely one extension of degree n.

A. *There exist for each prime power p^m cyclic extensions Z/F of degree p^m whose corresponding norm class group F^*/NZ^* contains a class of precise order p^m.*

B. *If k is a finite extension over F and K is a cyclic unramified extension of prime degree p, or an abelian extension of type (p, p), then the norm class group k^*/NK^* is isomorphic to the Galois group of K/k. This hypothesis holds for all primes p.*

In turn it is to be noted that the indicated properties of the

(1) M. Moriya, Eine notwendige Bedingung für die Gültigkeit der Klassenkörpertheorie im Kleinen, Math. Jour. Okayama Univ., **2** (1952), 13 - 20.

(2) See for example, O. F. G. Schilling, The theory of valuations, Math. Surveys, **6** (1950), in particular chapters 5 and 6.

residue class field imply that all standard theorems of the local class field theory hold, naturally with proper modifications for the existence theorem. In particular the strong form of the limitation thorem is valid, i.e., $F^*/NK^* = F^*/N_0K_0^*$ for the respective norm class groups of a finite normal extension K/F and its maximally abelian subfield K_0.

Although the latter theorem implies easily, if taken as a hypothesis, the algebraic structure of the residue class field, there is some advantage to the formulation of the present theorem with the conditions A and B since only *minor* parts of the 2-dimensional cohomology theory are assumed as axioms. In other words, one may, using the full force of the cohomology theory of non-abelian extensions[3], derive first the strong form of the limitation theorem on the basis of hypotheses A and B and then prove the present theorem as an additional concluding remark.

Suppose then that F is a field which is complete with respect to a discrete rank one valuation[4]. The residue class field of F with respect to this valuation shall be denoted by F'. Furthermore F^* shall denote the multiplicative group of F, and t shall denote an arbitrary, but fixed, prime element of F with respect to the given valuation.

The preceding notation for the passage to the residue class field and the multiplicative group shall also be used for finite algebraic extensions $k \supseteq F$ which in turn are complete with respect to the unique prolongations of the given valuation.

1. *The existence of cyclic unramified extensions.*

Lemma 1. *Suppose that $p \neq 0$ is the characteristic of F'. If $[k^* : NZ^*] = p$ for cyclic unramified extensions Z/k of degree p over arbitrary finite extensions k/F, then F' is perfect.*

Proof. We distinguish two cases; (i) F has characteristic 0 and (ii) F has characteristic p. In the first case suppose that $F'(A') \supset F'$ is an inseparable extension of degree p over F' with $A'^p = a' \in F'$. We pick any unit $a \in F$ in the residue class a' and consider the extension $k(A)$ for $A^p = a$ where $k = F(\zeta)$, ζ a primitive p-th root of

(3) See especially the recent work of G. Hochschild, T. Nakayama and J. Tate in the Annals of Mathematics.

(4) For properties of complete fields see loc. cit. (2), in particular chapter 3 for the theory of inertial extensions.

unity. Then $k(A) = Z$ is a cyclic unramified extension of degree p over k, and the hypothesis implies that every unit of k is the norm of some unit in Z.

In the second case we consider the equation $x^p - tx - a = 0$ where a is determined as before. Now let N be the splitting field of this equation. Then $[N:F] \mid p!$. We pick next a Sylow subfield $k \subset N$ so that $[N:k] = p$. We note that $([k:F], p) = 1$. Furthermore a root of the given equation generates N over k, thus N/k is unramified. Again we apply the hypothesis of the lemma and see that all units of k are norms of units in the cyclic unramified extension N/k.

But now the reasoning of M. Moriya[5] may be applied to show the existence of 1-units in k which are not norms of units in Z and N, respectively. Thus F' must be perfect.

Lemma 2. *If $[k^* : NZ^*] = p$ holds for all cyclic unramified extensions Z/k of prime degree p over arbitrary unramified extensions k/F, then F' cannot be the center of a finite dimensional division algebra.*

Proof. Suppose that D' is a central division algebra over F'. Then $D' \sim (U'/F', G, u'_{S,T})$ where U'/F' is a normal extension with the Galois group G and $u'_{S,T}$ is a suitable factor set[6]. Consequently there exists an essentially unique division algebra $D \sim (U/F, G, u_{S,T})$ for an unramified normal extension U/F with the residue class field U', the Galois group G, and a factor set of units $u_{S,T} \in u'_{S,T}$. Suppose that the prime p divides the index of D. Next the hypothesis of the lemma can be applied to the cyclic intermediate fields Z/k between U and a p-Sylow subfield W with $([W:F], p) = 1$, so as to show that all units of k are norms of units in Z. Consequently $D \times Z \sim Z$ will imply $D \times k \sim k$, and will ultimately give $D \times W \sim W$ which contradicts the assumption on p. Note that the factor sets can be chosen at each cyclic step to be equivalent to units, because the algebra D and its coefficient extensions are unramified.

Lemma 3. *If the hypothesis of* Lemma 2 *holds and if there exists a cyclic extension Z/F of prime power degree p^m for which F^*/NZ^* contains a class of precise order p^m, then F has a cyclic unramified extension U of degree p^m.*

(5) See loc. cit. (1), proof of Theorem 2, pp. 16 - 17.

(6) See for example, T. Nakayama, Divisionsalgebren über diskret bewerteten perfekten Körpern, Jour. Reine u. Angew. Math., **178** (1937), 11 - 13.

Proof. Suppose that the class $f \cdot NZ^*$ has precise order p^m. Then f is the factor set of a division algebra D/F of degree p^m. Next we observe that $D \sim (U/F, S, t)^r$ with a cyclic unramified extension U/F whose Galois group is generated by S, where $(r, [U:F]) = 1$, since the representation of D as the Kronecker product of a ramified algebra with an unramified algebra has the latter factor equivalent to F by virtue of Lemma 2. Consequently $[U:F] = p_1^m$, for D has the exponent p^m.

Remark 1. If it is assumed that F has a completely ramified cyclic extension Z/F of degree n, for which the norm factor group F^*/NZ^* has an element of precise order n, then there exists an unramified cyclic extension U/F of degree n.

For the proof we select a division algebra D as in the proof of Lemma 3. Then $D \sim (U/F, S, t)^r \times (W/F, G, u_{R,T})$ where (i) W/F is an unramified normal extension with the Galois group $G = \{R, T, \cdots\}$, (ii) $u_{R,T}$ is a factor set of units, (iii) U is a cyclic subfield of W, and (iv) $(r, [U:F]) = 1$. Since Z is a maximally commutative subfield of D, the hypothesis for Z implies that the ramification degree of D is at least equal to n. On the other hand the ramification degree of the Kronecker product on the right side of the above similiarity relation is at most equal to $[U:F]$[7]. Consequently $n \mid [U:F]$.

Remark 2. The preceding remark shows that there exist unramified cyclic extensions of prime degree p provided there exist cyclic extensions of degree p.

If p is the characteristic of F' then it will follow from the theory of cyclic extensions of degree p^m that there will necessarily exist cyclic extensions U'/F' of degree p^m[8]. The theory of inertial extensions then establishes unramified cyclic extensions U/F with the residue class fields U'/F'.

If p is distinct from the characteristic of F' and if all p-th roots of unity lie in F, then the validity of the isomorphism theorem $F^*/NZ^* \cong G(Z/F)$ for cyclic extensions of degree p^m implies the existence of unramified cyclic extensions of degree p^m.

The proof for this statement follows by induction. By the beginning of this remark there exists a cyclic extension U_1' of degree p over F'. Let U_1 be a cyclic unramified extension over F with the

(7) See (6) loc. cit.

(8) See for example, A. A. Albert, Cyclic fields of degree p^n over F of characteristic p, Bull. Am. Math. Soc., **40** (1934), 625 - 631, Lemma 7 on p. 629.

residue class field U_1'. Then the assumption on the norm class group implies that every unit of F, and thus every non-zero element of F', is a norm. In particular a primitive p-th root of unity in F and F', respectively, is a norm. But then U_1' can be imbedded into a cyclic extension U_2' of degree p^2 over F'[9]. This cyclic extension is in turn the residue class field of a cyclic extension U_2/F of degree p^2. Again the hypothesis on the norm class group implies that a primitive p-th root of unity is the norm of an element in U_2'. Complete induction from p^m to p^{m+1} thus finishes the proof.

This shows in particular for $p = 2$ that the validity of the isomorphism theorem implies $-1 = a'^2 + b'^2$ with $a', b' \in F'$.

Finally we note that the existence of a cyclic unramified extension of prime degree p will automatically imply the existence of cyclic unramified extensions of any prime power degree p^m if all p^{m+1}-th roots of unity lie in F and F', respectively. For then the primitive p-th roots of unity are always p^m-th powers, and induction shows that a cyclic extension U_m' of degree p^m can be imbedded in a cyclic extension U_{m+1}' of degree p^{m+1}.

2. *The uniqueness of unramified extensions.*

Lemma 4. *If, in addition to the hypothesis of* Lemma 3, *the isomorphism theorem* $k^*/NK^* \cong G(K/k)$ *holds for abelian extensions* K/k *whose Galois groups are direct products of two cyclic groups of prime order* p, *for arbitrary finite extensions* k/F, *then there exists precisely one cyclic unramified extension* U/F *of degree* n *for every integer* n.

Proof. Suppose that U_1 and U_2 were distinct cyclic unramified extensions of prime degree p over a finite extension $k \supseteq F$. Then the composite U_1U_2/k is an abelian extension of the type described in the lemma. On the other hand the norm class group of U_1U_2 with respect to k contains the cyclic subgroup of order p^2 which is generated by the coset of a prime element of k, since U_1U_2/k is unramified. Hence U_1 cannot be distinct from U_2.

Suppose next that K is an arbitrary normal unramified extension of F. Let $p \mid [K:F]$ and suppose that L is a p-Sylow subfield of K/F. Let M be the maximal subfield of K/L whose Galois group is a direct product of cyclic groups of order p. Then the exponent e

(9) See A. A. Albert, Modern higher algebra, Univ. of Chicago Press (1937), chapter IX, §6, Theorem 11, pp. 207 - 208.

in $[M:L]=p^e$ is the minimum number of generators of the group of K/L[10]. By the first part of this proof we must have $e=1$. Therefore the Sylow subgroup in question is cyclic.

This fact holds for every prime p dividing $[K:F]$, consequently the Galois group of K/F is metabelian, and we have $F \subseteqq k \subseteq K$ where K/k and k/F are cyclic with the respective degrees u and v for which $(u, v)=1$[11].

Finally, we apply Lemma 3 and take Z/F to be a cyclic unramified extension of degree u. Then K and the composite kZ are cyclic unramified extensions of degree u over k. The first part of the proof implies then that necessarily $kZ=K$. Thus K/F is cyclic as asserted. And this fact in turn implies the asserted uniqueness.

Remark 3. The preceding lemmas and the theorem remain valid if F is replaced by a field which is relatively complete with respect to a discrete rank one valuation[12]. One only has to notice that the field F and its completion have the same algebraic properties, that is, there exists a 1-1 correspondence between the distinct algebraic extensions of F and those of its completion.

UNIVERSITY OF CHICAGO

(*Received June 10, 1953*)

(10) See for example, H. Zassenhaus, The theory of groups, Chelsea Publishing Co. (1949), chapter IV, §3, p. 111.

(11) See loc. cit. (10), chapter V, §3, Theorem 11, p. 145.

(12) See for example, (2) loc. cit. chapter 2, §7, and chapter 6, §11. Also Eizi Inaba, Note on relatively complete fields, Natural Sci. Rep. Ochanomizu Univ., **3** (1952), 5-9.