NOTE ON AN ORDERING THEOREM FOR SUBFIELDS

TADASI NAKAYAMA

In a recent paper [3] Tannaka gave an interesting ordering theorem for subfields of a $\mathfrak{p}$-adic number field. The purpose of the present note[1] is firstly to observe, on modifying Tannaka's argument a little, that his restriction to those subfields over which the original field is abelian may be removed and in fact the theorem holds for arbitrary fields which are not $\mathfrak{p}$-adic number fields, indeed in a much refined form, and secondly to formulate a similar ordering theorem for algebraic number fields in terms of idèle-class groups in place of element groups.

1. Let K be a field, and let k_1, k_2 be two subfields of K such that K is finite and separable over $k_1 \cap k_2$. Put

$$M_1 = \{\xi \in K;\ N_{K/k_1}(\xi) = 1\}, \quad M_2 = \{\xi \in K;\ N_{K/k_2}(\xi) = 1\}.$$

THEOREM 1. *If* $k_1 \subseteq\!\!\!\!/\ k_2$ *then* (*and only then*) $M_1 \subseteq\!\!\!\!/\ M_2$. *Indeed, provided that K has infinitely many elements, the index* $(M_1M_2 : M_1)$ *is, then, infinite and, moreover the orders of elements of* M_1M_2/M_1 *are not bounded.*

Proof. We borrow an argument of Tannaka, but generalize as well as refine it so as to make it suitable for our generalized and refined formulation. Set namely $n_1 = (K : k_1)$, $n_2 = (K : k_2)$. Let θ be a generating element of K over $k_1 \cap k_2$. We denote by $\theta_1 = \theta, \theta_2, \ldots, \theta_{n_1}$ its n_1 conjugates with respect to k_1, while we denote its n_2 conjugates with respect to k_2 by $\theta^{(1)} = \theta, \theta^{(2)}, \ldots, \theta^{(n_2)}$.

$$f(x) = (x - \theta^{(1)})(x - \theta^{(2)}) \ldots (x - \theta^{(n_2)})$$

is the irreducible polynomial in k_2 satisfied by θ. Let α be an arbitrary element of $k_1 \cap k_2$. Then $f(\alpha) = N_{K/k_2}(\alpha - \theta)$, whence

$$N_{K/k_2}(f(\alpha)/(\alpha - \theta)^{n_2}) = 1$$

provided $\alpha \neq \theta$, which is certainly the case when $K \neq k_1 \cap k_2$ as we may assume in our proof.

Suppose now that the orders of elements of the factor group M_1M_2/M_1 are

Received January 17, 1952.

[1] The writer wants to thank Mr. M. Nagata for his kind intervention during the present study.

https://doi.org/10.1017/S0027763000023096 Published online by Cambridge University Press

bounded and thus all divide a certain natural number, say t. Then $f(\alpha)^t/(\alpha-\theta)^{n_2t}\in M_1$. If $f_1(x)=f(x), f_2(x), \ldots, f_{n_1}(x)$ are n_1 conjugates of $f(x)$ with respect to k_1, then $f_1(\alpha)^t f_2(\alpha)^t \ldots f_{n_1}(\alpha)^t/(\alpha-\theta_1)^{n_2t}(\alpha-\theta_2)^{n_2t}\ldots(\alpha-\theta_{n_1})^{n_2t}=1$ and the polynomial

$$f_1(x)^t f_2(x)^t \ldots f_{n_1}(x)^t-(x-\theta_1)^{n_2t}(x-\theta_2)^{n_2t}\ldots(x-\theta_{n_1})^{n_2t}$$

has α as its root. Since this is the case with arbitrary element α in $k_1\cap k_2$, the polynomial must be 0 provided that (K whence) $k_1\cap k_2$ has infinitely many elements, which we shall assume for meanwhile. Hence the roots $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n_2)}$ of $f_1(x)=f(x)$ all appear mong $\theta_1, \theta_2, \ldots, \theta_{n_1}$. Thus every $\theta^{(i)}$ coincides with one of θ_j and every isomorphism $\theta\to\theta^{(i)}$ of $K/k_1\cap k_2$ (into a conjugate field) leaving k_2 elementwise fixed is an isomorphism of K/k_1. It follows that $k_1\subseteqq k_2$.

The case when K is a finite field is rather evident. For then M_1 consists of $(K^*:1)/(k_1^*:1)$ elements, where K^*, k_1^* are the multiplicative groups of K, k_1; observe that every element of k_1 is a norm of K/k. Similarly M_2 contains exactly $(K^*:1)/(k_2^*:1)$ elements. If $M_1\supseteqq M_2$, then $(k_1^*:1)$ divides $(k_2^*:1)$, or, $l^{m_1}-1$ divides $l^{m_2}-1$, where l^{m_1}, l^{m_2} are the numbers of elements in k_1 and k_2 respectively, l being a prime number. This implies that m_1 divides m_2, as we readily see, and thus $k_1\subseteqq k_2$.

Remark 1. Suppose, in our theorem, k_2 has only a finite number of roots of unity. Then M_1M_2/M_1 has, in case $k_1\not\subseteqq k_2$ and K is infinite, an element of infinite order. For, the operation N_{K/k_1} maps M_1M_2/M_1 isomorphically into the multiplicative group k_1^* of k_1. Elements of finite order in M_1M_2/M_1 are mapped then onto roots of unity. Since $(M_1M_2:M_1)$ is infinite, there must exist an element of infinite order, if k_2 has only a finite number of roots of unity.

Remark 2. The same is the case also if K has an uncountably infinite number of elements, even when K (whence k) has infinitely many roots of unity. In fact, there are then infinitely many[2] mutually independent elements of infinite order in M_1M_2/M_1. For, otherwise there would exist an infinite family $\{\alpha_i\}$ of elements in $k_1\cap k_2$ such that $N_{K/k_1}(f(\alpha_i)/(\alpha_i-\theta)^{n_2})$ are all equal to a single element γ of k_1. Then $f_1(x)f_2(x)\ldots f_{n_1}(x)-\gamma(x-\theta_1)^{n_2}(x-\theta_2)^{n_2}\ldots(x-\theta_{n_1})^{n_2}$ would vanish identically, whence $k_1\subseteqq k_2$.

Remark 3. Our assumption that (both K/k_1 and K/k_2, or) $K/k_1\cap k_2$ be separable may be weakened to that K/k_2 be separable. As a matter of fact, the condition $k_1\not\subseteqq k_2$ may be replaced generally by $k_1'\not\subseteqq k_2'$, where k_1', k_2' are the maximal purely inseparable subfields of K/k_1, K/k_2.

[2] As many as the power of K.

2. Let now k_0 be the p-adic completion of the rational number field, p being a prime number, and let K, k_1, k_2 be finite extensions of k_0 such that $K \supseteqq k_1$, k_2. Our Theorem 1 and Remarks 1, 2 naturally apply to these K, k_1, k_2. The result may be interpreted as follows in terms of the full abelian extensions A_{k_1}, A_{k_2} over k_1, k_2 (in a certain algebraic closure of K).

THEOREM 2. *If $k_1 \not\subseteqq k_2$ then (and only then) A_{k_1} is not contained in KA_{k_2} and $KA_{k_1}A_{k_2}$ is infinite over KA_{k_2} and, in fact, there exists a field X between $KA_{k_1}A_{k_2}$ and KA_{k_2} such that the (compact) Galois group of $KA_{k_1}A_{k_2}/X$ is homeomorphically isomorphic to the additive group of p-adic integers.*

Proof. Let A_K be the full abelian extension of K. The Galois group of A_K/K may be identified, by means of norm residue symbols, with the completion $\tilde{K}^*$ of the multiplicative group K^* of K topologized by subgroups of finite indices as neighborhoods of unity.[3] On the group of units in K the topology coincides with the one given by the valuation of K. As the transition theorem for norm residue symbols tells, an element of $\tilde{K}^*$ leaves A_{k_1} elementwise fixed if and only if its norm with respect to K/k_1 is unity. It is clear that such an element of $\tilde{K}^*$ is the limit of a sequence of units in K and is thus by itself a unit of K. It follows that the totality of such elements is simply our M_1. Thus M_1 is the subgroup of $\tilde{K}^*$ belonging to KA_{k_1} in the sense of Galois theory. Similarly M_2 belongs to KA_{k_2}, and $M_1 \cap M_2$ belongs to $KA_{k_1}A_{k_2}$. Thus $M_2/M_1 \cap M_2$ is the Galois group of $KA_{k_1}A_{k_2}/KA_{k_2}$. But $M_2/M_1 \cap M_2$, isomorphic to M_1M_2/M_1, contains an element of infinite order, by Theorem 1 and Remark 1 (or Remark 2). Consider the closed subgroup of $M_2/M_1 \cap M_2$ generated by such an element of infinite order. Because of the well known structure of K^*, it is easy to see that either this subgroup or its subgroup is the limit of a sequence of cyclic groups of order p^i (which is homeomorphically isomorphic to the (additive) group of p-adic integers).

3. Let us next turn to an algebraic number field K and its subfields k_1, k_2. It is needless to say that again Theorem 1 and Remark 1 apply to these fields. We may further obtain a similar theorem for multiplicative groups of idèles, in place of multiplicative groups of field elements. Let, for instance, $\mathfrak{P}$ be a (finite) prime in K such that we have $\bar{k}_1 \not\subseteqq \bar{k}_2$ for completions $\bar{k}_1$, $\bar{k}_2$ of k_1, k_2 with respect to $\mathfrak{P}$. Then there exists in the $\mathfrak{P}$-adic completion $\bar{K}$ of K an element ξ such that $N_{\bar{K}/\bar{k}_2}(\xi) = 1$ but $N_{\bar{K}/\bar{k}_1}(\xi^i) \neq 1$ for $i = 1, 2, \ldots,$ according to the $\mathfrak{P}$-adic case of Theorem 1 and Remark 1. Let a be the idèle of K whose $\mathfrak{P}$-component is ξ and whose other components are all 1. Then the idèle a satisfies a similar condition with respect to the operations N_{K/k_2} and N_{K/k_1}; if $\mathfrak{p}$ is the prime in $k_1 \cap k_2$ divisible by $\mathfrak{P}$, then decompose the regular represent-

[3] See for instance [1].

https://doi.org/10.1017/S0027763000023096 Published online by Cambridge University Press

ation of $K/k_1 \cap k_2$ into components belonging to different prime divisors of $\mathfrak{p}$ in K, $\mathfrak{P}$ being a one. Indeed, since there are infinitely many primes which satisfy our requirement ($\bar{k}_1 \not\supseteq \bar{k}_2$), it follows that there exists an infinite family of idèles in K whose norms with respect to K/k_2 are all 1 such that no (non-trivial) power-product of them has norm 1 with respect to K/k_1, even when we discard the possibility of constructing such a family with respect to a single prime $\mathfrak{P}$ accroding to Remark 2.

However, this argument of taking a prime $\mathfrak{P}$ with $\bar{k}_1 \not\supseteq \bar{k}_2$ is rather indirect. We may in fact apply Theorem 1 and Remark 1 directly to K, k_1, k_2, on considering them as subfields of (the semi-simple algebra) $K_\mathfrak{p}$ ($= K \times (k_1 \cap k_2)_\mathfrak{p}$ (over $k_1 \cap k_2$)), $\mathfrak{p}$ being a prime in $k_1 \cap k_2$, to obtain an element ξ of K ($\subseteq K_\mathfrak{p}$) such that $N_{K/k_2}(\xi) = 1$ but $N_{K/k_1}(\xi^i) \neq 1$ for $i = 1, 2, \ldots$. Consider then the idèle whose $\mathfrak{p}$-component (i.e. the product of components belonging to different prime divisors (in K) of $\mathfrak{p}$) is ξ and whose components belong to primes not dividing $\mathfrak{p}$ are all 1. Then this idèle has norm 1 with respect to K/k_2 while no power of it has norm 1 for K/k_1. Letting $\mathfrak{p}$ run over all primes in $k_1 \cap k_2$, we obtain an infinite family of such idèles which are independent in the sense as above. (As a matter of fact, if we apply the argument of Remark 2 to the semi-simple algebra $K_\mathfrak{p}/(k_1 \cap k_2)_\mathfrak{p}$ (generated by the same generating element θ as $K/k_1 \cap k_2$), as is allowed, we can construct a similar (even uncountable) infinite family with respect to each single prime $\mathfrak{p}$.)

We next turn to idèle-classes. However, the transition is rather easy. Since almost all components of each of the constructed idèles (in either construction) are 1, none of the norms for K/k or its powers is principal idèle. The same is the case for any of their power-products. Thus

THEOREM 3. *Let $\mathfrak{M}_1$, $\mathfrak{M}_2$ be the groups of idèles (idèle-classes) in K whose norms with respect to k_1, k_2, respectively, are unity idèle (idèle-class). If $k_1 \not\supseteq k_2$ then (and only then) $\mathfrak{M}_1 \not\supseteq \mathfrak{M}_2$ and $\mathfrak{M}_1\mathfrak{M}_2/\mathfrak{M}_1$ has infinitely many independent elements of infinite order.*

We observe further that the (idèle-)class of an idèle whose components at a finite number of (finite) primes are $\neq 1$ and whose other components are all 1 never belongs to the connected component of unity of the idèle-class group.[4)5)] This remark applies naturally to the above constructed idèles and their norms with respect to K/k_1, as well as to their power-products. Another remark is that our element of infinite order in $\mathfrak{M}_1\mathfrak{M}_2/\mathfrak{M}_1$ constructed with respect to $\mathfrak{p}$ generates a closed subgroup possessing a subgroup (homeomorphically)

4) The topology is the natural one employed by Artin, Dieudonné, Iwasawa, Weil and others; cf [4].

5) This can be seen by means of the (generalized) Dirichlet theorem and a theorem of Chevalley [2].

isomorphic to the additive group of p-adic integers, p being the rational prime divisible by $\mathfrak{p}$.

Now the Galois group of the full abelian extension A_K over K may be identified with the idèle-class group of K modulo its copmonent of unity, by virtue of the class field theory. On referring to the above remarks and to the latter of our above constructions, we have, by means of an argument similar to Theorem 2,

THEOREM 4. *Let A_{k_1}, A_{k_2} be the full abelian extensions of k_1, k_2. If $k_1 \subsetneqq k_2$ then (and only then) A_{k_1} is not contained in KA_{k_2} and indeed there exists for each prime number p a field X between $KA_{k_1}A_{k_2}$ and KA_{k_2} such that the Galois group of $KA_{k_1}A_{k_2}/X$ is (homeomorphically) isomorphic with the group of p-adic integers.*

Remark 4. Conversely, the idèle-class part of Theorem 3 may be derived from Theorem 4 too, because of the fact that the image by N_{K/k_2} of the component of unity in the idèle-class group of K is exactly the component of unity of the idèle-class group of k_2.[6]

Remark 5. Theorem 4 implies in particular that the extension $KA_{k_1}A_{k_2}/KA_{k_2}$ contains, in case $k_1 \subsetneqq k_2$, a (finite) cyclic extension of arbitrary given degree. However, we shall not try to study the possible types of infinite subfields of $KA_{k_1}A_{k_2}/KA_{k_2}$ (i.e. the possible types of infinite factor groups of $\mathfrak{M}_2/\mathfrak{M}_1 \cap \mathfrak{M}_2$ (of the idèle-class case) modulo the component of unity), since that would involve some complicated argument foreign to the straightforward ones of the present note, being here satisfied with our Theorem 4 which is sufficient for our purpose to see that $KA_{k_1}A_{k_2}$ is very much larger than KA_{k_2} (in case $k_1 \subsetneqq k_2$).

REFERENCES

[1] E. Artin, Algebraic Numbers and Algebraic Functions, New York 1951.

[2] C. Chevalley, Deux théorèms d'arithmétique, Jour. Math. Soc. Japan 3 (1951) (Takagi commemoration number).

[3] T. Tannaka, Some remarks concerning p-adic number field, ibid.

[4] A. Weil, Sur la théorie du corps de classes, ibid.

Nagoya University

[6] See Weil [4].