Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Phillip Ratner

An Isomorphism of Infinite Galois Theory

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **60** (1976), n.4, p. 385–387.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1976_8_60_4_385_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1976.

Algebra. — *An Isomorphism of Infinite Galois Theory.* Nota di PHILLIP RATNER, presentata (*) dal Corrisp. G. ZAPPA.

RIASSUNTO. — Viene costruito un esplicito isomorfismo tra due diverse descrizioni del gruppo di Galois relativo ad un ampliamento infinito di Galois di un campo finito.

Let k be a finite field with q elements, Ω an infinite Galois extension of k, $G = G(\Omega/k)$, and $\rho : x \rightarrow x^q$ the automorphism which generates a dense subgroup of G. For a given integer n, there is at most one extension of k of degree n in Ω, which we denote by K_n; $G(K_n/k)$ is then C_n, the cyclic group of order n generated by ρ. G may be thought of as the totality of (non-equivalent) Cauchy sequences of powers of ρ, where a sequence $\{\rho^{a_\nu}\}$ is Cauchy with respect to the Krull topology on G iff for any n for which $k \subset K_n \subset \Omega$, there is an integer $N(n)$ such that $\nu, \mu \geq N \Rightarrow \rho^{a_\nu - a_\mu}$ is in $G(\Omega/K_n)$; equivalently $n \mid a_\nu - a_\mu$.

If I is the set of integers n for which $k \subset K_n \subset \Omega$, then G may also be described as the inverse limit of the system $(I, \{C_n\}, \varphi_{mn})$, where $\varphi_{mn} : C_m \rightarrow C_n$ is the natural map for n dividing m. In this paper we construct an explicit isomorphism which relates the seemingly two disparate descriptions of the group G. The idea is to use instead of a lattice of subgroups $G(\Omega/K_n)$ and an inverse lattice of fixed fields K_n, a totally ordered set of subgroups of G to describe the topologies.

Let the degrees of the extension fields of k in Ω be (in natural order) $i_1, i_2, i_3, \cdots$. Define the integers $j_n, n = 1, 2, \cdots$, inductively as follows: $j_1 = i_1$; $j_n = \mathrm{LCM}(j_{n-1}, i_n)$. Let $F_n = K_{j_n}$, $C_n = G(\Omega/F_n)$, and $G_n = G(F_n/k)$, so G_n is cyclic of order j_n. Then

(i) $F_n \subset \Omega$ for each n.

(ii) $F_n \subset F_{n+1}$.

(iii) For each n, $K_{i_n} \subset F_n$.

The fundamental system $\{C_n\}$ of neighborhoods of the identity yields the Krull topology on G; with respect to this neighborhood system, a sequence $\{\rho^{a_\nu}\}$ is Cauchy iff given any $n, j_n \mid a_\nu - a_\mu$ for $\nu, \mu \geq N(n)$, Also, we observe that in obtaining G as an inverse limit, we can take the family of groups $G_n \cong G/C_n$. Thus $G \cong \underleftarrow{G}$, the inverse limit, which is that subgroup of ΠG_n,

(*) Nella seduta del 10 aprile 1976.

consisting of all elements $\{\rho_n\}$ (with $\rho_n \in G_n$) such that for any pair of integers $s \geq t$, the t-coordinate ρ_t is the image of the s-coordinate ρ_s under the homomorphism $\varphi_{st} : G_s \to G_t$.

Given any such element $\{\rho_n\}$, it will consist of a sequence, each of whose terms is a power ρ^{a_n} of ρ, where $0 \leq a_n < j_n$. We claim this sequence is Cauchy. For, given any integer s, let $y \geq x \geq s$, and let ρ^a, ρ^b, ρ^c be the powers of ρ appearing as the s, x and y coordinates respectively. Then $\varphi_{xs} : \rho^b \to \rho^a$, and $\varphi_{ys} : \rho^c \to \rho^a$, so that $j_s \mid (b - a)$ and $j_s \mid (c - a)$. Therefore, $i_s \mid (b - c)$, and this is the Cauchy criterion.

We therefore have a mapping from $\underleftarrow{G}$ into the set of all equivalence classes of Cauchy sequences $\{\rho^{a_\nu}\}$. To see the mapping is $1 - 1$ we ask: can two distinct elements of $\underleftarrow{G}$ give rise to equivalent sequences? Two sequences $\{\rho^{a_\nu}\}, \{\rho^{b_\nu}\}$ will be equivalent iff the combined sequence $\rho^{a_1}, \rho^{b_1}, \rho^{a_2}, \rho^{b_2}, \cdots,$ is Cauchy. Suppose the elements of $\underleftarrow{G}$ differ in the n-*th* coordinate, which is ρ^a, ρ^b, respectively. If the combined sequence were Cauchy, then $j_n \mid a_\nu - b_\mu$ for $\nu, \mu \geq N(n)$. In particular, $j_n \mid a_\nu - b_\nu$ for $\nu \geq N$. For any such ν, consider the ν-*th* coordinates ρ^x, ρ^y. We have $\varphi_{\nu n}(\rho^x) = \rho^a \Rightarrow j_n \mid (x - a), \varphi_{\nu n}(\rho^y) = \rho^b \Rightarrow j_n \mid (y - b)$. But $j_n \mid (x - y)$, so $j_n \mid (a - b)$, a contradiction since $a \neq b$, and $a, b < j_n$. Therefore the mapping is $1 - 1$.

Is it onto? Given the Cauchy sequence $\{\rho^{a_\nu}\}$, the class to which it belongs is uniquely determined by its limit, some $\sigma \in G$ (G is Hausdorff). Consider the homomorphisms $G \to G/C_n \cong G_n$, given for each n by $\sigma \to \sigma G_n$. Now G/C_n is cyclic of order j_n, generated by the coset ρC_n. Hence σC_n is the same coset as some $\rho^{u_n} C_n$, where $0 \leq u_n < j_n$. Consider the sequence $\{\rho^{u_n}\}$. It is an element of $\underleftarrow{G}$, for if $m \geq n$, then $C_m \subset C_n$, and by the way the u_i were chosen, $\rho^{u_m} \sigma^{-1} \in C_m$, $\rho^{u_n} \sigma^{-1} \in C_n$, so $\rho^{u_m - u_n} \in C_n$. But then $j_n \mid (u_m - u_n)$. Therefore, $\varphi_{mn}(\rho^{u_m}) = \rho^{u_n}$. Thus $\{\rho^{u_n}\} \in \underleftarrow{G}$, and its image under the mapping is clearly the equivalence class of the given sequence $\{\rho^{a_\nu}\}$. Thus the mapping is onto.

To see it is continuous, let C_n be any neighborhood of the identity in G. Now the topology in $\underleftarrow{G}$ is that induced in it as a subspace of ΠG_n. The neighborhood of the identity $U = \underleftarrow{G} \cap (\underbrace{\rho^0, \rho^0, \cdots, \rho^0}_{1 \text{ st } n \text{ entries}}, \chi \prod_{k>n} G_k)$ will be mapped into C_n, since the images will all leave F_n fixed. Thus the mapping, being continuous at the identity, is continuous. It is easily verified that the mapping preserves products. Since it is $1 - 1$, continuous and onto from one compact Hausdorff space to another, it is a homeomorphism as well as a group isomorphism.

We note that the device of using a totally ordered collection of groups to establish the isomorphism was necessary since otherwise not every element of $\underleftarrow{G}$ would give rise to a

Cauchy sequence. For example, if Ω is the algebraic closure of k, then $\underleftarrow{G}$ is the inverse limit of the cyclic groups C_n, for every n. Consider, e.g., the element $\{\rho^{a_n}\}$, with a_n defined as follows: (i) if $2 \nmid n$, $a_n = 0$; (ii) if $n = 2^s \prod_{i=1}^{r} p_i^{s_i}$ $(s > 0, p_i \neq 2)$, a_n is the unique solution (mod n) of the congruences

$$x \equiv 1 \ (2^s)$$

$$x \equiv 0 \left(\prod_{i=1}^{r} p_i^{s_i}\right).$$

If a_n is so defined, and $d \mid n$, it is easy to verify that $\varphi_{nd}(\rho^{a_n}) = \rho^{a_d}$, so $\{\rho^{a_n}\} \in \underleftarrow{G}$. But one sees easily that $\{\rho^{a_n}\}$ is not a Cauchy sequence.