MATHEMATICS

HELMUT KOCH

1961

SovietRxiv

Abstract

Full Text

MATHEMATICS

HELMUT KOCH

THE GALOIS GROUP OF A LOCAL FIELD

(Presented by Academician I. M. Vinogradov on 1 XII 1960)

Let k be an extension of finite degree m of the field R_p of rational p-adic numbers. The field k is called **regular** if it does not contain a p-th root of unity.

Let k be a regular field. In the work of I. R. Shafarevich ([1]) it is shown that if K is the union of all normal finite p-extensions of the field k, then the group Φ of the field K over k is a free topological p-group with $m+1$ generators.

Z. I. Borevich ([2]) considered the case where K is the maximal extension without simple branching of the field k. The result of his work is that Φ is a free group with another topology. But in doing so he did not notice that an unramified extension of a regular field is not always regular. For example, let $k = R_3(\sqrt{3})$; then $k(\sqrt{-1})$ is an unramified irregular extension of the regular field k. Therefore Borevich' s result will be valid only in the case when K is a regular field.

Let us now consider the totality of fields K having the following property: every finite regular extension of the field k is contained in one of the fields K.

Let K_0 be a finite regular normal extension of the field k without higher ramification, having a solvable Galois group. K_0 has the representation

$$K_0 = k\left(\sqrt[e]{\pi}, \zeta\right), \qquad e \equiv 0 \pmod{q^f - 1},$$

where π is a prime element of the field k; ζ is a q^f-th root of unity; q is the number of elements of the residue class field of the field k.

Let K be the union of all finite normal p-extensions of the field K_0; F a free group with $m+2$ generators $s, t, a_1, \dots, a_m$; $W = (t^e, sts^{-1}s^{-q})$ and $F_0 = (W, s^f, a_1, \dots, a_m)$ normal divisors of the group F. Then the following holds:

Theorem 1. *The group Φ of the field K over k is isomorphic to the completion $(F/W)^*$ of the group F/W with respect to the topology defined by the system of neighborhoods of the identity consisting of the set of normal divisors N of the group F/W that satisfy the conditions $N \subseteq F_0/W$ and $[F_0/W : N]$ is a power of p.*

Proof. We construct the fields K_n inductively. Let K_{n+1} be the union of all normal extensions of degree p of the field K_n. Then K_{n+1} will be a normal field over k and will be the class field of the field K_n for the group $(K_n^*)^p$ (K_n^* denotes the multiplicative group of the field K_n). Let Φ_n be the group of the field K_n over k. K is the union of all fields K_n.

The group Φ_0 is generated by two automorphisms:

$$\sigma = (\zeta \to \zeta^q,\ \sqrt[e]{\pi} \to \sqrt[e]{\pi})\,; \tag{1}$$

$$\tau = \left(\zeta \to \zeta,\ \sqrt[e]{\pi} \to \zeta^{\frac{q^f-1}{e}} \sqrt[e]{\pi}\right). \tag{2}$$

σ and τ satisfy the relations $\sigma^f = 1,\ \tau^e = 1,\ \sigma\tau\sigma^{-1} = \tau^q$. Our next aim is the computation of the group Φ_1. Let $\eta \in \Phi_0$, and let η_1 be its extension to the field K_1.

For the norm residue symbol $\left(\dfrac{K_1/K_0}{\alpha}\right)$ the following equality holds:

$$\left(\frac{K_1/K_0}{\alpha^\eta}\right) = \eta_1 \left(\frac{K_1/K_0}{\alpha}\right) \eta_1^{-1}, \qquad \alpha \in K_0^*. \tag{3}$$

Krassner ([3]) showed that every $\alpha \in K_0^*$ has a representation

$$\alpha = \sqrt[e]{\pi}^{\,a} \zeta^b \prod_{\nu=1}^{m} \varepsilon_\nu^{a_{\nu,\eta}}, \tag{4}$$

where $\varepsilon_1, \dots, \varepsilon_m$ is a system of independent principal units of the field K_0; a and b are integral rational numbers, and $a_{\nu,\eta}$ is an integral p-adic number.

One can find representatives σ_1, τ_1 of the automorphisms σ, τ which satisfy the relations

$$\sigma_1^f = \left(\frac{K_0'/K_0}{\sqrt[e]{\pi^g}\varepsilon}\right), \qquad g \not\equiv 0\ (p), \quad \varepsilon \in K_0 \text{ a unit}; \tag{5}$$

$$\sigma_1\tau_1\sigma_1^{-1} = \tau_1^q, \qquad \tau_1^e = 1. \tag{6}$$

From (3)–(6) it follows that the elements $\sigma_1, \tau_1, \gamma_{11} = \left(\dfrac{K_1/K_0}{\varepsilon_0}\right), \dots, \gamma_{m1} = \left(\dfrac{K_1/K_0}{\varepsilon_m}\right)$ will form a system of generators of the group Φ_1. Therefore the mapping

$$s \to \sigma_1, \qquad t \to \tau_1, \qquad a_1 \to \gamma_{11}, \dots,\ a_m \to \gamma_{m1}$$

defines a homomorphism $\mathfrak{S}$ of the group F onto Φ_1. Let F_0' be the Frattini subgroup of the group F_0, and let F_1 be the normal divisor of the group F generated by the groups F_0' and W. Then F_1 is the kernel of the homomorphism $\mathfrak{S}$.

Next let $F_0^{(n+1)}$ be the Frattini subgroup of the group $F_0^{(n)}$, $n = 1, 2, ...$, and let F_n be the normal divisor of the group F generated by the groups $F_0^{(n)}$ and W.

We choose inductively in Φ_n representatives $\sigma_n, \tau_n, \gamma_{1n}, \dots, \gamma_{mn}$ of the automorphisms $\sigma_{n-1}, \tau_{n-1}, \gamma_{1,n-1}, \dots, \gamma_{m,n-1}$ so that the relations

$$\tau_n^e = 1, \qquad \sigma_n \tau_n \sigma_n^{-1} = \tau_n^q$$

are satisfied. The mapping

$$s \to \sigma_n, \qquad t \to \tau_n, \qquad a_1 \to \gamma_{1n}, \dots, \; a_m \to \gamma_{mn}$$

defines a homomorphism of the group F onto Φ_n, whose kernel coincides with F_n. The group Φ of the field K over k is the projective limit of the sequence

$$\Phi_0 \leftarrow \Phi_1 \leftarrow \cdots \leftarrow \Phi_n \leftarrow \cdots$$

Therefore Φ is isomorphic to the projective limit of the sequence

$$F/F_0 \leftarrow F/F_1 \leftarrow \cdots \leftarrow F/F_n \leftarrow \cdots$$

The intersection of all F_n is equal to W. The sequence $\{F_n/W, \; n = 0, 1, 2, ...\}$ forms a system of neighborhoods of the identity of the group F/W, which consists of

all normal divisors N of the group F/W satisfying the conditions $N \subseteq F_0/W$, and $[F_0/W; N]$ is equal to a power of p. Theorem 1 follows from this.

An analogous result can be obtained in the case where k is any finite extension of the field R_p, and K is the algebraic closure of the field.

Let K_0 be the maximal extension of the field k without higher ramification. Over k the field K_0 is generated by means of the totality of pairs of elements

$$(\zeta_e, \sqrt[e]{\pi}),$$

where e runs through all natural numbers relatively prime to p, and ζ_e is a primitive e-th root of unity.

The group Φ_0 of the field K_0 over k is the total completion of the group Γ with two generators σ and τ, defined as follows:

$$\sigma = (\zeta_e \to \zeta_e^q,\ \sqrt[e]{\pi} \to \zeta_e \sqrt[e]{\pi}),$$

$$\tau = (\zeta_e \to \zeta_e,\ \sqrt[e]{\pi} \to \zeta_e \sqrt[e]{\pi});$$

σ and τ satisfy the single relation $\sigma\tau\sigma^{-1} = \tau^q$.

Iwasawa ([4]) showed that the group Ψ of the field K over K_0 is a free topological p-group with a countable number of generators, and that the group Φ of the field K over k is a semidirect extension of the group Φ_0 by means of Ψ.

Moreover, Iwasawa showed that there exists a sequence of fields k_n, $n = 1, 2, \dots, \infty$, with the following properties:

1. k_n is a finite normal extension of the field k with simple ramification.
2. $$\bigcup_{n=1}^{\infty} k_n = K_0.$$
3. Every principal unit ε_n of the field k_n has a representation

$$\varepsilon_n = \varepsilon_{0n}^a \prod_{\substack{\nu=1 \\ \eta \in \varphi_n}}^{m} \varepsilon_{\nu n}^{a_{\nu n} \eta^i},$$

where $\varepsilon_{0n}, \varepsilon_{1n}, \dots, \varepsilon_{mn}$ is a system of principal units of the field k_n; a and $a_{\nu n}$ are integral p-adic numbers; φ_n is the group of the field k_n over k.

4. Let p^K be the maximal p-power order of a root of unity ζ_K contained in K_0. Then the representation (7) is unique up to p^K-th powers, and the congruences

$$\varepsilon_{0n}^\sigma \equiv \varepsilon_{0n}^g, \qquad \varepsilon_{0n}^\tau \equiv \varepsilon_{0n}^h, \quad (\mathrm{mod}\ p^K) \qquad\qquad (\mathrm{mod}\ p^K)$$

hold, where g and h are determined by the equalities

$$\zeta_K^\sigma = \zeta_K^g, \qquad \zeta_K^\tau = \zeta_K^h.$$

5. $N_{k_l/k_n}(\varepsilon_{\nu n}) = \varepsilon_{\nu l}$.

Let K_{1n} (respectively, K_1) be the union of all normal cyclic extensions of degree p^K of the field k_n (respectively, K_0). As above, we can compute the group Φ_{1n} of the field K_{1n} over k and then pass to the projective limit of the sequence of groups $\Phi_{11} \leftarrow \Phi_{12} \leftarrow \cdots \leftarrow \Phi_{1n} \leftarrow \cdots$.

Thus we obtain that the group of the field K_1 over K_0 has a minimal basis of the form

$$\{\gamma_0',\ \eta'\gamma_\nu'\eta a'^{-1};\ \nu = 1, \dots, m;\ \eta \in \Gamma\},$$

where

$$\gamma_\nu' = \lim_{n\to\infty} \left(\frac{K_{1n}/k_n}{\varepsilon_{\nu n}} \right)$$

and η' is the extension of the automorphism η to K_1. γ_0' satisfies the relations

$$\sigma'\gamma_0'\sigma a'^{-1} = \gamma_0'^{\,g}, \qquad \tau'\gamma_0'\tau u'^{-1} = \gamma_0'^{\,h}.$$

Choose in Φ representatives $\bar\sigma, \bar\tau, \gamma_0, \dots, \gamma_m$ of the automorphisms $\sigma', \tau', \gamma_0', \dots, \gamma_m'$ so that the relations

$$\bar\sigma\bar\tau\bar\sigma^{-1} = \bar\tau^q, \qquad \bar\tau\gamma_0\bar\sigma\bar\tau^{-1} = \gamma_0^h$$

are satisfied.

The relation $\sigma'\gamma_0'\sigma a'^{-1} = \gamma_0'^{g}$ extends to the relation

$$\bar\sigma\gamma_0\bar\sigma^{-1} = \rho\gamma_0^g,$$

where $\rho \in \Psi^{p^K}[\Psi, \Psi]$.

By the theorem on Burnside bases (^{5}), the elements $\gamma_0, \bar\eta\gamma_\nu\bar\eta^{-1}$, $\nu = 1, \dots, m;\ \eta \in \Gamma$, form a minimal system of generators of the free topological p-group Ψ. Consequently, the following holds.

Theorem 2. The group Φ of the algebraic closure K of the field k is a semidirect extension of the group Φ_0 by means of the free topological p-group Ψ with minimal system of generators

$$\{\gamma_0, \bar\eta\gamma_\nu\bar\eta^{-1};\ \nu = 1, \dots, m;\ \eta \in \Gamma\}.$$

The automorphism $\bar\sigma$ (respectively $\bar\tau$) sends γ_0 to $\rho\gamma_0^g$ (respectively γ_0^h), where $\rho \in \Psi^{p^K}[\Psi, \Psi]$.

V. A. Steklov Mathematical Institute
Academy of Sciences of the USSR

Received
23 XI 1960

REFERENCES

1. I. R. Shafarevich, *Matem. sborn.*, **20** (62), No. 2 (1947).

2. Z. I. Borevich, *Vestn. Leningradsk. univ.*, ser. matem., No. 19 (1956).

3. M. Krasner, *Acta Arithmetica*, **3**, No. 2 (1939).

4. K. Iwasawa, *Trans. Am. Math. Soc.*, **80**, 448 (1955).

5. H. Zassenhaus, *Lehrbuch der Gruppentheorie*, 1, 1937.

Note: Figure translations are in progress. See original paper for figures.