COLLOQUIUM MATHEMATICUM

VOL. XXXVII 1977 FASC. 1

PRIMES WHICH REMAIN IRREDUCIBLE IN A NORMAL FIELD

BY

JAN ŚLIWA (WROCŁAW)

1. For a given algebraic number field K let us denote by $\mathrm{IP}(K)$ the set of those rational primes unramified in K which remain irreducible in K.

Narkiewicz ([2], Chapter 9.2.3) noted that if K/Q is normal and $\mathrm{IP}(K) \neq \emptyset$, then the Galois group of K contains a cyclic subgroup of index not exceeding the Davenport constant of $H(K)$ ($H(K)$ — the class group of K).

If K is a cyclic extension, then there exist rational primes which generate a prime ideal in K, and so in this case $\mathrm{IP}(K) \neq \emptyset$. In [2], p. 434, an example was given of a non-cyclic extension K with $\mathrm{IP}(K) = \emptyset$ (namely $K = Q(e)$, where e is a primitive eighth root of unity).

Here we characterize those normal fields K for which $\mathrm{IP}(K)$ is non-empty and we prove some related facts about $\mathrm{IP}(K)$.

2. Let K/Q be normal with Galois group G. Denote by K_H the Hilbert class field of K. We shall identify, by Artin's automorphism, the Galois group of K_H/K with the class group $H(K)$ (see [1]). It is easy to note that the extension K_H/Q is normal. Denote its Galois group by $\bar{G}$. The group $\bar{G}$ depends on G, $H(K)$ and the action of G on $H(K)$. For this action we write

$$\varphi: G \to \mathrm{Aut}\big(H(K)\big)$$

or else $h \to h^{\sigma}$, $\sigma \in G$.

The group $\bar{G}$ is an extension of $H(K)$ by G,

$$1 \longrightarrow H(K) \xrightarrow{i} \bar{G} \xrightarrow{\pi} G \longrightarrow 1, \tag{1}$$

where i denotes the injection and π is the restriction on K. For $X \in H(K)$ and $\sigma \in G$ we have

$$\varphi(\sigma)X = gXg^{-1}, \tag{2}$$

where g denotes an arbitrary element of $\bar{G}$ with $\pi g = \sigma$.

Definition 1. The elements $\sigma \in G$ and $X \in H(K)$ will be called *related* in $\bar{G}$ if there exists $g \in \bar{G}$ such that

$$\pi g = \sigma \quad \text{and} \quad g^{\operatorname{ord} \pi g} = X.$$

(Note that, for all $g \in \bar{G}$, we have $g^{\operatorname{ord} \pi g} \in H(K)$ as $\pi(g^{\operatorname{ord} \pi g}) = 1$ and sequence (1) is exact.)

Definition 2. Let H be an Abelian group and let $h_1, \ldots, h_m \in H$. The equality

$$h_1 \ldots h_m = 1$$

will be called *minimal* if

$$h_{i_1} \ldots h_{i_r} = 1 \quad \text{with } 1 \leqslant i_1 < \ldots < i_r \leqslant m,\ r \geqslant 1,$$

implies $m = r$.

For any group G and its subgroup H we write $G \bmod H$ for any set of representatives of G with respect to H, and for $\sigma \in G$ we denote by $\langle \sigma \rangle$ the subgroup of G generated by σ.

THEOREM 1. *Let K/Q be normal with the Galois group G and class group $H(K)$. Then the set $\mathrm{IP}(K)$ is non-empty if and only if there exist related $\sigma \in G$ and $X \in H(K)$ such that the equality*

$$(*) \qquad \prod_{a \in G \bmod \langle \sigma \rangle} \varphi(a) X = 1$$

is minimal (¹).

Proof. Let p be a rational prime unramified in K_H, $\mathfrak{p}$ a prime ideal in K dividing p, and $\mathfrak{P}$ a prime ideal in K_H dividing $\mathfrak{p}$. Let

$$g = \left[\frac{K_H/Q}{\mathfrak{P}}\right]$$

be the Frobenius automorphism of $\mathfrak{P}$. For the Artin symbol of p we have

$$\left(\frac{K_H/Q}{p}\right) = \left\{\left[\frac{K_H/Q}{\mathfrak{P}'}\right]\right\}_{\mathfrak{P}'|p} = \left\{\left[\frac{K_H/Q}{t(\mathfrak{P})}\right]\right\}_{t \in \bar{G} \bmod \bar{G}_{\mathfrak{P}}},$$

where

$$\bar{G}_{\mathfrak{P}} = \{s \in \bar{G} : s(\mathfrak{P}) = \mathfrak{P}\}$$

is the decomposition group of $\mathfrak{P}$. Utilizing the properties of the Frobenius symbol and the equality $\bar{G}_{\mathfrak{P}} = \langle g \rangle$ (see [1]) we get

$$(3) \qquad \left(\frac{K_H/Q}{p}\right) = \{tgt^{-1}\}_{t \in \bar{G} \bmod \langle g \rangle}.$$

(¹) This product does not depend on the choice of $G \bmod \langle \sigma \rangle$, since for related σ and X we have $\varphi(\sigma) X = X$.

The ideal $\mathfrak{p}$ lies in the class $((K_H/K)/\mathfrak{P})$ of $H(K)$. But K_H/K is Abelian, so

$$\left(\frac{K_H/K}{\mathfrak{p}}\right) = \left[\frac{K_H/K}{\mathfrak{P}}\right] = g^f,$$

where f denotes the degree of $\mathfrak{p}$, equal to the order of

$$\left[\frac{K/Q}{\mathfrak{p}}\right] = \pi g \quad \text{in } G.$$

If $(p) = \mathfrak{p}_1 \dots \mathfrak{p}_m$ is the decomposition of (p) into prime ideals in K, and $\mathfrak{p}_i \in X_i \in H(K)$ $(1 \leqslant i \leqslant m)$, then we shall call the collection

$$O_p = \{X_1, \dots, X_m\}$$

the *orbit of* p.

Note that $s_1(\mathfrak{P})$ and $s_2(\mathfrak{P})$ divide the same ideal $\mathfrak{p}_i$ if and only if $s_1 s_2^{-1} \in \mathrm{Gal}(K_H/K) = H(K)$. Hence (3) implies

$$O_p = \{tg^{\operatorname{ord}\pi g}t^{-1}\}_{t \in \bar{G} \bmod \langle g \rangle H(K)}.$$

That, in view of (1) and (2), gives

$$O_p = \{\varphi(t)g^{\operatorname{ord}\pi g}\}_{t \in G \bmod \langle \pi g \rangle}.$$

Now it is sufficient to observe that p is irreducible in K if and only if the equality $X_1 \dots X_m = 1$ is minimal.

3. Now we describe related elements (Definition 1) in terms of G, $H(K)$, the action of G on $H(K)$ and the class of $H^2(G, H(K))$ which corresponds to the extension $\bar{G}$. To do this we write, for $\sigma \in G$ and $Y \in H(K)$,

$$Y^{N_\sigma} = Y \cdot Y^\sigma \cdot \dots \cdot Y^{\sigma^{\operatorname{ord}\sigma - 1}}$$

and, for x in $H^2(G, H(K))$, the element which corresponds to $\bar{G}$,

$$W(\sigma) = x(\sigma, \sigma)x(\sigma^2, \sigma) \dots x(\sigma^{\operatorname{ord}\sigma - 1}, \sigma).$$

PROPOSITION 1. *The elements* $\sigma \in G$ *and* $X \in H(K)$ *are related if and only if* $X \in H(K)^{N_\sigma} W(\sigma)$.

Proof. For every $\sigma \in G$, choose $u_\sigma \in \bar{G}$ such that $\pi(u_\sigma) = \sigma$ and $u_1 = 1$. Each element of $\bar{G}$ can uniquely be written in the form hu_σ $(h \in H(K),\ \sigma \in G)$. We have

$$\pi(hu_\sigma) = \sigma, \qquad u_\sigma h = h^\sigma u_\sigma, \qquad u_\sigma u_\tau = x(\sigma, \tau)u_{\sigma\tau}.$$

Thus the elements σ and X are related if and only if there exists $h \in H(K)$ such that

$$X = (hu_\sigma)^{\operatorname{ord}\pi(hu_\sigma)} = (hu_\sigma)^{\operatorname{ord}\sigma}.$$

But for $k = 0, 1, 2, \ldots$ we have

$$(hu_{\sigma})^{k} = h\cdot h^{\sigma}\cdot\ldots\cdot h^{\sigma^{k-1}}x(\sigma,\sigma)x(\sigma^{2},\sigma)\ldots x(\sigma^{k-1},\sigma)\,u_{\sigma^{k}},$$

whence

$$X = h^{N_{\sigma}}W(\sigma).$$

4. Now we give some consequences of Theorem 1.

COROLLARY 1. *Suppose that G acts trivially on $H(K)$. Each of the following conditions is equivalent to $\mathbb{P}(K) \neq \emptyset$.*

(a) *There exist related $\sigma \in G$ and $X \in H(K)$ such that*

$$(\operatorname{ord}\sigma)(\operatorname{ord}X) = [K:Q].$$

(b) *There exists $g \in \overline{G}$ of order $[K:Q]$.*

Proof. In this case, $\varphi(a)X = X$ for all a and X. So the minimality of $(*)$ means $\operatorname{ord}X = |G|/\operatorname{ord}\sigma$ and this gives (a).

Further, if $g \in \overline{G}$ satisfies

$$\pi g = \sigma \quad\text{and}\quad g^{\operatorname{ord}\pi g} = X,$$

then $\operatorname{ord}\pi g \mid \operatorname{ord} g$, and so

$$\operatorname{ord} g = (\operatorname{ord}\pi g)(\operatorname{ord} g^{\operatorname{ord}\pi g}) = (\operatorname{ord}\sigma)(\operatorname{ord}X) = [K:Q].$$

COROLLARY 2. *Suppose that G acts trivially on $H(K)$ and*

$$([K:Q],\, |H(K)|) = 1.$$

Then $\mathbb{P}(K) \neq \emptyset$ if and only if G is cyclic.

This fact is an immediate consequence of Corollary 1 (a).

5. It follows from the proof of Theorem 1 that primes in $\mathbb{P}(K)$ are characterized by some conjugacy classes in $\overline{G}$, namely, $p \in \mathbb{P}(K)$ if and only if, for any $\sigma \in \big((K_H/Q)\; p\big)$, the equality

$$\prod_{t \in \overline{G} \bmod \langle\sigma\rangle H(K)} (t\sigma^{\operatorname{ord}\pi\sigma}t^{-1}) = 1 \tag{4}$$

is minimal. We shall denote by $A(K)$ the subset of $\overline{G} = \operatorname{Gal}(K_H/Q)$ consisting of all σ for which equality (4) is minimal. Chebotarev's density theorem (see [2]) implies now, for

$$a(K) = \lim_{x\to\infty}\frac{\log x}{x}\Big(\sum_{p\leq x,\ p\in\mathbb{P}(K)} 1\Big),$$

the formula

$$a(K) = \frac{1}{nh} \sum_{\sigma \in A(K)} 1, \qquad n = [K:Q],\ h = |H(K)|. \tag{5}$$

If $K \neq Q$, then always $\sigma = 1 \notin A(K)$, as this element corresponds to primes which split completely into principal ideals. Hence

$$a(K) \leqslant 1 - \frac{1}{nh}. \tag{6}$$

In some simple cases it is possible to obtain an exact formula for $a(K)$.

THEOREM 2. *For normal K with $n = 2$ or $n = 3$ we have*

$$a(K) = 1 - \frac{1}{nh}.$$

Proof. We prove our theorem for $n = 2$ only. The case $n = 3$ is quite analogous. If K is quadratic, then only those unramified primes p for which $(p) = \mathfrak{p}_1\mathfrak{p}_2$ with principal $\mathfrak{p}_1, \mathfrak{p}_2$ are not contained in $\mathrm{IP}(K)$. But this means that

$$\left[\frac{K_H/Q}{\mathfrak{P}_i}\right] = \left[\frac{K_H/K}{\mathfrak{p}_i}\right] = 1 \qquad (i = 1, 2)$$

for $\mathfrak{P}_i | \mathfrak{p}_i$ in K_H. Applying now Chebotarev's theorem we get our assertion.

6. Let K and L be normal extensions of Q. We shall consider the connections between the sets $\mathrm{IP}(K)$ and $\mathrm{IP}(L)$. As we are interested only in unramified primes, we shall consider in $\mathrm{IP}(K)$ and $\mathrm{IP}(L)$ only those primes which do not ramify in the composite KL.

Note that if $K \subset L$, then $\mathrm{IP}(L) \subset \mathrm{IP}(K)$. The converse is not true as, for L with $\mathrm{IP}(L) = \emptyset$ and for all K, we have $\mathrm{IP}(L) \subset \mathrm{IP}(K)$. But, nevertheless, it is possible to obtain some results. Let

$$\Gamma = \mathrm{Gal}(K_H L_H/Q), \qquad \bar{G}_1 = \mathrm{Gal}(K_H/Q), \qquad \bar{G}_2 = \mathrm{Gal}(L_H/Q).$$

Clearly $\Gamma \subset \bar{G}_1 \times \bar{G}_2$.

THEOREM 3. *For normal K and L we have:*

(a) $\mathrm{IP}(K) \subset \mathrm{IP}(L)$ *if and only if*

$$\Gamma \cap \big(A(K) \times (\bar{G}_2 \setminus A(L))\big) = \emptyset.$$

(b) $\mathrm{IP}(K) \subset \mathrm{IP}(L)$ *implies that if* $(\sigma, 1) \in \Gamma$, *then*

$$\langle\sigma\rangle \cap A(K) = \emptyset,$$

and that

$$[K_H L_H : Q] \leqslant [K_H : Q][L_H : Q]\big(1 - a(K) + a(K)a(L)\big).$$

(c) $\mathrm{IP}(K) = \mathrm{IP}(L)$ *if and only if*

$$\Gamma \subset \big(A(K) \times A(L)\big) \cup \Big(\big(\bar{G}_1 \setminus A(K)\big) \times \big(\bar{G}_2 \setminus A(L)\big)\Big).$$

(d) $\mathrm{IP}(K) = \mathrm{IP}(L)$ *implies that if*

$$(\sigma, \tau) \in \Gamma \quad \text{and} \quad (\operatorname{ord}\sigma, \operatorname{ord}\tau) = 1,$$

then

$$\langle\sigma\rangle \cap A(K) = \langle\tau\rangle \cap A(L) = \emptyset,$$

and that

$$[K_H L_H : Q] \leq [K_H : Q][L_H : Q]\Big(a(K)a(L) + \big(1 - a(K)\big)\big(1 - a(L)\big)\Big).$$

(e) *If* $\mathrm{IP}(K) \neq \emptyset$, $\mathrm{IP}(L) \neq \emptyset$ *and* $K_H \cap L_H = Q$, *then*

$$\mathrm{IP}(K) \not\subset \mathrm{IP}(L) \quad \textit{and} \quad \mathrm{IP}(L) \not\subset \mathrm{IP}(K).$$

Proof. Consider a rational prime p unramified in KL and the Artin symbol

$$\left(\frac{K_H L_H / Q}{p}\right).$$

Let

$$(\sigma, \tau) \in \left(\frac{K_H L_H / Q}{p}\right), \qquad \sigma \in \bar{G}_1, \ \tau \in \bar{G}_2.$$

It is obvious that $p \in \mathrm{IP}(K)$ (respectively, $p \in \mathrm{IP}(L)$) if and only if $\sigma \in A(K)$ (respectively, $\tau \in A(L)$). Therefore, the condition $\mathrm{IP}(K) \subset \mathrm{IP}(L)$ is satisfied if and only if $(\sigma, \tau) \in \Gamma$ and $\sigma \in A(K)$ imply $\tau \in A(L)$. But that is equivalent to (a).

Now, as $1 \notin A(L)$, no element of the form $(\sigma, 1)$, $\sigma \in A(K)$, can be contained in Γ. This gives the first part of (b). The inequality of (b) is an immediate consequence of (a) and (5).

The assertion of (c) follows from (a).

Let now $(\sigma, \tau) \in \Gamma$ and $(\operatorname{ord}\sigma, \operatorname{ord}\tau) = 1$; then

$$(\sigma, \tau)^{\operatorname{ord}\sigma} = (1, \tau^{\operatorname{ord}\sigma}) \in \Gamma,$$

but $\langle\tau\rangle = \langle\tau^{\operatorname{ord}\sigma}\rangle$, so, in view of (b), $\langle\tau\rangle \cap A(L) = \emptyset$. The same argument gives $\langle\sigma\rangle \cap A(K) = \emptyset$. The inequality of (d) follows from (c) and (5) by counting the number of elements in the set

$$\big(A(K) \times A(L)\big) \cup \Big(\big(G_1 \setminus A(K)\big) \times \big(G_2 \setminus A(L)\big)\Big).$$

Finally, if $K_H \cap L_H = Q$, then

$$[L_H K_H : Q] = [L_H : Q][K_H : Q],$$

and so, in view of (6), the inequality of (b) cannot be true.

7. It is possible to prove analogous facts for non-normal extensions. Here we give only a sufficient condition for $\mathrm{IP}(K) \neq \emptyset$.

(o) *Let K be a finite extension of Q, $\bar{K}$ the normal closure of K, G its Galois group, and U the subgroup of G which corresponds by the Galois theory to K. If there exists $g \in G$ such that $\langle g \rangle U = G$, then* $\mathrm{IP}(K) \neq \emptyset$.

Indeed, the condition in (o) means (see [1], p. 123) that there exist rational primes unramified in K, which remain primes in K.

REFERENCES

[1] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Vol. II, Würzburg-Wien 1965.

[2] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Warszawa 1974.

INSTITUTE OF MATHEMATICS
WROCŁAW UNIVERSITY

Reçu par la Rédaction le 12. 1. 1976