ACTA ARITHMETICA
XIX (1971)

Algebraic number fields with the principal ideal condition

by

CHARLES J. PARRY (Baton Rouge, La.)

A finite extension K of an algebraic number field k will be said to have the *Principal Ideal Condition* (*PIC*) if each prime ideal $\mathfrak{p}$ of k which is unramified in K and has one principal prime ideal factor in K, actually has all of its prime ideal factors principal in K.

It is a well known result of algebraic number theory that every Galois extension K/k has PIC. Purely cubic extensions of the rational numbers with class number 1 show that converse of the above statement is false. The objective of this paper is to characterize all number field extensions with PIC. Since all quadratic extensions are Galois and thus have PIC, it is reasonable to first consider the case when $(K:k) = 3$.

PROPOSITION I. *Let* $(K:k) = 3$ *and* $\mathrm{CF}(K)$ *denote the Hilbert class field of* K. *Now* K/k *has PIC if and only if* $\bar{K}\,\mathrm{CF}(K)/k$ *is Galois,* $\bar{K}$ *denotes the Galois closure of* K *with respect to* k.

Proof. Let $\mathfrak{p}$ be a prime of k which is unramified in K and has one principal prime factor in K. Now there are only three possible ways for $\mathfrak{p}$ to decompose in K:

$$\text{(i)}\ \mathfrak{p} = P,$$

$$\text{(ii)}\ \mathfrak{p} = P_1P_2,$$

$$\text{(iii)}\ \mathfrak{p} = P_1P_2P_3.$$

The condition could only fail in the third case. In this case $\mathfrak{p}$ splits completely in K and hence splits completely in $\bar{K}$. Now since $\mathfrak{p}$ has one principal prime factor in K, this factor gains degree 1 when lifted to $\mathrm{CF}(K)$. Thus $\mathfrak{p}$ will have at least one linear prime factor in $\bar{K}\,\mathrm{CF}(K)$, but $\bar{K}\,\mathrm{CF}(K)/k$ is Galois so $\mathfrak{p}$ must split completely in $\bar{K}\,\mathrm{CF}(K)$. Thus every prime ideal factor of $\mathfrak{p}$ in K is principal.

The other part of the proposition will be proved in the general case by Lemma I.

In general we need slightly stronger hypothesis than in the cubic case. To make the result more readable I first introduce the following notation:

$$\begin{aligned}
\mathrm{CF}(K)\ &:\ \text{Hilbert class field of } K,\\
\bar{K}\ &:\ \text{Galois closure of } K \text{ over } k,\\
H &= G(\mathrm{CF}(K)/K)\text{: Galois group of } \mathrm{CF}(K)/K,\\
L &= \mathrm{CF}(K)\cap \bar{K},\\
H_1 &= G(\mathrm{CF}(K)/L),\\
h &= (\mathrm{CF}(K):K),\\
h_1 &= (\mathrm{CF}(K):L),\\
n &= (\bar{K}:K),\\
n_1 &= (\bar{K}:L),
\end{aligned}$$

$R: H\to H/H_1$, the natural homomorphism is the restriction mapping

$$R(\sigma) = \sigma|_L.$$

THEOREM I. *A finite extension K/k has PIC if and only if $\bar{K}\,\mathrm{CF}(K)/k$ is Galois, $(n_1, h_1) = 1$ and R does not preserve the order of any element $\sigma\neq 1$ of H.*

The proof of this theorem results from a series of lemmas. First an Artin diagram will be helpful:

$$\begin{tikzcd}[column sep=small]
 & \bar{K}\,\mathrm{CF}(K) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathrm{CF}(K) \arrow[dr, dash] & & \bar{K} \arrow[dl, dash] \\
 & L = \mathrm{CF}(K)\cap\bar{K} \arrow[d, dash] & \\
 & K \arrow[d, dash] & \\
 & k. &
\end{tikzcd}$$

LEMMA I. *If K/k has PIC then $\bar{K}\,\mathrm{CF}(K)/k$ is Galois.*

Proof. Let $\mathfrak{p}$ be a prime of k which has one linear factor P in $\bar{K}\,\mathrm{CF}(K)$. Now $\mathfrak{p}$ has one linear prime factor in $\bar{K}$ and so must split completely there. Also $\mathfrak{p}$ has one principal prime factor in K and since K/k has PIC, every prime factor of $\mathfrak{p}$ in K must be principal. Thus every prime factor of $\mathfrak{p}$ in the composition $\bar{K}\,\mathrm{CF}(K)$ must be linear over k, i.e. $\mathfrak{p}$ splits completely in $\bar{K}\,\mathrm{CF}(K)$. Hence $\bar{K}\,\mathrm{CF}(K)/k$ is Galois.

LEMMA II. *If K/k has PIC then $(n_1, h_1) = 1$.*

Proof. First note that $G(\bar{K}\,\mathrm{CF}(K)/L)\cong G(\mathrm{CF}(K)/L)\otimes G(\bar{K}/L)$. If a prime number q divides both n_1 and h_1 then there are elements $\sigma\in G(\mathrm{CF}(K)/L)$ and $\tau\in G(\bar{K}/L)$ which have order q. Thus $(\sigma,\tau)\in G(\bar{K}\,\mathrm{CF}(K)/L)$ and has order q. By the Čebotarev density theorem we can choose a prime P of K which is linear over k and has Artin symbol

$$\left(\frac{\bar{K}\,\mathrm{CF}(K)/K}{P}\right) = \varkappa\big((\sigma,\tau)\big)$$

(where $\varkappa\big((\sigma,\tau)\big)$ denotes the conjugacy class of (σ,τ)). Letting $\mathfrak{p} = P\cap k$ we see that each prime factor of $\mathfrak{p}$ in $\bar{K}$ has degree q over k. Now $\mathfrak{p}$ must have at least one prime factor P' in K which has degree q over k, since otherwise $\mathfrak{p}$ would split completely in $\bar{K}$. By Lemma I $\bar{K}\,\mathrm{CF}(K)/k$ is Galois so each prime factor of P' in $\bar{K}\,\mathrm{CF}(K)$ must be of degree q over k. Hence these factors of P' are linear over K and so P' must be principal in K. This contradicts the fact that K/k has PIC. Hence $(n_1, h_1) = 1$.

LEMMA III. *If K/k has PIC and $\sigma\neq 1$ is in H then $R(\sigma)$ has order less than order of σ.*

Proof. Assume there is a $\sigma\neq 1$ in H with the order of $R(\sigma)$ equal to the order of σ. By taking powers of σ we may assume the order of σ is a prime number q. Now we can find an extension σ^* of σ in $G(\bar{K}\,\mathrm{CF}(K)/K)$ where σ^* has order q^α for some integer $\alpha\geqslant 1$. By the Čebotarev density theorem we can find infinitely many primes P in K which are linear over k and with Artin symbol

$$\left(\frac{\bar{K}\,\mathrm{CF}(K)/K}{P}\right) = \varkappa(\sigma^*).$$

Now

$$\left(\frac{\mathrm{CF}(K)/K}{P}\right) = \varkappa(\sigma^*)|_{\mathrm{CF}(K)} = \varkappa(\sigma) = \sigma.$$

Also

$$\left(\frac{L/K}{P}\right) = \sigma|_L.$$

Thus P must gain degree q when lifted to L and no further degree when lifted to $\mathrm{CF}(K)$. Also P must gain degree q^α when lifted to $\bar{K}$, hence some other prime factor P' in K of $P\cap k$ must be of degree q^α over k. Thus P' gains degree 1 when lifted to $\bar{K}\,\mathrm{CF}(K)$. So P' is principal in K contradicting that K/k has PIC. Hence no such σ can exist.

LEMMA IV. *Suppose $\bar{K}\,\mathrm{CF}(K)/k$ is Galois, $(n_1, h_1) = 1$ and R does not preserve the order of any element of H except the identity. Then K/k has PIC.*

Proof. Suppose K/k does not have PIC. Then there exists a prime $\mathfrak{p}$ of k which has factors P and P' in K with P principal and P' not principal in K. Let f_1 and f_1' denote the degrees of P and P' respectively over k. Let $f_2, f_2'; f_3, f_3'; f_4$ and f_4' denote the degrees gained when P and P' are respectively lifted from K to L; from L to $\mathrm{CF}(K)$ and from L to $\bar{K}$

respectively. Now since P is principal in $K, f_2 = f_3 = 1$. However, teh total degree over k of the prime factors of P and P' in $\bar{K}\mathrm{CF}(K)$ is teh same, so from ([1], p. 358, Satz II) it follows

$$f_1 f_4 = f_1' f_2' f_3' f_4'.$$

Also the total degree over k of the prime factors of P and P' in $\bar{K}$ is the same and thus

$$f_1 f_4 = f_1' f_2' f_4'.$$

From these two equations it follows $f_3' = 1$. Let

$$\sigma = \left(\frac{\mathrm{CF}(K)/K}{P}\right).$$

The order of σ is $f_2' f_3' = f_2'$ which is the order of $R(\sigma)$, contradicting the hypothesis.

This completes the proof of Theorem I. Some interesting corollaries are easy consequences of the above theorem and proposition.

Corollary I. *If $L = K$ then K/k has PIC if and only if $\bar{K}\mathrm{CF}(K)/k$ is Galois and $(n, h) = 1$.*

Proof. Immediate.

Corollary II. *Let h be square free, then K/k has PIC if and only if $\bar{K}\mathrm{CF}(K)/k$ is Galois and $(n, h) = 1$.*

Proof. Only the necessity requires proof. Now if $L = K$ we are done by Corollary I. Suppose $L \neq K$ and let q be any prime which divides $(L:K)$. Choose $\sigma \epsilon H$ to have order q. Since $(h_1, q) = 1$, $R(\sigma)$ must also have order q. By Theorem I this contradicts the fact that K has PIC.

Corollary III. *Let $(K:k) = 3$, K/k not be Galois, $L = K$ and $\bar{K}\mathrm{CF}(K)/k$ be Galois, then the class number h of K is odd.*

Proof. By Proposition I K/k has PIC. By Corollary I $(h, 2) = 1$.

Specializing to the case $k = Q$, the rational number field, we obtain:

Lemma V. *If $(K:Q) = 3$ then* $\mathrm{CF}(K) \cap \bar{K} = K$.

Proof. If $K = \bar{K}$ we are done so we may assume $(\bar{K}:K) = 2$. Suppose some prime p of Q has even ramification index in $\bar{K}$. This index must be either 2 or 6. In the latter case p is totally ramified in $\bar{K}$ and thus $\bar{K}/K$ is ramified. In the other case we must have

$$p = P_1^2 P_2 \text{ in } K.$$

Now P_2 must ramify when lifted to $\bar{K}$.

To see such a rational prime p always exists, we merely note that $\bar{K}$ contains a quadratic subfield. In this subfield some rational prime must have ramification index 2 and hence has even ramification index when lifted to $\bar{K}$.

Corollary IV. *If $(K:Q) = 3$, K/Q is not Galois and K/Q has PIC then K has odd class number.*

Proof. Immediate from Corollary III and Lemma V.

Reference

[1] M. Bauer, *Über zusammengesetzte Zahlkörper*, Math. Ann. 77 (1916), pp. 357–361.

Received on 1. 8. 1970 (109)