which can be made arbitrarily small by choosing $N$ large enough. This proves Erdős' theorem for $f(p) \neq f(q)$ ($f(p) \neq 0$, $f(q) \neq 0$). If for some sequence $f(p_1) = f(p_2) = \ldots$, then, considering the expression

$$ \sum_{f(p) = y_1} \frac{1}{p} \sum_{f(p) = y_1} \frac{1}{p} \cos \left( \frac{T_y}{p} - 1 \right) \frac{1}{p} $$

instead of

$$ \sum_{f(p) = y_1} \frac{1}{p} \cos \left( \frac{T_y}{p} - 1 \right) \frac{1}{p} $$

one can repeat the argument above and our statement follows again.

References


MATH. DEPT. SUNY AT STONY BROOK
MATH. INST. DER ALBERT-LUDWIGS-UNIVERSITÄT, FREIBURG I. BR.

Received on 7. 7. 1973

---

Some remarks on the decomposition of a rational prime
in a Galois extension

by

M. Bhaskaran (Perth, W. Australia)

1. **Introduction.** Not much is known about the law of decomposition of rational primes in a Galois extension if the extension is not abelian. It is known that only for abelian extensions we can give a simple law of decomposition depending on the residue of the given prime with respect to a certain modulus. The object of the present paper is to get some information about the relationship between the number of prime divisors of a given rational prime and a rational prime which is ramified in a Galois extension. This information also helps us to get some idea about the class numbers of certain algebraic number fields. For example, the well-known result that the class number of the field $Q(\sqrt{a})$ ($r$ odd prime and $a$ is divisible by a prime of the form $rt+1$) is divisible by $r$ could be deduced from our result.

I would like to thank Professor A. Schinzel and the referee for their valuable comments in the preparation of the paper.

2. **Notations and preliminaries.** Throughout this paper, $Q$ denotes the rational number field, $k$ denotes a finite Galois extension of $Q$ with Galois group $G$ and $\mathcal{O}_k$ denotes the ring of integers of $k$. The prime ideals of $\mathcal{O}_k$ are called $k$-primes. $p$ and $q$ denote distinct rational primes and $\mathfrak{P}$ and $\mathfrak{Q}$ denote the $k$-primes lying above $p$ and $q$ respectively. $\mathfrak{G}_l$ denotes the number of distinct $k$-primes lying above the rational prime $l$. $e_l$ and $f_l$ denote the ramification index and residue class degree respectively of $l$. $G_k$ and $T_k$ denote the decomposition group and inertia group of $l$. They are subgroups of $G$ of order $e_l f_l$ and $e_l$ respectively. $T_k$ is a subgroup of $G_k$ and its elements induce the trivial automorphism on the residue field of $L$. $g_l$ will be the number of cosets of $G_k$ in $G$. Let $G = \bigcup_{j=1}^{g_l} \tau_j G_k$ be a coset decomposition of $G_k$ in $G$. Then the $k$-primes $\tau_j \mathfrak{G}$ are precisely the distinct $k$-primes lying above $l$. 
If \( x \) is the smallest positive integer such that \( q^x \equiv 1 \mod p \), then we say that \( x \) is the order of \( q \) with respect to \( p \) and it is denoted by \( \text{ord}_q \). \((a, b, c, \ldots)\) denotes the G.C.F. of \( a, b, c, \ldots \); \( a \mid b \) means \( a \) divides \( b \); \( a^\omega \equiv b \mod p \) means \( a^\omega \equiv b \mod p \) but \( a^{\omega+1} \not\equiv b \).

3. Main results. We first prove the following

Theorem 1. Let \((k, \mathbb{Q}) = a \) and \( e \) be a positive integer such that \((e, n/e) = 1 \) and \( e|(g_{a}, b, p - 1) \). Then if \( q \) splits into principal \( k \)-primes,

\[
e | c(p - 1)/\text{ord}_q q,
\]

where

\[
c = \begin{cases} 1 & \text{if } e \text{ is odd or } p = 1 \mod 2e, \\ 2 & \text{otherwise}. \end{cases}
\]

Proof. If \( e = 1 \), there is nothing to prove. So let us assume \( e > 1 \). Let \( u \) be a prime factor of \( e \) and \( u \mid e \). Without loss of generality, we prove the theorem when \( e \) is replaced by \( u^e \). Take any Sylow \( u \)-subgroup \( E \) of \( T_\mathbb{Q} \) which is of order \( u^e \) since \((u^e, n/u^e) = 1 \). The elements of \( E \) belong to distinct cosets of \( G_{a} \); for otherwise, if \( \tau_1 \) and \( \tau_2 \) of \( E \) belong to the same coset of \( G_{a} \), then \( \tau_1 \tau_2^{-1} \in G_{a} \) and so its order divides \( u^e \), which is a contradiction. Let the elements of \( E \) be \( \tau_i \) \((i = 1, 2, \ldots, u^e)\), \( \tau_1 \) being the identity of \( G \).

Extend \( E \) to a set \( S \) consisting of elements in \( G \) which represent the \( g_i \) cosets of \( G_{a} \) in \( G \). Let \( \tau_i \) \((i = 1, 2, \ldots, u^e)\) (the first \( u^e \) elements being those of \( E \)) be the elements in \( S \). Let the coset of \( \tau_i \) be denoted by \( \tau_i \) and \( S \) be the set of these cosets. Now, we shall arrange \( g_i \) elements of \( G \) which represent the distinct cosets in \( g_i/u^e \) columns in a suitable manner. For this, first put \( \tau_1, \tau_2, \ldots, \tau_u \) in the first column. Take a \( \tau_i \) from \( S \) not belonging to the cosets \( \tau_1, \tau_2, \ldots, \tau_u \) and put \( \tau_1, \tau_2, \tau_1, \ldots, \tau_u, \tau_i \) in the second column. It is easy to see that the \( 2u^e \) elements in these two columns belong to \( 2u^e \) distinct cosets. Take a \( \tau_i \) from \( S \) not belonging to the cosets of the \( 2u^e \) elements already arranged. Put \( \tau_1, \tau_2, \tau_1, \ldots, \tau_u, \tau_i \) in the third column. We easily see that all the \( 3u^e \) elements thus arranged belong to \( 3u^e \) distinct cosets. Repeating this process \( g_i/u^e \) times, we get the desired result. Thus, we get a set of \( g_i \) elements of \( G \), which represent the \( g_i \) cosets in \( S \), in the form \( \bigcup_{i=1}^{u^e} \tau_i \mathcal{E} \) where \( \mathcal{E} \) consists of \( g_i/u^e \) elements say \( \sigma_1, \sigma_2, \ldots, \sigma_{g_i/u^e} \).

Now, let us assume that the \( k \)-primes lying above \( q \) are principal and write the factorization of \((q)\) in the following manner:

\[
(q) = \prod_{i=1}^{\sigma_q} \tau_i \mathcal{Q}^\sigma_q = \prod_{j=1}^{u^e} \tau_j \left( \prod_{i=1}^{\sigma_j} \tau_i \mathcal{Q}^\sigma_i \right)
\]

where \( \mathcal{Q} \) is a principal \( k \)-prime lying above \( q \). Hence

\[
q = s \prod_{j=1}^{u^e} \tau_j \left( \prod_{i=1}^{\sigma_j} \tau_i \mathcal{Q}^\sigma_i \right)
\]

where \( s \in \mathcal{E} \) and \( s \) is a unit in \( \mathcal{E} \) such that \( \tau_i \) \((i = 1, 2, \ldots, u^e)\) fix \( s \). Applying \( n/g_i \) automorphisms \( \nu_i \) \((i = 1, 2, \ldots, u/g_i)\) of \( G_{a} \) on both sides, we get

\[
g_i s^{\nu_i} = s \prod_{i=1}^{u^e} \tau_i \left( \prod_{j=1}^{\sigma_j} \tau_j \right)
\]

for some \( a \in \mathcal{E} \) and \( a \) a unit \( s' \) which remains fixed under all the automorphisms of \( G \), i.e. \( s' = \pm 1 \).

Now

\[
\tau_i a = a \mod \mathcal{Q} (j = 1, 2, \ldots, u^e)
\]

since \( \tau_i a \in T_\mathcal{E} \) and so induces the trivial automorphism on the residue class field of \( \mathcal{Q} \).

Hence

\[
\pm q s^{\nu_i} = a \mod \mathcal{Q}.
\]

Since \((s, n/e) = 1 \) and \( e|g_{a} \), we have \((u^e, n/g_i) = 1 \). Then, it follows that

\[
\pm q = b \mod \mathcal{Q}
\]

for some \( \beta \in \mathcal{E} \).

This shows that, if \( u \) is odd or \( p = 1 \mod 2^{e+1} \), \( q \) is a \( u^e \)-th power \( \mod \mathcal{Q} \). Otherwise, \( q \) is a \( u^e/2 \)-th power \( \mod \mathcal{Q} \).

Hence

\[
\text{ord}_q \left( \frac{p^u - 1}{u}, p - 1 \right)
\]

if \( u \) is an odd prime or \( p = 1 \mod 2^{e+1} \) and

\[
\text{ord}_q \left( \frac{p^u - 1}{u^e}, p - 1 \right)
\]

otherwise.

Now

\[
(p^u - 1, p - 1)|f_p(p - 1)
\]

and

\[
\text{if } u \text{ is an odd prime or } p = 1 \mod 2^{e+1} \text{ and } u|2(p - 1)/\text{ord}_q q \text{ otherwise.}
\]

Consequently, we have

\[
u^e(p - 1)/\text{ord}_q q \text{ if } u \text{ is an odd prime or } p = 1 \mod 2^{e+1}
\]

and

\[
u^e/2(p - 1)/\text{ord}_q q \text{ otherwise.}
\]
Repeating our method for all other prime power factors of $e$ instead of $u'$, we get our theorem.

When the class number of $k$ is relatively prime to $n$, we can delete the condition on $q$ that it splits into principal $k$-primes and state the theorem in the following manner:

**Theorem 2.** Let $(k : Q) = n$ and let the class number of $k$ be relatively prime to $n$. Let $e$ be a positive integer such that

$$(e, n|e) = 1 \quad \text{and} \quad e|(g_q, e_p, p - 1).$$

Then

$$e|c(p - 1)/\text{ord}_e q$$

where $c = 1$ if $e$ is odd or $p = 1 \mod 2e$ and $c = 2$ otherwise.

**Proof.** Let $K$ be the Hilbert class field of $k$ and let $(K : k) = h$. Then $(h, n) = 1$ and $(K : Q) = nh$. Let $e_l^K$ and $g^K_l$ denote the ramification index of a $K$-prime lying above the rational prime $l$ and the number of distinct $K$-primes lying above $l$ respectively. Then, we can easily see that

$$(e, n|e) = 1 \quad \text{implies} \quad (e, nh|e) = 1$$

and

$$e|(g_q, e_p, p - 1) \quad \text{implies} \quad e|(g^K_q, e^K_p, p - 1).$$

Taking $K$ for $k$ in Theorem 1, we see that $e$ satisfies the required conditions and so the theorem follows since every $k$-prime splits into principal $K$-primes.

*Received on 28. 8. 1973* (444)

---

**Arithmetic euclidean rings**

**by**

**CLIFFORD QUEEN (Bethlehem, Penn.)**

---

1. **Introduction.** Let $A$ be an integral domain. We shall say that $A$ is a euclidean ring, or simply $A$ is euclidean, if there exists a map $\varphi : A - \{0\} \to \mathbb{N}$, $\mathbb{N}$ the non-negative integers, satisfying the following two properties:

1. If $a, b \in A - \{0\}$, then $\varphi(ab) = \varphi(a)$;
2. If $a, b \in A$, $b \neq 0$, then there exist $q, r \in A$ such that $a = bq + r$, where $r = 0$ or $\varphi(r) < \varphi(b)$.

It is easy to see that condition 1) is an unnecessary restriction; i.e., if there is a map $\varphi : A - \{0\} \to \mathbb{N}$ satisfying only condition 2), then there is always another map $\varphi'$, derived from $\varphi$, such that $\varphi'$ satisfies both 1) and 2). Further, it is apparently unknown whether one enlarges the class of euclidean integral domains by enlarging $\mathbb{N}$ to a well-ordered set of arbitrary cardinality, but this question will not concern us here except to say that whenever $A$ has finite residue classes; i.e., $A$ modulo any non-zero ideal is finite, then insisting on $\mathbb{N}$ as a set of values is no restriction. We refer the reader to an excellent paper by P. Samuel [3] in which all of the above and much more is exposed with great clarity.

Let $A$ be as above. We define subsets $A_n$ of $A$ for all $n \in \mathbb{N}$ by induction as follows: $A_1 = \{0\}$ and if $n \geq 1$, then $A_{n+1} = \bigcup_{m | n} A_m$. Finally $A_{\infty} = \{b \in A| b$ has a representative in $A_n$ of every residue class of $A$ modulo $b\}$. Setting $A_{\infty}' = \bigcup A_n$, $A$ is euclidean if and only if $A_{\infty}' = A$ (see Motzkin [6]). Further when $A_{\infty}' = A$ we get a map $\varphi : A - \{0\} \to \mathbb{N}$, where if $a \in A - \{0\}$ then there exists a unique $n \geq 0$ such that $a \in A_{n+1} - A_n$ and $\varphi(a) = n$. Now not only does $\varphi$ satisfy conditions 1) and 2) above, but if $\varphi'$ is any other map satisfying condition 2), then $\varphi'(a) < \varphi(a)$ for all $a \in A - \{0\}$. Hence Motzkin justifiably calls $\varphi$ the minimal algorithm for $A$.

Let $F$ be a global field, so $F$ is a finite extension of the rational numbers $\mathbb{Q}$ or $F$ is a function field of one variable over a finite field. Let $S$ be a non-empty finite set of prime divisors of $F$ such that $S$ contains all finite (i.e. archimedean) prime divisors. For each finite (i.e. non-archimedean)