which can be made arbitrarily small by choosing N large enough. This proves Erdös' 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

$$\sum_{f(p)=g_l} (\cos g_l Ty - 1) \sum_{f(p)=g_l} \frac{1}{p}$$

instead of

$$\sum \frac{\cos f(p) Ty - 1}{p}$$

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

References

[1] P. Erdös, *On the density of some sequences of numbers III*, J. London Math. Soc. 13 (1938), pp. 119–127.

[2] P. Erdös and A. Wintner, *Additive arithmetical functions and statistical independence*, Amer. J. Math. 61 (1939), pp. 713–721.

[3] M. Kac, *Statistical independence in probability, analysis and number theory*, Carus Math. Monographs, 1964.

[4] A. Rényi, *On the distribution of values of additive number-theoretical functions*, Publ. Math. 10 (1963), pp. 264–273.

[5] — *Probability Theory*, Amsterdam–London 1970.

[6] I. J. Schoenberg, *On asymptotic distributions of arithmetic functions*, Trans. Amer. Math. Soc. 39 (1936), pp. 315–330.

MATH. DEPT. SUNY AT STONY BROOK
MATH. INST. DER ALBERT-LUDWIGS-UNIVERSITÄT, Freiburg i. Br.

Received on 7. 7. 1973 (435)

ACTA ARITHMETICA XXVI (1974)

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 $Q(\sqrt[r]{a})$ (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. g_l denotes the number of distinct k-primes $\mathfrak{L}$ lying above the rational prime l. e_l and f_l denote the ramification index and residue class degree respectively of $\mathfrak{L}$. $G_{\mathfrak{L}}$ and $T_{\mathfrak{L}}$ denote the decomposition group and inertia group of $\mathfrak{L}$. They are subgroups of G of order $e_l f_l$ and e_l respectively. $T_{\mathfrak{L}}$ is a subgroup of $G_{\mathfrak{L}}$ and its elements induce the trivial automorphism on the residue class field of $\mathfrak{L}$. g_l will be the number of cosets of $G_{\mathfrak{L}}$ in G. Let $G = \bigcup_{j=1}^{g_l} \tau_j G_{\mathfrak{L}}$ be a coset decomposition of $G_{\mathfrak{L}}$ in G. Then the k-primes $\tau_j \mathfrak{L}$ are precisely the distinct k-primes lying above l.

If x is the smallest positive integer such that $q^x \equiv 1 \bmod p$, then we say that x is the *order* of q with respect to p and it is denoted by $\operatorname{ord}_p q$. $(a, b, c, \ldots)$ denotes the G.C.F. of $a, b, c, \ldots$, $a|b$ means a divides b, $a \nmid b$ means a does not divide b and $a^w \| b$ means $a^w | b$ but $a^{w+1} \nmid b$.

3. Main results. We first prove the following

THEOREM 1. *Let $(k: Q) = n$ and e be a positive integer such that $(e, n/e) = 1$ and $e|(g_q, e_p, p-1)$. Then if q splits into principal k-primes,*

$$e \mid c(p-1)/\operatorname{ord}_p q$$

where

$$c = \begin{cases} 1 & \text{if } e \text{ is odd or } p \equiv 1 \bmod 2e, \\ 2 & \text{otherwise.} \end{cases}$$

Proof. If $e = 1$, there is nothing to prove. So let us assume $e > 1$. Let u be a prime factor of e and $u^t \| e$. Without loss of generality, we prove the theorem when e is replaced by u^t. Take any Sylow u-subgroup E of $T_{\mathfrak{P}}$ which is of order u^t since $(u^t, n/u^t) = 1$. The elements of E belong to distinct cosets of $G_{\mathfrak{Q}}$; for otherwise, if τ_i and τ_j of E belong to the same coset of $G_{\mathfrak{Q}}$, then $\tau_i \tau_j^{-1} \in G_{\mathfrak{Q}}$ and so its order divides n/u^t which is a contradiction. Let the elements of E be τ_i $(i = 1, 2, \ldots, u^t)$, τ_1 being the identity of G.

Extend E to a set S consisting of elements in G which represent the g_q cosets of $G_{\mathfrak{Q}}$ in G. Let τ_s $(s = 1, 2, \ldots, g_q)$ (the first u^t elements being those of E) be the elements in S. Let the coset of τ_s be denoted by $\bar{\tau}_s$ and $\bar{S}$ be the set of these cosets. Now, we will arrange g_q elements of G which represent the distinct cosets in g_q/u^t columns in a suitable manner. For this, first put $\tau_1, \tau_2, \ldots, \tau_{u^t}$ in the first column. Take a τ_i from S not belonging to the cosets $\bar{\tau}_1, \bar{\tau}_2, \ldots, \bar{\tau}_{u^t}$ and put $\tau_1\tau_i, \tau_2\tau_i, \ldots, \tau_{u^t}\tau_i$ in the second column. It is easy to see that the $2u^t$ elements in these two columns belong to $2u^t$ distinct cosets. Take a τ_j from S not belonging to the cosets of the $2u^t$ elements already arranged. Put $\tau_1\tau_j, \tau_2\tau_j, \ldots, \tau_{u^t}\tau_j$ in the third column. We easily see that all the $3u^t$ elements thus arranged belong to $3u^t$ distinct cosets. Repeating this process g_q/u^t times, we get the desired result. Thus, we get a set of g_q elements of G, which represent the g_q cosets in $\bar{S}$, in the form $\bigcup_{i=1}^{u^t} \tau_i F$ where F consists of g_q/u^t elements say $\sigma_1, \sigma_2, \ldots, \sigma_{g_q/u^t}$.

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

$$(q) = \prod_{i=1}^{g_q} \tau_i \mathfrak{Q}^{e_q} = \prod_{j=1}^{u^t} \tau_j \Big(\prod_{i=1}^{g_q/u^t} \sigma_i \mathfrak{Q}^{e_q}\Big)$$

where $\mathfrak{Q}$ is a principal k-prime lying above q. Hence

$$q = \varepsilon \prod_{j=1}^{u^t} \tau_j \Big(\prod_{i=1}^{g_q/u^t} \sigma_i \gamma^{e_q}\Big)$$

where $\gamma \in \mathcal{O}_k$ and generates $\mathfrak{Q}$ and ε is a unit in $\mathcal{O}_k$ such that τ_i $(i = 1, 2, \ldots, g_q)$ fix ε. Applying n/g_q automorphisms ν_s $(s = 1, 2, \ldots, n/g_q)$ of $G_{\mathfrak{Q}}$ on both sides, we get

$$q^{n/g_q} = \varepsilon' \prod_{s=1}^{n/g_q} \nu_s \Big(\prod_{j=1}^{u^t} \tau_j a\Big)$$

for some $a \in \mathcal{O}_k$ and a unit ε' which remains fixed under all the automorphisms of G, i.e. $\varepsilon' = \pm 1$.

Now

$$\tau_j a \equiv a \bmod \mathfrak{P} \quad (j = 1, 2, \ldots, u^t)$$

since $\tau_j \in T_{\mathfrak{P}}$ and so induces the trivial automorphism on the residue class field of $\mathfrak{P}$.

Hence

$$\pm q^{n/g_q} \equiv a^{u^t} \bmod \mathfrak{P}.$$

Since $(e, n/e) = 1$ and $e|g_q$, we have $(u^t, n/g_q) = 1$. Then, it follows that

$$\pm q \equiv \beta^{u^t} \bmod \mathfrak{P}$$

for some $\beta \in \mathcal{O}_k$.

This shows that, if u is odd or $p \equiv 1 \bmod 2^{t+1}$, q is a u^t-th power $\bmod \mathfrak{P}$. Otherwise, q is a $u^t/2$-th power $\bmod \mathfrak{P}$.

Hence

$$\operatorname{ord}_p q \,\Big|\, \Big(\frac{p^{f_p}-1}{u^t}, p-1\Big)$$

if u is an odd prime or $p \equiv 1 \bmod 2^{t+1}$ and

$$\operatorname{ord}_p q \,\Big|\, \Big(\frac{p^{f_p}-1}{u^t/2}, p-1\Big)$$

otherwise.

Now

$$(p^{f_p}-1, p-1) \mid f_p(p-1)$$

and

$$(u^t, f_p) = 1.$$

Consequently, we have

$$u^t \mid (p-1)/\operatorname{ord}_p q \quad \text{if } u \text{ is an odd prime or } p \equiv 1 \bmod 2^{t+1}$$

and

$$u^t \mid 2(p-1)/\operatorname{ord}_p q \quad \text{otherwise.}$$

Repeating our method for all other prime power factors of e instead of u^t, 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 $(k\colon Q) = n$ 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

$$e\,|\,c(p-1)/\mathrm{ord}_p q$$

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

Proof. Let K be the Hilbert class field of k and let $(K\colon k) = h$. Then $(h, n) = 1$ and $(K\colon Q) = nh$. Let e_l^K and g_l^K 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

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

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 20. 8. 1973 (444)

ACTA ARITHMETICA
XXVI (1974)

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 $\varphi\colon A-\{0\}\to N$, N the non-negative integers, satisfying the following two properties:

1) If $a, b \in A-\{0\}$, then $\varphi(ab) \geqslant \varphi(a)$;

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 $\varphi\colon A-\{0\}\to N$ satisfying only condition 2), then there is always another map φ', derived from φ, such that φ' satisfies both 1) and 2). Further, it is apparently unknown whether one enlarges the class of euclidean integral domains by enlarging 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 N as a set of values is no restriction. We refer the reader to an excellent paper by P. Samuel [8] 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 $n \in N$ by induction as follows: $A_0 = \{0\}$ and if $n \geqslant 1$, then $A_n' = \bigcup_{a<n} A_a$. Finally $A_n = \{b \in A\,|$ there is a representative in A_n' of every residue class of A modulo $bA\}$. Setting $A' = \bigcup_{n \in N} A_n$, A is euclidean if and only if $A' = A$ (see Motzkin [6]). Further when $A' = A$ we get a map $\varphi\colon A-\{0\}\to N$, where if $x \in A-\{0\}$ then there exists a unique $n \geqslant 0$ such that $x \in A_{n+1}-A_n$ and $\varphi(x) = n$. Now not only does φ satisfy conditions 1) and 2) above, but if φ' is any other map satisfying condition 2), then $\varphi(x) \leqslant \varphi'(x)$ for all $x \in A-\{0\}$. Hence Motzkin justifiably calls φ the minimal algorithm for A.

Let F be a global field, so F is a finite extension of the rational numbers 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 infinite (i.e. archimedean) prime divisors. For each finite (i.e. non-archimedean)