ON A PROBLEM OF SCHINZEL CONCERNING PRINCIPAL DIVISORS IN ARITHMETIC PROGRESSIONS

Thesis for the Degree of Ph. D.

MICHIGAN STATE UNIVERSITY
CHARLES JOHN PARRY

1970

This is to certify that the

thesis entitled

"ON A PROBLEM OF SCHINZEL
CONCERNING PRINCIPAL DIVISORS
IN ARITHMETIC PROGRESSIONS"

presented by

Charles John Parry

has been accepted towards fulfillment
of the requirements for

Ph.D. degree in Mathematics

Major professor

Date May 4, 1970

O-169

ABSTRACT

ON A PROBLEM OF SCHINZEL CONCERNING PRINCIPAL DIVISORS IN ARITHMETIC PROGRESSIONS

BY

Charles J. Parry

The following problem was proposed by A. Schinzel at the A. M. S. Number Theory Summer Institute held at Stony Brook in July 1969: "Let $f(x)$ be a primitive polynomial and k an algebraic number field. Do there exist infinitely many integers x such that $f(x)$ factors into principal ideals in k? (unknown even for f linear)."

I have solved this problem in the affirmative when f is linear. My proof uses Frobenius and Artin symbols in certain extensions of the Hilbert class field of k.

ON A PROBLEM OF SCHINZEL CONCERNING PRINCIPAL DIVISORS IN ARITHMETIC PROGRESSIONS

BY

Charles John Parry

A THESIS

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

Department of Mathematics

1970

ACKNOWLEDGMENTS

I would like to express my thanks to my advisor Charles R. MacCluer for his helpful suggestions and for the many hours he has spent discussing this problem with me. Also I would like to thank Andrzej Schinzel for calling the problem to my attention and for the helpful comments which he has communicated to me.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

1. STATEMENT OF PROBLEM

The following problem was proposed by Andrzej Schinzel at the A. M. S. Number Theory Summer Institute held at Stony Brook, New York during July, 1969:

> Question I: "Let $f(x)$ be a primitive polynomial and K an algebraic number field. Do there exist infinitely many integers x such that $f(x)$ factorizes in K into principal ideals? (unknown even for f linear)."

In this paper I shall prove the answer is yes when f is linear. It has been noted [1] for polynomials of higher degree that the following additional assumptions on $f(x)$ are necessary:

(i) The content of any factor of $f(x)$ in K is principal (MacCluer).

(ii) Each fixed divisor of $f(x)$ is principal (Schinzel).

In the linear case, i.e. when $f(x) = mx + b$, it seems reasonable to ask the slightly stronger

<u>Question II</u>: Do there exist infinitely many primes of the form $mx + b$ which have principal prime factors in K?

Although the answer to question II can be seen to be no by an example, this question is worth examining more closely as it suggests an approach to the first question. First, however, I shall present some basic definitions and theorems of algebraic number theory and class field theory which are not readily available in the literature.

2. SOME HILBERT THEORY.

Throughout this section let K be a finite galois extension of the number field k with galois group G of order n. Let R and S denote the rings of algebraic integers in k and K respectively. Suppose $\mathfrak{P}$ is a prime of K.

<u>Definition A</u>: $Z(\mathfrak{P}) = \{\sigma | \sigma \in G, \sigma(\mathfrak{P}) = \mathfrak{P}\}$ is called the <u>decomposition group</u> of $\mathfrak{P}$.

<u>Definition B</u>: $T(\mathfrak{P}) = \{\sigma | \sigma(x) \equiv x \mod \mathfrak{P} \text{ for all } x \in S\}$ is called the <u>inertial group</u> of $\mathfrak{P}$. The subfield I of K corresponding to T is called the <u>inertial field</u> of $\mathfrak{P}$.

It is easy to verify that $Z(\mathfrak{P})$ is a subgroup of G and that $T(\mathfrak{P})$ is a normal subgroup of $Z(\mathfrak{P})$. Furthermore suppose $\mathfrak{p} = \mathfrak{P} \cap k$ and $\mathfrak{p} = (\mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_g)^e$ in K where $\mathfrak{P}_1 = \mathfrak{P}$. Then since G acts transitively on the primes $\mathfrak{P}_1,\ldots,\mathfrak{P}_g$ it follows that the index $(G:Z) = g$ and so $Z(\mathfrak{P})$ has order n/g.

<u>Definition C</u>: The sequence of groups

$$G \supseteq Z \supseteq T \supseteq 1$$

is called the (short) <u>Hilbert sequence</u> of $\mathfrak{P}$ over k.

The importance of the Hilbert sequence is due to the following:

<u>Result I</u>: For each prime $\mathfrak{P}$ of K

$$Z(\mathfrak{P}) \;/\; T(\mathfrak{P})$$

is naturally isomorphic to

$$G(S/\mathfrak{P} \mid R/\mathfrak{p}),$$

the galois group of $S/\mathfrak{P}$ over $R/\mathfrak{p}$.

<u>Result II</u>: $\mathfrak{P}$ is totally ramified over its inertial field $I(\mathfrak{P})$. Moreover, $\mathfrak{P}_I = \mathfrak{P} \cap I$ is unramified over k and $(T:1) = (K:I) = e$, the ramification index of $\mathfrak{P}$ over k.

For proofs of these results we refer the reader to Weiss [2].

Now suppose $\mathfrak{P}$ is unramified over k, so $T(\mathfrak{P}) = 1$ and

$$Z(\mathfrak{P}) \cong G(S/\mathfrak{P} \mid R/\mathfrak{p}).$$

But $R/\mathfrak{p} = GF(\|\mathfrak{p}\|_k)$ and $S/\mathfrak{P} = GF(\|\mathfrak{p}\|_k^f)$ where $\|\mathfrak{p}\|_k$ is the absolute norm of $\mathfrak{p}$. Thus $G(S/\mathfrak{P} \mid R/\mathfrak{p})$ is cyclic and generated by the map

$$x \longmapsto x^{\|\mathfrak{p}\|_k}.$$

Hence we can choose a generator σ of $Z(\mathfrak{P})$ so that

$$\sigma(x) \equiv x^{\|\mathfrak{p}\|_k} \mod \mathfrak{P}$$

for all $x \in S$. This unique element of $Z(\mathfrak{P})$ is called the <u>Frobenius Automorphism</u> of $\mathfrak{P}$ over k. The symbol

$$\left[\frac{K/k}{\mathfrak{P}}\right] = \sigma$$

is called the <u>Frobenius Symbol</u> of $\mathfrak{P}$ over k.

<u>Remark I</u>: The Frobenius automorphisms of the prime factors of $\mathfrak{p}$ are all conjugate under G.

<u>PROOF</u>: Note that for $\tau \in G$, $x \in S$

$$\sigma(\tau^{-1}x) \equiv (\tau^{-1}x)^{\|\mathfrak{p}\|_k} \equiv \tau^{-1}(x^{\|\mathfrak{p}\|_k}) \mod \mathfrak{P}$$

so that

$$\tau\,\sigma\,\tau^{-1}(x) \equiv x^{\|\mathfrak{p}\|_k} \mod (\tau\mathfrak{P}).$$

Hence

$$\left[\frac{K/k}{\tau\mathfrak{P}}\right] = \tau\left[\frac{K/k}{\mathfrak{P}}\right]\tau^{-1}.$$

The conjugacy class to which the Frobenius symbols of the factors of $\mathfrak{p}$ belong is called the Artin Symbol of $\mathfrak{p}$ and is denoted by $\left(\frac{K/k}{\mathfrak{p}}\right)$. If G is abelian then the Artin Symbol becomes a unique element of G.

Now assume that $k \subset L \subset K$ and let $P = \mathfrak{P} \cap L$.

Remark II: If P is of degree f over k then

$$\left[\frac{K/L}{\mathfrak{P}}\right] = \left[\frac{K/k}{\mathfrak{P}}\right]^f$$

PROOF: Let $\left[\frac{K/k}{\mathfrak{P}}\right] = \sigma$.

Then $\sigma^f(x) \equiv x^{\|\mathfrak{p}\|_k^f} \mod \mathfrak{P}$ for all $x \in S$. But $\|\mathfrak{p}\|_k^f = \|P\|_L$.

Remark III: If L/k is galois then

$$\left[\frac{L/k}{P}\right] = \left[\frac{K/k}{\mathfrak{P}}\right]\Bigg|_L .$$

PROOF: Obvious.

I now consider the Artin Symbol in the case that K is a cyclotomic extension of k, i.e. $K = k(\zeta)$ where ζ is a primitive m^{th} root of unity. In this case all elements of the galois group $G(k(\zeta)/k)$ can be obtained by a substitution of the form

$$\zeta \longmapsto \zeta^a$$

for some a with $(a,m) = 1$.

<u>Remark IV</u>: Suppose $\sigma_a(\zeta) = \zeta^a$ is in $G(k(\zeta)/k)$ and $(\mathfrak{p}, m) = 1$, then

$$\left(\frac{k(\zeta)/k}{\mathfrak{p}}\right) = \sigma_a \Leftrightarrow \|\mathfrak{p}\|_k \equiv a \mod m.$$

<u>PROOF</u>: Note

$$\sigma_a(x) \equiv x^{\|\mathfrak{p}\|_k} \mod \mathfrak{p}$$

for all integers x of $k(\zeta)$. In particular

$$\sigma_a(\zeta) = \zeta^a \equiv \zeta^{\|\mathfrak{p}\|_k} \mod \mathfrak{p}.$$

However $\zeta^a \equiv \zeta^b \mod \mathfrak{p}$ implies

$$\zeta^a(1 - \zeta^{b-a}) \equiv 0 \mod \mathfrak{p}$$

and hence

$$1 - \zeta^{b-a} \equiv 0 \mod \mathfrak{p}.$$

Now if $b-a \not\equiv 0 \mod m$ then

$$m = \prod_{j=1}^{m-1} (1 - \zeta^j) \equiv 0 \mod \mathfrak{p}$$

contradicting that $(\mathfrak{p}, m) = 1$. Thus

$$b - a \equiv 0 \mod m.$$

Substituting $\|\mathfrak{p}\|_k$ for b we get

$$\|\mathfrak{p}\|_k \equiv a \mod m.$$

From Result II we obtain some properties of inertial fields. First,

<u>Lemma I</u>: If $k \subset k' \subset K$ and T' is the inertial group of $\mathfrak{P}$ over k', then $T' = G \cap T$ where $G' = G(K/k')$.

PROOF: Clear from the definition.

Corollary A: (Maximal Property) If $\mathfrak{P} \cap k'$ is unramified over k then $k' \subset I(\mathfrak{P})$.

PROOF: Let I' be the inertial field of $\mathfrak{P}$ over k'. Then $G(K/I') = T' = T \cap G'$, hence $I \subset I'$. But $\mathfrak{P} \cap I'$ is unramified over k' and hence over k. Thus $I = I'$ and $k' \subset I' = I$.

Corollary B: If a prime $\mathfrak{p}$ of k is unramified in k', then it is unramified in the galois closure $\overline{k'}$ of k'.

PROOF: Note that $\mathfrak{p}$ is unramified in each conjugate field of k' since it has a factorization there identical to that in k. If $\mathfrak{P}$ is any factor of $\mathfrak{p}$ in $\overline{k'}$ then the inertial field $I(\mathfrak{P})$ contains k' and all its conjugates by Corollary A. Thus $I = \overline{k'}$.

3. THE CEBOTAREV DENSITY THEOREM

In this section I state the theorem which is the key to most results of this paper. But first,

Definition: Let Π be a set of prime ideals of k. The limit

$$d(\Pi) = \lim_{s\to 1^+} \sum_{\mathfrak{p}\in\Pi} 1/\|\mathfrak{p}\|_k^s \Big/ \sum_{\mathfrak{p}\in k} 1/\|\mathfrak{p}\|_k^s$$

(if it exists) is called the Dedekind density of Π.

Result: The set of primes $\mathfrak{p}$ in k of degree greater than 1 over Q has Dedekind density 0.

PROOF: As $s \to 1^+$

$$\sum_{\substack{\text{degree} \\ \mathfrak{p}>1}} \frac{1}{\|\mathfrak{p}\|_k^s} \leq (k:Q) \sum_{p\in Q} \frac{1}{p^{2s}} = O(1)$$

Cebotarev Density Theorem: If $\sigma \in G(K/k)$, then the Dedekind density of all primes $\mathfrak{p}$ of k with

$$\left(\frac{K/k}{\mathfrak{p}}\right) = \mathfrak{K}_G(\sigma)$$

is

$$|\mathfrak{K}_G(\sigma)| \;/\; (G:1).$$

($\mathfrak{K}_G(\sigma)$ denotes the conjugacy class of σ in G and $|\mathfrak{K}_G(\sigma)|$ denotes the order of this class).

Corollary: The set of primes $\mathfrak{P}$ of K with $\left[\frac{K/k}{\mathfrak{P}}\right] = \sigma$ has Dedekind density $1/(G:1)$.

Recall the Dedekind zeta function $\zeta_K(s)$ of a number field K is defined to be the series

$$\zeta_K(s) = \sum_{A\in K} 1/\|A\|_K^s$$

where A runs through all integral ideals of K. It is easy to see for $\text{Re } s > 1$

$$\zeta_K(s) = \prod_P (1 - 1/\|P\|_K^s)^{-1}$$

where the product is over all prime ideals of K. Now for any number field K, $\zeta_K(s)$ can be shown by analytic continuation to have a simple pole at $s = 1$. Now

$$\begin{aligned} \log \zeta_K(s) &= \log \prod_P (1 - \|P\|_K^{-s})^{-1} \\ &= -\sum_P \log (1 - \|P\|_K^{-s}) \\ &= \sum_P \|P\|_K^{-s} + \sum_P \sum_{j=2}^{\infty} \|P\|_K^{-js} \\ &= \sum_P \|P\|_K^{-s} + O(1). \end{aligned}$$

Since $\zeta_k(s)$ has a simple pole at $s = 1$ we have

$$\lim_{s\to 1} (s-1)\, \zeta_k(s) = c \quad \text{for some } c > 0.$$

Hence for $s > 1$,

$$\log \zeta_K(s) = -\log (s-1) + O(1)$$

and so as $s \to 1^+$,

$$\log \zeta_K(s) \sim -\log (s-1).$$

This gives the important

<u>Result</u>: For any two number fields K and L, as $s \to 1^+$,

$$\sum_{P\in K} 1/\|P\|_K^s \sim \sum_{P\in L} 1/\|P\|_L^s \sim -\log (s-1).$$

Now I prove

<u>Lemma II</u>: A finite extension K of the number field k is galois over k if and only if almost every prime $\mathfrak{p}$ of k that has one linear factor in K splits completely in K.

<u>PROOF</u>: If K/k is galois, then the condition follows easily from Kummer's Theorem. Conversely assume the condition holds. Let Π be the set of primes of k which splits completely in K. Since a prime splits completely in K if and only if it splits completely in $\bar{K}$, the galois closure of K, it follows easily that

$$d(\Pi) = 1/(\bar{K}:k).$$

However

$$\sum_{P \in K} 1/\|P\|_K^s = \sum_{P \in K}{}' 1/\|P\|_K^s + O(1)$$

where $\sum'$ indicates summation over all primes P of K which are linear and unramified over k.

But $\displaystyle\sum_{P \in K}{}' 1/\|P\|_K^s = (K:k) \sum_{\mathfrak{p} \in \Pi} 1/\|\mathfrak{p}\|_k^s + O(1).$

So

$$1 = (K:k) \quad d(\Pi) = (K:k)/(\bar{K}:k)$$

Hence $K = \bar{K}$.

4. RESULTS FROM CLASS FIELD THEORY.

By the class field $CF(k)$ of the number field k I mean the Hilbert class field of k, that is, the maximal abelian unramified extension of k. Most of the properties of the Hilbert class field can be summarized in the

<u>Artin Reciprocity Theorem</u>: The homomorphism defined by linearly extending the map

$$\mathfrak{p} \longmapsto \left(\frac{CF(k)/k}{\mathfrak{p}} \right)$$

to all of I, the group of fractional ideals of k, is surjective and has kernel H, the group of principal ideals of k. Thus the galois group of CF(k)/k is canonically isomorphic to the ideal class group of k.

I now prove the useful

<u>Lemma III</u>: If K/k is galois then CF(K)/k is galois.

<u>PROOF</u>: Suppose $\mathfrak{P}$ is a prime of K that is linear over k. If $\mathfrak{p} = \mathfrak{P} \cap k$ then $\mathfrak{p}$ has a linear factor $P = \mathfrak{P} \cap K$ in K and since K/k is galois, $\mathfrak{p}$ splits completely in K. However P is principal by Artin reciprocity and since K/k is galois, all conjugate factors P′ of P in K are principal. So again by Artin reciprocity each conjugate factor P′ gains degree 1 in CF(K). Hence $\mathfrak{p}$ must split completely and by Lemma II, CF(K)/k is galois.

CHAPTER II

PRELIMINARY RESULTS

1. AN EXAMPLE

The following example (MacCluer) shows that the answer to question II is no. (A. Schinzel has informed me that a similar counterexample was found earlier by J. Tate.)

The number field $Q(\sqrt{10})$ has class number $h = 2$ and Hilbert class field

$$CF(Q(\sqrt{10})) = Q(\sqrt{2},\sqrt{5}).$$

According to Artin reciprocity, a rational prime $p \nmid 2, 5$ has non-principal divisors in $Q(\sqrt{10})$ if and only if p splits in $Q(\sqrt{10})$ into two distinct prime divisors, each of which remains prime in $Q(\sqrt{2},\sqrt{5})$. In Legendre symbols this is equivalent to

$$\left(\frac{2}{p}\right) = \left(\frac{5}{p}\right) = -1$$

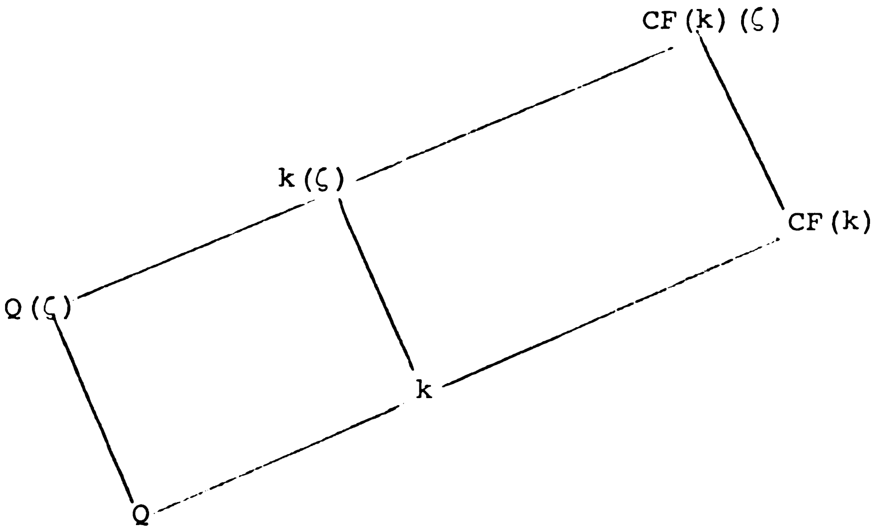
which obtains if and only if $P \equiv \pm 3, \pm 13 \pmod{40}$. Thus for instance, no prime of the form $p = 40x + 3$ has principal divisors in $Q(\sqrt{10})$.

2. SPECIAL CASES

Now question II is worthy of closer examination as it suggests an approach to the first question and is of some interest in itself. Specifically I shall prove:

<u>Theorem I</u>: Let k be a number field galois over Q, $CF(k)$ the class field of k, and ζ a primitive m-th root of unity. If $CF(k) \cap k(\zeta) = k$ and if $k \cap Q(\zeta) = Q$, then for each $(a,m) = 1$ there are infinitely many primes $p \equiv a \pmod{m}$ which split principally and completely in k. (I will say a rational prime p <u>splits principally</u> in k if each prime factor of p in k is principal in k.)

<u>PROOF</u>: We have the following Artin diagram



A prime $\mathfrak{p}$ of k with Artin Symbol $\left(\frac{k(\zeta)/k}{\mathfrak{p}}\right) = \sigma_a$, where $\sigma_a(\zeta) = \zeta^a$, has absolute norm $\|\mathfrak{p}\|_k \equiv a \mod m$. Thus if in addition $\mathfrak{p}$ is linear over Q then $\|\mathfrak{p}\|_k = p \equiv a \mod m$. It now only remains to produce infinitely many such principal primes $\mathfrak{p}$, i.e., with Artin symbol $\left(\frac{CF(k)/k}{\mathfrak{p}}\right) = 1$.

But by hypothesis the galois group

$$G(CF(k)(\zeta)/k) \cong G(CF(k)/k) x G(k(\zeta)/k).$$

Thus by the Cebotarev density theorem $1/h\,\varphi(m)$ of the primes of k have $\left(\frac{CF(k)(\zeta)/k}{\mathfrak{p}}\right) = 1 \times \sigma_a$, where h is the class number of k.

But this means

$$\left(\frac{k(\zeta)/k}{\mathfrak{p}}\right) = \sigma_a \text{ and } \left(\frac{CF(k)/k}{\mathfrak{p}}\right) = 1.$$

Since almost all primes of k are linear over Q, we need only consider such primes $\mathfrak{p}$ of k. But this means $\|\mathfrak{p}\|_k = p \equiv a \mod m$. Also $\mathfrak{p}$ principal and k/Q galois implies p splits principally in k. Thus at least $1/h\cdot\varphi(m)\cdot(k:Q)$ of the rational primes p split principally and completely in k and satisfy

$$p \equiv a \mod m.$$

<u>Corollary I</u>: Let k be a number field (not necessarily galois over Q) and Δ be the discriminant of k. Suppose $(m,\Delta) = 1$, then there are infinitely many primes $p \equiv a \pmod m$ which split principally and completely in k.

<u>PROOF</u>: Since $(\Delta,m) = 1$, every prime divisor of m is unramified in k and hence unramified in the galois closure $\bar{k}$ of k. However, the primes which ramify in $Q(\zeta)$ are exactly the divisors of m and so $Q(\zeta) \cap \bar{k} = Q$. From this it follows that

$$[CF(\bar{k}) \cap \bar{k}(\zeta):\bar{k}] = [(CF(\bar{k}) \cap \bar{k}(\zeta)) \cap Q(\zeta):Q].$$

Now because $(\Delta, m) = 1$, no prime can ramify in the extension $(CF(\bar{k}) \cap \bar{k}(\zeta) \cap Q(\zeta))/Q$ and so this extension is of degree 1, hence $CF(\bar{k}) \cap \bar{k}(\zeta) = \bar{k}$. We can thus apply Theorem I to get infinitely many primes $p \equiv a \mod m$ which split principally and completely in $\bar{k}$ and hence also split principally and completely in k.

Remark: It is worth noting that there are always infinitely many positive rational primes $p \equiv 1 \mod m$ (for any m) which split principally and completely in any number field k.

PROOF: By the Cebotarev density theorem the set of primes which split completely in $CF(\bar{k})(\zeta)$ has positive density.

Also under certain hypothesis question II is true for all modulii m. I now prove

Theorem II: Suppose the number field k is galois over the rational numbers Q and has class number h. Let $n = (k:Q)$ and take $m > 1$ and a to be any integers with $(a,m) = 1$. If $(n,h) = 1$, then there are infinitely many rational primes p with

$$p \equiv a \mod m$$

which factor into principal ideals in k.

PROOF: Let $CF(k)$ be the Hilbert class field of k and let G and H denote the galois groups $G(CF(k)/Q)$ and $G(CF(k)/k)$ respectively. Then H has order h and is a normal subgroup of G. Also $(G:H) = (k:Q) = n$. Since $(n,h) = 1$, the Schur-Zassenhaus Lemma [3] applies to give a subgroup A of G for which G is semi-direct product of A and H. Let L be the subfield of $CF(k)$ with galois group $G(CF(k)/L) = A$. Note that $CF(k) = kL$ and that $k \cap L = Q$.

I now show that if a prime $\mathfrak{P}$ of $CF(k)$ has its Frobenius automorphism $\left[\frac{CF(k)/Q}{\mathfrak{P}}\right]$ in A, then $p = \mathfrak{P} \cap Q$ splits into principal prime ideals in k. We need only note that the restriction map

$$\sigma \longmapsto \sigma|_k$$

gives an isomorphism of $G(CF(k)/L)$ and $G(k/Q)$. Also

$$\left[\frac{CF(k)/Q}{\mathfrak{P}}\right]\Bigg|_k = \left[\frac{k/Q}{\mathfrak{P}\cap k}\right]$$

Thus if $\left[\frac{CF(k)/Q}{\mathfrak{P}}\right]$ is in A then $p = \mathfrak{P} \cap Q$ gains the same degree in both k and $CF(k)$. Since k/Q is normal, p splits into principal prime ideals in k.

Next we note that $L \cap Q(\zeta) = Q$ where ζ is an m-th root of unity. Suppose some rational prime q has ramification index e' in $L \cap Q(\zeta)$. Then e' divides $(L:Q) = h$. On the other hand e' must divide the ramification index e of q in $CF(k)$. But e divides n so e' also divides n. Hence $e' = 1$ and $L \cap Q(\zeta) = Q$. Therefore the substitution determined by

$$\sigma_a(\zeta) = \zeta^a \qquad (a,m) = 1$$

is in $G(L(\zeta)/L)$. By the Cebotarev density theorem, the set of primes P of L with Artin Symbol

$$\left(\frac{L(\zeta)/L}{P} \right) = \sigma_a$$

has positive density. Since almost all primes of L are of degree 1 over Q, we need only consider such primes P. Now $\left(\frac{L(\zeta)/L}{P} \right) = \sigma_a$ and P linear over Q implies

$$p = \|P\|_L \equiv a \mod m.$$

Now let $\mathfrak{P}$ be a divisor of P in $CF(k)$. Since P is linear over Q we have that $\left[\frac{CF(k)/Q}{\mathfrak{P}} \right]$ is in A and as was shown above, $p = \mathfrak{P} \cap Q$ must split into principal prime ideals in k. This gives the desired result.

CHAPTER III

RESOLUTION OF THE LINEAR CASE

As we have just seen, there are infinitely many primes $p \equiv a \mod m$ that split principally in k provided the modulus m contains no primes that ramify in k. On the other hand we have seen that there are no primes $p \equiv 3 \mod 40$ that split principally in $Q(\sqrt{10})$, a field in which both 2 and 5 ramify. We shall soon see that the non-existence of such primes is not solely because of the ramification of the factors 2 or 5 of $m = 40$, but because $m = 40$ has at least two distinct prime factors, both of which are ramified. For

<u>Theorem III</u>: Let k/Q be galois, ℓ be prime, $(a,\ell) = 1$, and $(m',\ell) = 1$. Then for any $n \geq 1$ there are infinitely many positive rational primes p which split principally in k with

$$p \equiv a \mod \ell^n$$

and

$$p \equiv 1 \mod m'.$$

Once that we have proved Theorem III we have an immediate solution to Question I for k/Q galois. That is:

<u>Theorem IV</u>: If k/Q is galois and $(a,m) = 1$, then there are infinitely many rational integers

$$x \equiv a \mod m$$

all of whose prime factors split principally in k.

Later I will show that the assumption of normality on k/Q can be deleted. But now I prove Theorem III via two lemmas.

<u>Lemma IV</u>: Let M/L and N/L be finite extensions of the number field L. Suppose M/L and MN/L are galois and $M \cap N = L$. Let $\mathfrak{P}$ be a prime of MN such that the degree of $\mathfrak{P}_N = \mathfrak{P} \cap N$ over L equals 1. Let $\mathfrak{p} = \mathfrak{P} \cap M$. Then the order of $\left[\frac{M/L}{\mathfrak{p}} \right]$ is precisely the order of $\left[\frac{MN/N}{\mathfrak{P}} \right]$.

<u>PROOF</u>: We first note that we have an isomorphism between the galois groups $G(MN/N)$ and $G(M/L)$ and that the isomorphism is given by the restriction map

$$\sigma \longmapsto \sigma|_M .$$

Let $\left[\frac{MN/L}{\mathfrak{P}} \right] = \sigma$. Since the degree of $\mathfrak{P}_N$ over L is 1, it follows that $\left[\frac{MN/N}{\mathfrak{P}} \right] = \left[\frac{MN/L}{\mathfrak{P}} \right] = \sigma$ and so $\sigma \in G(MN/N)$. Thus the order of σ equals the order of $\sigma|_M$. But from the definition of the Frobenius symbol

$$\sigma|_M = \left[\frac{M/L}{\mathfrak{p}} \right] .$$

<u>Lemma V</u>: Let k/Q be a finite galois extension and ℓ a rational prime. Let $\mathfrak{Q}$ be a prime divisor of ℓ in the class field $CF(k)$ of k with inertial field $I = I(\mathfrak{Q})$ over Q. Finally let $\mathfrak{P}$ be a prime of $CF(k)$ unramified over Q.

If the degree of the prime $\mathfrak{P}_I = \mathfrak{P} \cap I$ is 1 over Q, (or even over $k \cap I$), then the prime

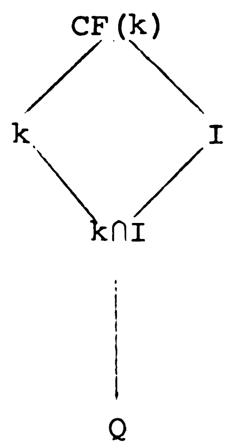
$$\mathfrak{p} = \mathfrak{P} \cap k$$

is principal in k. Moreover the rational prime

$$\mathfrak{p} = \mathfrak{P} \cap Q$$

splits principally in k.

<u>PROOF</u>: We have the following diagram



Recall that $CF(k)/Q$ is galois.

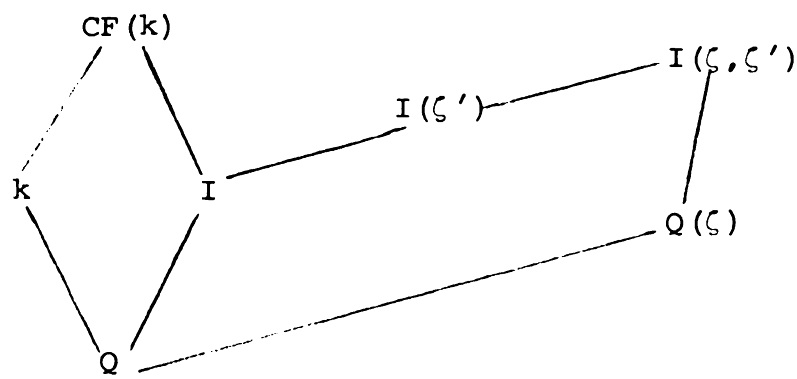
Note that $k \cap I$ is the inertial field of $\mathfrak{Q} \cap k$ over Q and, since $CF(k)/k$ is unramified,

$$[CF(k):I] = [k:(k \cap I)].$$

Since $k/(k \cap I)$ is normal it follows that $CF(k) = kI$.

By Lemma IV it follows that the order of $\left[\frac{CF(k)/I}{\mathfrak{P}}\right]$ equals the order of $\left[\frac{k/(k\cap I)}{\mathfrak{p}}\right]$ equals f, say. Now since the degree of $\mathfrak{P}_I$ over $k \cap I$ is 1, the degree of $\mathfrak{P}$ over Q is f. But the degree of $\mathfrak{p}$ over $k \cap I$ is also f so $\mathfrak{p}$ must gain degree 1 in the extension $CF(k)/k$. Thus $\mathfrak{p}$ is principal in k and since k is normal, p must split principally in k.

<u>PROOF OF THEOREM III</u>: We let ζ be a primitive ℓ^n-th root of unity, ζ' a primitive m'-th root of unity. We have



where I is as in Lemma V. Now $I(\zeta') \cap Q(\zeta) = Q$ since ℓ is totally ramified in $Q(\zeta)$ yet has an unramified prime factor in $I(\zeta')$. Hence

$$G(Q(\zeta)/Q) \cong G(I(\zeta,\zeta')/I(\zeta')).$$

Thus the substitution $\sigma_a(\zeta) = \zeta^a$ is an automorphism of $I(\zeta,\zeta')/I(\zeta')$. By the Cebotarev density theorem, the set of primes $\mathfrak{p}$ of $I(\zeta')$ with Artin Symbol

$$\left(\frac{I(\zeta,\zeta')/I(\zeta')}{\mathfrak{p}}\right) = \sigma_a$$

has positive density. Since almost all primes of $I(\zeta')$ are of degree 1 over Q, we need only consider such linear primes. However, if $\mathfrak{p}$ is such a prime then

$$p = \|\mathfrak{p}\| \equiv a \mod \ell^n$$

and

$$p \equiv 1 \mod m'.$$

Let $\mathfrak{p}_I = \mathfrak{p} \cap I$, then the degree of $\mathfrak{p}_I$ over Q is 1. So by Lemma V, p must split principally in k which proves Theorem III.

I will now show that the assumption of normality on k/Q can be deleted.

<u>Lemma VI</u>: Let k be an arbitrary number field and $\bar{k}$ be the galois closure of k. Suppose ℓ is a rational prime and $\mathfrak{L}$ is a prime factor of ℓ in $CF(\bar{k})$. Take $I = I(\mathfrak{L})$ to be the inertial field of $\mathfrak{L}$ over Q and $T = T(\mathfrak{L})$ the inertial group. Then

$$T \cap G(CF(\bar{k})/CF(k)) = T \cap G(CF(\bar{k})/k)$$

<u>PROOF</u>: Let I' and I'' be the inertial fields of $\mathfrak{L}$ over k and $CF(k)$ respectively. Since $CF(k)/k$ is unramified, it follows that $CF(k) \subset I'$, and so $I' = I''$. However,

$$G(CF(\bar{k})/I') = T \cap G(CF(\bar{k})/k)$$

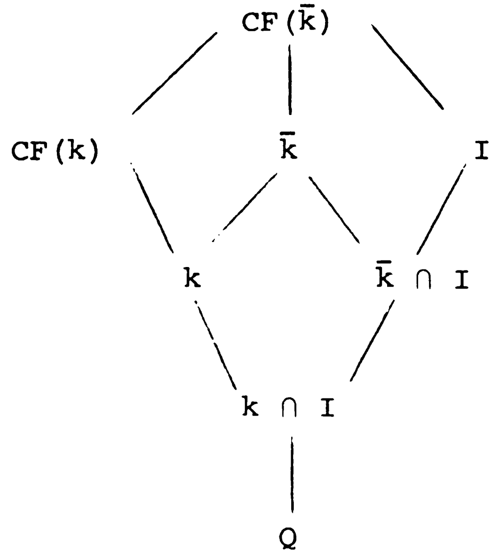
and

$$G(CF(\bar{k})/I'') = T \cap G(CF(\bar{k})/CF(k))$$

With the same notation we now have

<u>Lemma VII</u>: If $\mathfrak{P}$ is any prime of $CF(\bar{k})$ such that $\left[\frac{CF(\bar{k})/Q}{\mathfrak{P}}\right] \in T$ then $\mathfrak{p} = \mathfrak{P} \cap k$ is principal in k.

PROOF: We have the following diagram



Say $\left[\frac{CF(\bar{k})/Q}{\mathfrak{P}}\right] = \sigma$ and that the degree of $\mathfrak{p}$ over Q is f_1 then

$$\left[\frac{CF(\bar{k})/k}{\mathfrak{P}}\right] = \sigma^{f_1} \in G\left(CF(\bar{k})/k\right) \cap T.$$

Hence

$$\sigma^{f_1} \in G\left(CF(\bar{k})/CF(k)\right) \cap T$$

by Lemma VI. Thus $\mathfrak{p} = \mathfrak{P} \cap k$ gains degree 1 in $CF(k)/k$.

Corollary II: If $\left[\frac{CF(\bar{k})/Q}{\mathfrak{P}}\right] \in T$ then $p = \mathfrak{P} \cap Q$ splits principally in k.

PROOF: In the preceding proof we can replace k by any of its conjugate fields $\sigma(k)$ and $CF(k)$ by $CF(\sigma(k))$ and get that $\mathfrak{p}_\sigma = \mathfrak{P} \cap \sigma(k)$ is principal. Say $\mathfrak{p}_\sigma = \sigma(\alpha)$. Then $\sigma^{-1}(\mathfrak{p}_\sigma) = \alpha$ is principal in k. But $\sigma^{-1}(\mathfrak{P})$ lies above $\sigma^{-1}(\mathfrak{p}_\sigma)$ and since the galois group acts transitively on the primes of $CF(\bar{k})$ dividing p, it follows that all prime factors of p are principal in k.

And so finally we have

<u>Theorem V</u>: If k is an arbitrary number field and $(a,m) = 1$, then there are infinitely many rational integers

$$x \equiv a \mod m$$

all of whose prime factors split principally in k.

<u>PROOF</u>: Using the result of the preceding corollary we can now retrace the proof of Theorem III and the desired result follows.

It is now possible to slightly strengthen Corollary I of the previous chapter. Specifically I shall prove

<u>Theorem VI</u>: Let k be a number field with discriminant Δ. If m is a positive integer with $(m,\Delta) = \ell^n$ where ℓ is prime, then for each a with $(a,m) = 1$ there are infinitely many primes

$$p \equiv a \mod m$$

which split principally in k.

PROOF: Let $\mathfrak{L}$ be a prime factor of ℓ in $CF(\bar{k})$ and take $I = I(\mathfrak{L})$ to be the inertial field of $\mathfrak{L}$. If ζ is an m-th root of unity then

$$Q(\zeta) \cap I = Q.$$

Hence the substitution

$$\sigma_a : \zeta \longmapsto \zeta^a$$

is in $G(I(\zeta)/I)$. Now the set of linear primes P of I with

$$\left(\frac{I(\zeta)/I}{P}\right) = \sigma_a$$

has positive density. But

$$p = \|P\|_I \equiv a \mod m$$

and by Corollary II, p splits principally in k.

REFERENCES

[1] MacCluer, C. R., Non-principal Divisors among the Values of Polynomials; Acta. Arith.

[2] Weiss, Edwin, "Algebraic Number Theory". McGraw-Hill, New York, 1963, 172-182.

[3] Rotman, Joseph J., "Theory of Groups". Allyn and Bacon, Boston, 1965, 144-145.