ACTA ARITHMETICA
XXVIII (1975)

A purely algebraic proof of special cases of Tchebotarev's theorem

by

J. Wójcik (Warszawa)

I have given in [7] a purely algebraic proof of the following

Theorem. *Let G, J be subgroups of the multiplicative group of residues* mod m *and J be a proper subgroup of G. Then there exist infinitely many primes belonging* mod m *to $G-J$.*

The aim of the present paper is to prove on similar lines some special cases of Tchebotarev's density theorem in its qualitative form which comprise the above result. The proof is based on the upper estimate for the number of genera in a cyclic field of prime degree.

Notation. Terminology and notation are taken from [4]. In particular k denotes a fixed algebraic number field, all considered fields are extension of k unless stated to the contrary and all prime ideals are defined in k. For instance, an inclusion $\Omega \leqslant K$ means that $k \leqslant \Omega \leqslant K$. Q is the rational field, ζ_m is a primitive mth root of unity, $|\Omega| = (\Omega:Q)$. For a finite set S, $|S|$ is its cardinality. We say that the extension K/Ω is non-trivial if $K \neq \Omega$. A prime ideal of degree one means a prime ideal of degree one over Q.

Theorem 1. *Let K be a normal non-trivial extension of k. There exist infinitely many prime ideals* $\mathfrak{p}$ *of degree one such that* $\left(\frac{K}{\mathfrak{p}}\right) \neq 1$.

Remark 1. For K being abelian a similar statement proved again in a purely algebraic way occurs in [1] as Corollary 8.8. However we assert in contrast to [1] that $\mathfrak{p}$ is of degree one.

Lemma 1. *Let K be a cyclic field of prime degree and* $\mathfrak{d}$ *be its relative discriminant. For every positive integer M there exists a prime ideal* $\mathfrak{p}$ *of k prime to $\mathfrak{d}M$ such that* $\left(\frac{K}{\mathfrak{p}}\right) \neq 1$.

Proof. Let $l = (K:k)$, where l is a prime. It is well known that $\mathfrak{d} = f^{l-1}$, where f is an ideal of k. Let A be the group of all classes of ideals

mod f prime to f, H_f be the group of the classes of ideals mod f which contain a relative norm of an ideal from K, finally H_1 let be the group of the classes of ideals mod f which contain a norm of a principal ideal of K.

The following inequality holds

$$(H_f:H_1) \leqslant a \leqslant \frac{1}{l}(A:H_1)$$

where a is the number of ambiguous classes ([3], I)

Hence

$$|H_f| \leqslant \frac{1}{l}|A|. \tag{1}$$

Suppose that there exists a positive integer M such that for every prime ideal $\mathfrak{p}$ of k prime to $\mathfrak{d}M$ we have

$$\left(\frac{K}{\mathfrak{p}}\right) = 1. \tag{2}$$

In each class of ideals of k mod f there exists an integral ideal $\mathfrak{a}$ prime to $\mathfrak{d}M$ ([3], Ia, p. 63). Let

$$\mathfrak{a} = \prod \mathfrak{p}, \tag{3}$$

where $\mathfrak{p}$ are prime ideals.

By (2) $\mathfrak{p}$ splits completely in K into prime ideals of degree one over k (cf. [4], § 1, I'), thus $\mathfrak{p} = N_{K/k}\mathfrak{P}$, where $\mathfrak{P}$ is an ideal of K. Hence by (3) $\mathfrak{a} = N_{K/k}(\prod \mathfrak{P})$ and each class of ideals in k mod f contain a relative norm of an ideal of K, i.e. $H_f = A$, contrary to (1).

Proof of Theorem 1. Let $\mathfrak{G}$ be the Galois group of K and σ an element of $\mathfrak{G}$ of order l, where l is a prime. There exists a prime q satisfying the condition

$$q \equiv 1 \bmod l, \qquad q \nmid \operatorname{disc} K/Q.$$

Hence

$$[K, Q(\zeta_q)] = Q. \tag{4}$$

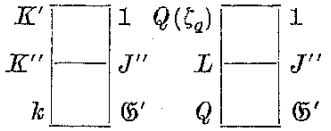
Put $K' = k(\zeta_q)$. The Galois groups of the extensions K'/k, $Q(\zeta_q)/Q$ are isomorphic with the group of all substitutions $\mathfrak{G}'$: $\sigma' = (\zeta_q \to \zeta_q^r)$, $(r, q) = 1$ where σ' acts trivialy on the fields k and Q respectively.

Let K'' be a field satisfying the conditions: $K'' \leqslant K$, $K'' \leqslant K'$.

Let J'' be a subgroup of $\mathfrak{G}'$ corresponding to K''. Finally, let L be the subfield of $Q(\zeta_q)$ corresponding to the subgroup J''.

Clearly $L \leqslant K'' \leqslant K$. Hence by (4)

$$L = Q, \qquad J'' = \mathfrak{G}', \qquad K'' = k.$$



It follows that the fields K, K' are *relatively prime over* k. The Galois group of KK' is the direct product $\mathfrak{G}\mathfrak{G}'$, where $\mathfrak{G}'$ acts trivially on K, and $\mathfrak{G}$ acts trivially on K'. Put $\sigma' = (\zeta_q \to \zeta_q^{g^{(q-1)/l}})$, where g is a primitive root mod q. σ' is of order l.

Let Ω be a subfield of KK' corresponding to the cyclic subgroup $\{\sigma\sigma'\}$ of the group $\mathfrak{G}\mathfrak{G}'$. The extension KK'/Ω is cyclic of degree l with the Galois group $\{\sigma\sigma'\}$.

In virtue of Lemma 1 there exists a prime ideal $\mathfrak{q}$ of Ω prime to $q \cdot \operatorname{disc} KK'/\Omega$ and such that:

$$\left(\frac{KK'/\Omega}{\mathfrak{q}}\right) \neq 1. \tag{5}$$

It follows that

$$N_{\Omega/Q}\mathfrak{q} \not\equiv 1 \bmod q. \tag{6}$$

Indeed,

$$\left(\frac{KK'/\Omega}{\mathfrak{q}}\right) = \sigma^t\sigma'^t, \qquad 0 \leqslant t < l, \qquad \sigma'^t\zeta_q = \zeta_q^r, \qquad (r, q) = 1 \tag{7}$$

for some t, r.

If $N_{\Omega/Q}\mathfrak{q} \equiv 1 \bmod q$ we have by (7) (cf. [4], § 2, (1))

$$\zeta_q = \zeta_q^{N_{\Omega/Q}\mathfrak{q}} \equiv \left(\frac{KK'/\Omega}{\mathfrak{q}}\right)\zeta_q = \sigma^t\sigma'^t\zeta_q = \sigma^t\zeta_q^r = \zeta_q^r \bmod \mathfrak{q}.$$

Thus, since $\mathfrak{q} \nmid q$: $\sigma'^t\zeta_q = \zeta_q^r = \zeta_q$. This means that σ'^t does not change elements of K', K' being generated by ζ_q.

Hence $\sigma'^t = 1$, $t = 0$ and by (7) $\left(\frac{KK'/\Omega}{\mathfrak{q}}\right) = 1$ contrary to (5).

Let $\mathfrak{p}_0, \mathfrak{p}_1, \ldots, \mathfrak{p}_{r-1}$ $(r \geqslant 0)$ be prime ideals of degree one satisfying the condition $\left(\frac{K}{\mathfrak{p}_i}\right) \neq 1$ $(0 \leqslant i \leqslant r-1)$. We shall construct a prime ideal $\mathfrak{p}_r$ of degree one different from the ideals $\mathfrak{p}_i$ $(0 \leqslant i \leqslant r-1)$ and such that $\left(\frac{K}{\mathfrak{p}_r}\right) \neq 1$.

In virtue of Lemma 2 in [7] there exists an integral ideal $\mathfrak{b}$ of Ω such that

$$\mathfrak{q} \cdot \mathfrak{b} = (\alpha), \qquad N_{\Omega/Q}\alpha > 0, \qquad \Omega = Q(\alpha), \qquad (\mathfrak{b}, N_{\Omega/Q}\mathfrak{q}) = 1. \tag{8}$$

Put $p_i = N_{k/Q}\mathfrak{p}_i \quad (0 \leqslant i \leqslant r-1), \quad M = \operatorname{disc}\alpha \cdot N_{k/Q}(\operatorname{disc}KK'/k) \cdot \prod_{i=0}^{r-1} p_i$, $M = M_1 M_2$, where $(M_1, qN_{\Omega/Q}\mathfrak{b}) = 1$ and M_2 contains only prime factors dividing $qN_{\Omega/Q}\mathfrak{b}$.

$$f(x, y) = \prod_{i=1}^{s} (x - a_i y),$$

where $a_1 = a, a_2, \ldots, a_s$ are conjugates of a with respect to Q, $s = |\Omega|$.

By the Chinese Remainder Theorem there exist rational integers y, x satisfying the conditions

$$(9) \qquad y \equiv \begin{cases} -1 \bmod q(N_{\Omega/Q}\mathfrak{b})^2, \\ 0 \bmod M_1, \end{cases} \qquad x \equiv \begin{cases} 0 \bmod q(N_{\Omega/Q}\mathfrak{b})^2, \\ 1 \bmod y, \end{cases}$$

$$C = f(x, y)/N_{\Omega/Q}\mathfrak{b} > 1.$$

Hence we have

$$(10) \qquad f(x, y) \equiv \begin{cases} 1 \bmod y, \\ N_{\Omega/Q}\alpha \bmod q(N_{\Omega/Q}\mathfrak{b})^2. \end{cases}$$

By (8)

$$(11) \qquad N_{\Omega/Q}\alpha = N_{\Omega/Q}\mathfrak{q} \cdot N_{\Omega/Q}\mathfrak{b}.$$

Hence by (10) C is a positive integer.

By (10) and (11)

$$(12) \qquad C \equiv N_{\Omega/Q}\mathfrak{q} \bmod q \cdot N_{\Omega/Q}\mathfrak{b}.$$

Hence by (6)

$$(13) \qquad C \not\equiv 1 \bmod q.$$

By (8), (9), (10) and (12)

$$(14) \qquad (C, yM) = (C, yM_1M_2) = 1.$$

According to (13) the positive integer $C > 1$ has a prime factor p_r such that

$$(15) \qquad p_r \not\equiv 1 \bmod q.$$

Hence $p_r | f(x, y)$ and by (14) $p_r \nmid y \operatorname{disc}\alpha$. In virtue of Dedekind's theorem there exists a prime ideal $\mathfrak{P}_r$ of degree one in Ω dividing p_r. Let $\mathfrak{p}_r$ be a prime ideal of k such that $\mathfrak{P}_r | \mathfrak{p}_r$, $\mathfrak{p}_r | p_r$. It follows (cf. [4], § 1, V′)

$$\sigma^t \sigma'^t = \left(\frac{KK'/\Omega}{\mathfrak{P}_r}\right) \leqslant \left(\frac{KK'/k}{\mathfrak{p}_r}\right), \qquad 0 \leqslant t < l.$$

This means that

$$\left(\frac{KK'}{\mathfrak{p}_r}\right) = \langle \sigma^t \sigma'^t \rangle, \qquad 0 \leqslant t < l.$$

Hence by the well known formula ([4], § 1, IV) we have on decomposing into direct factors

$$(16) \qquad \left(\frac{K}{\mathfrak{p}_r}\right) = \langle \sigma^t \rangle, \qquad \left(\frac{K'}{\mathfrak{p}_r}\right) = \langle \sigma'^t \rangle = \sigma'^t, \qquad 0 \leqslant t < l.$$

Clearly $\mathfrak{p}_r$ is of degree one, i.e. $p_r = N_{k/Q}\mathfrak{p}_r$ because $\mathfrak{P}_r$ is of degree one. It must be $\left(\frac{K}{\mathfrak{p}_r}\right) \neq 1$. Otherwise we had by (16)

$$t = 0, \qquad \left(\frac{K'}{\mathfrak{p}_r}\right) = 1, \qquad \zeta_q^{p_r} = \zeta_q^{N_{k/Q}\mathfrak{p}_r} \equiv \left(\frac{K'}{\mathfrak{p}_r}\right) \zeta_q = \zeta_q \bmod \mathfrak{p}_r.$$

Since $(\mathfrak{q}, q) = 1$ we have by (12): $(p_r, q) = 1$, thus $\zeta_q^{p_r} = \zeta_q$, $p_r \equiv 1 \bmod q$ contrary to (15).

By (14) $p_r \nmid \prod_{i=0}^{r-1} p_i$. Hence $\mathfrak{p}_r$ is different from $\mathfrak{p}_0, \ldots, \mathfrak{p}_{r-1}$ and the proof is complete.

As an application we shall prove now a special case of Tchebotarev density theorem in its qualitative form. We shall show the following

THEOREM 2. *Let K be a normal field and σ an automorphism of K satisfying $\sigma^2 = 1$. There exist infinitely many prime ideals $\mathfrak{p}$ of degree one such that $(K/\mathfrak{p}) = \langle \sigma \rangle$.*

Proof. 1. $\sigma = 1$. The theorem follows at once from the existence of infinitely many prime ideals of degree one in K which can easily be proved in a purely algebraic way (see [2]).

2. $\sigma \neq 1$. Let Ω be subfield of K corresponding to $\{\sigma\}$. The extension K/Ω is quadratic. By Theorem 1 there exist infinitely many prime ideals $\mathfrak{q}$ of degree one in Ω such that

$$(17) \qquad \left(\frac{K/\Omega}{\mathfrak{q}}\right) \neq 1.$$

Let $\mathfrak{p}$ be a prime ideal of k such that $\mathfrak{q} | \mathfrak{p}$. Clearly $\mathfrak{p}$ is of degree one.

By (17) we have (cf. [4], § 1, V′)

$$(18) \qquad \sigma = \left(\frac{K/\Omega}{\mathfrak{q}}\right) \leqslant \left(\frac{K/k}{\mathfrak{p}}\right)$$

since the Galois group of the extension K/Ω consists of two elements: 1, σ. By (18) $(K/\mathfrak{p}) = \langle \sigma \rangle$, Q.E.D.

Remark 2. Theorem 2 is a generalization of Theorem 2 of [7].

Let K be a finite extension of k, $K^{(1)} = K, K^{(2)}, \ldots, K^{(n)}$, $n = (K:k)$ be the conjugates of K and $\bar{K}$ its normal closure. We shall say that K is quasi-normal if it satisfies the condition $K^{(i)}K^{(j)} = \bar{K}$ for all pairs i, j, where $i \neq j$. Clearly a normal extension is also quasi-normal.

An example of a non-normal but a quasi-normal extension is furnished by $Q(\sqrt[3]{2})$. For an arbitrary extension Ω/k we denote by $P(\Omega)$ the set of prime ideals of k with at least one prime factor of degree one in Ω. We say that the extension K/k is Bauerian if for any Ω the condition $P(\Omega) \leqslant P(K)$ implies that Ω contains at least one of the conjugates of K ($P(\Omega) \leqslant P(K)$ means that the set $P(\Omega) - P(K)$ is finite); see [5], p. 221 for $k = Q$.

We have the following extension of the original result of Bauer ([4], § 25, III).

THEOREM 3. *Every quasi-normal extension is Bauerian.*

LEMMA 2. *Let $\mathfrak{G}$ be a transitive permutation group on n digits, whose all elements except the identity fix at most one digit. Let G_j $(1 \leqslant j \leqslant n)$ be the stability subgroups of $\mathfrak{G}$. Finally let $\mathfrak{U}$ be an arbitrary subgroup of $\mathfrak{G}$. If $[\mathfrak{U}, G_i] \neq 1$ then the set $\mathfrak{M}$ of those elements of $\mathfrak{U}$ which fix no digit, forms together with the identity a group of order $(\mathfrak{U}:[\mathfrak{U}, G_i])$.*

Proof. Let $\mathfrak{N}$ be the set of those elements of $\mathfrak{G}$ which fix no letter. Put $H_j = [\mathfrak{U}, G_j]$, $n_j = |H_j|$ $(1 \leqslant j \leqslant n)$, $\overline{\mathfrak{N}} = \mathfrak{N} + \{1\}$, $\overline{\mathfrak{M}} = \mathfrak{M} + \{1\}$.

We have $\mathfrak{M} = [\mathfrak{N}, \mathfrak{U}]$, In virtue of Frobenius theorem (see [6], Theorem 180, pp. 202–203) the set $\overline{\mathfrak{N}}$ is a group. Hence $\overline{\mathfrak{M}}$ is a group. It remains to prove that $|\overline{\mathfrak{M}}| = m = (\mathfrak{U}:H_i)$. Put

$$\mathfrak{U} = \sum_{j=1}^{m} \tau_j H_i, \quad \tau_1 = 1, \quad \tau_j = \begin{pmatrix} 1 \dots i \dots n \\ \dots \nu_j \dots \end{pmatrix} \quad (1 \leqslant j \leqslant m), \quad \nu_1 = i. \tag{19}$$

Since the permutations τ_j are distinct mod G_i the digits ν_j $(1 \leqslant j \leqslant m)$ are distinct.

Let F be the family of the sets H_j for which $n_j > 1$. Two sets H_r, H_s of F are assigned to the same class if $H_r = \tau H_s \tau^{-1}$ for a certain $\tau \in \mathfrak{U}$.

Clearly the latter relation is reflexive, symmetric and transitive. By the assumptions of the lemma $[H_r, H_s] = 1$ for $r \neq s$. Hence

$$H_r \neq H_s \quad \text{for} \quad H_r, H_s \in F, \quad r \neq s. \tag{20}$$

By the assumption $H_i \in F$. By (19) $G_{\nu_j} = \tau_j G_i \tau_j^{-1}$ and hence $H_{\nu_j} = \tau_j H_i \tau_j^{-1}$ $(1 \leqslant j \leqslant m)$.

This means that the class represented by H_i consists of m sets: $H_{\nu_1} = H_i, H_{\nu_2}, \dots, H_{\nu_m}$.

Let S be the set theoretic union of these sets. We have by (19)

$$|S| = m|H_i| - (m-1) = |\mathfrak{U}| - m + 1 \geqslant \tfrac{1}{2}|\mathfrak{U}| + 1 \tag{21}$$

since $H_i \in F$ and $m \leqslant \frac{1}{2}|\mathfrak{U}|$.

Suppose that there exists another class with the set theoretic union S', say. Then on one hand

$$S + S' \subset \mathfrak{U}, \tag{22}$$

on the other hand by (21)

$$|S'| \geqslant \tfrac{1}{2}|\mathfrak{U}| + 1. \tag{23}$$

Since $[H_r, H_s] = 1$ for $r \neq s$ we have $[S, S'] = 1$. Hence by (21) and (23) we infer that

$$|S + S|' = |S| + |S'| - 1 \geqslant |\mathfrak{U}| + 1 > |\mathfrak{U}|$$

contrary to (22).

The contradiction shows that the family F reduces to one class

$$F = \{H_{\nu_1} = H_i, H_{\nu_2}, \dots, H_{\nu_m}\}. \tag{24}$$

Hence

$$\mathfrak{M} = \mathfrak{U} - S. \tag{25}$$

Indeed, if $\sigma \in \mathfrak{U} - S$ and $\sigma \notin \mathfrak{M}$ then $\sigma \in H_j$ for some j, $\sigma \neq 1$. $H_j \in F$, $\sigma \in S$ contrary to assumption. This implies the inclusion $\mathfrak{U} - S \subset \mathfrak{M}$ which together with the obvious inclusion $\mathfrak{M} \subset \mathfrak{U} - S$ gives (25). By (25), (21) and the definition of $\mathfrak{M}$

$$|\overline{\mathfrak{M}}| = |\mathfrak{U}| - |S| + 1 = m,$$

and the proof is complete.

Proof of Theorem 3. Let K be a quasi-normal extension of k and suppose that Ω does not contain any of the fields $K^{(j)}$ $(1 \leqslant j \leqslant n)$.

Let $\mathfrak{G}$ be the Galois group of $\overline{K}/k$ represented as a transitive permutation group of n fields $K^{(j)}$ $(1 \leqslant j \leqslant n)$. Then $K^{(j)}$ corresponds to jth stability subgroups of $\mathfrak{G}$ denoted by G_j.

Let $\mathfrak{U}$ be the subgroup of $\mathfrak{G}$ corresponding to the field $[\overline{K}, \Omega]$. $\mathfrak{U}$ is Galois group of the extension $\Omega\overline{K}/\Omega$, it being assumed that $\mathfrak{U}$ acts trivially on Ω (see [4], § 1, p. 8). We have

$$\mathfrak{U} \neq 1. \tag{26}$$

Indeed, if $\mathfrak{U} = 1$ then $\Omega\overline{K} = \Omega$, $K \leqslant \overline{K} \leqslant \Omega$ contrary to the assumption. Let $\mathfrak{M}$ be the set of those permutations of $\mathfrak{U}$ which fix no letter.

Put $\overline{\mathfrak{M}} = \mathfrak{M} + \{1\}$.

The set $\mathfrak{M}$ is a group of order > 1. For $\overline{\mathfrak{M}} = \mathfrak{U}$ this follows from (26). If $\overline{\mathfrak{M}} \neq \mathfrak{U}$, $\mathfrak{U}$ contains a permutation different from the identity that fixes a digit, say i. Further the group $\mathfrak{G}$ is transitive and the condition $K^{(r)}K^{(s)} = \overline{K}$ $(r \neq s)$ implies $[G_r, G_s] = 1$. This means that the permutations of $\mathfrak{G}$ except the identity fix at most one digit. By Lemma 2 $\overline{\mathfrak{M}}$ is a group of order $m = (\mathfrak{U}:[\mathfrak{U}, G_i])$. The condition $m = 1$ implies $K^{(i)} \leqslant [\overline{K}, \Omega] \leqslant \Omega$ contrary to the assumption.

Let L be the subextension of $\Omega\overline{K}/\Omega$ corresponding to $\overline{\mathfrak{M}}$. The extension $\Omega\overline{K}/L$ is normal and non-trivial with the Galois group $\overline{\mathfrak{M}}$.

In virtue of Theorem 1 there exist infinitely many prime ideals $\mathfrak{P}$ of degree one in L such that

$$\left(\frac{\Omega\overline{K}/L}{\mathfrak{P}}\right) \neq 1. \tag{27}$$

Let $\mathfrak{q}, \mathfrak{p}$ be prime ideals of the fields Ω, k respectively such that $\mathfrak{P}|\mathfrak{q}$, $\mathfrak{q}|\mathfrak{p}$. The ideals $\mathfrak{p}, \mathfrak{q}$ are of degree one, thus

$$\mathfrak{p} \in P(\Omega).$$

We have (cf. [4], § 1, V, V′)

$$\langle\sigma\rangle_{\overline{\mathfrak{M}}} = \left(\frac{\Omega\overline{K}/L}{\mathfrak{P}}\right) \leqslant \left(\frac{\Omega\overline{K}/\Omega}{\mathfrak{q}}\right) \leqslant \left(\frac{\overline{K}/k}{\mathfrak{p}}\right)$$

on restriction to $\overline{K}$, where $\langle\sigma\rangle_{\overline{\mathfrak{M}}}$ is the set of elements $\tau\sigma\tau^{-1}$, $\tau \in \overline{\mathfrak{M}}$. Hence $\left(\frac{\overline{K}}{\mathfrak{p}}\right) = \langle\sigma\rangle$.

Clearly $\sigma = \sigma(\mathfrak{P}) \in \overline{\mathfrak{M}}$. Hence by (27) $\sigma \in \mathfrak{M}$. This means that σ and also $\tau\sigma\tau^{-1}$ $(\tau \in \mathfrak{G})$ do not fix any digit. In particular $\tau\sigma\tau^{-1} \notin G_1$ $(\tau \in \mathfrak{G})$. Since the group G_1 corresponds to the field $K^{(1)} = K$ we have $\mathfrak{p} \notin P(K)$ (cf. [4], § 23, II).

Thus we have proved that if the field Ω contains no conjugate of K then there exist infinitely many prime ideals $\mathfrak{p}$ such that $\mathfrak{p} \in P(\Omega) - P(K)$. This means that the field K is Bauerian. Q.E.D.

Remark 3. It is easy to see that quasi-normal fields have property P (see [5]).

Using class field theory and Artin's reciprocity law we shall give one more application of Theorem 1.

Let $\mathfrak{m}$ be a modulus as defined in [3], Ia, § 3, p.60 ($\overline{\mathfrak{m}}$ can contain the factor $\mathfrak{p}_\infty$ to the first power). By a group G of ideals mod $\overline{\mathfrak{m}}$ we shall understand a set of ideals of k satisfying the following conditions:

1) G is a group with respect to multiplication of ideals.

2) Every ideal of G is prime to $\overline{\mathfrak{m}}$.

3) G contains all principal ideals (a), where $a \equiv 1 \bmod \overline{\mathfrak{m}}$.

A subset J of a group G of ideals mod $\overline{\mathfrak{m}}$ which itself satisfies the conditions 1), 2), 3) is called a subgroup of G.

We have

THEOREM 4. *Let G be a group of ideals* mod $\overline{\mathfrak{m}}$ *and J a proper subgroup of G. There exist infinitely many prime ideals $\mathfrak{p}$ of degree one in k such that $\mathfrak{p} \in G - J$.*

Proof. Let fields Ω, K correspond to the groups G, J, respectively. We have $\Omega \leqslant K$, $\Omega \neq K$. By Theorem 1 there exist infinitely many prime ideals $\mathfrak{q}$ of degree one in Ω such that

$$\left(\frac{K/\Omega}{\mathfrak{q}}\right) \neq 1. \tag{28}$$

Let $\mathfrak{p}$ be a prime ideal of k such that $\mathfrak{q}|\mathfrak{p}$. The ideal $\mathfrak{p}$ is of degree one and $\mathfrak{p} = N_{\Omega/k}\mathfrak{q}$. By the definition of a class-field $\mathfrak{p} \in G$.

On the other hand since K, Ω are abelian we have by (28) (cf. [4], § 1, V′)

$$\left(\frac{K/\Omega}{\mathfrak{q}}\right) = \left(\frac{K/k}{\mathfrak{p}}\right) \neq 1.$$

By Artins reciprocity law $\mathfrak{p} \notin J$, Q.E.D.

References

[1] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, London and New York 1967.

[2] T. Nagell, *Sur les diviseurs premiers des polynomes*, Acta Arith. 15 (1969), pp. 235–244.

[3] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil I: *Klassenkörpertheorie*, Teil Ia: *Beweise zu Teil I*, Würzburg–Wien 1965.

[4] —, —, Teil II: *Reziprozitätsgesetz*, Wien–Würzburg 1965.

[5] A. Schinzel, *On a theorem of Bauer and some of its applications II*, Acta Arith. 12 (1973), pp. 221–231.

[6] A. Speiser, *Die Theorie der Gruppen von endlicher Ordnung*, Basel und Stuttgart 1956.

[7] J. Wójcik, *A refinement of a theorem of Schur on primes in arithmetic progressions III*, Acta Arith. 15 (1969), pp. 193–197.

Received on 10. 12. 1973 (519)