soit de mesure nulle, soit de mesure pleine. Ces conditions sont-elles suffisantes? (Cela m'étonnerait.)

4° Si A et B sont deux ensembles normaux, en est-il de même de $A \cup B$? Sinon, trouver un ensemble normal C non trivial (différent de $\boldsymbol{R}-\{0\}$ ou $\boldsymbol{R}-\boldsymbol{Q}$) qui contienne $A \cup B$.

5° Est-il vrai qu'un nombre complètement normal soit nécessairement transcendant? Ce problème, vraisemblablement très difficile est à l'origine de cette étude.

Travaux cités

[1] M. Mendès France, *Deux remarques concernant l'équirépartition des suites*, Acta Arith. 14 (1968), p. 163-167.

[2] Ch. Pisot, *La répartition modulo 1 et les nombres algébriques*, Ann. Sc. Norm. Sup. Pisa, Série 2, 7 (1938), p. 205-248 (Thèse Sc. Paris, 1938).

Reçu par la Rédaction le 29. 3. 1968

ACTA ARITHMETICA
XV (1969)

A refinement of a theorem of Schur on primes in arithmetic progressions III

by

J. Wójcik (Warszawa)

I have given in [4] a purely algebraic proof of the following specia case of Dirichlet's theorem on arithmetic progression: Let $l^2 \equiv 1 \bmod m$, $m = p^\nu n$, where p is a prime, $\nu > 0$, $p \nmid n$, $l \equiv 1$ or $p \bmod n$. Then there exist infinitely many primes $\equiv l \bmod m$.

The aim of this paper is to extend this result. The proof, again purely algebraic, is based on the well known upper estimate for the number of genera in a cyclic field of prime degree.

Notation: Q is the rational field, m — any positive integer, E_m — the multiplicative group of rationals congruent to 1 mod m, ζ_m — mth primitive root of unity, $P_m = Q(\zeta_m)$.

For any two fields k and K, $k \subset K$, N_{Kk} is the norm from K to k. $(K; k)$ is the degree of K over k, $|k| = (k : Q)$.

For any two abelian groups J and G, $J \subset G$, $|G|$ is the order of G, G/J the quotient group, $(G : J) = |G/J|$.

The term *group of rationals* mod m *prime to* m denotes any set $G \subset Q$ such that 1) $E_m \subset G$, 2) G is multiplicative group, 3) any element of G is prime to m. (Clearly G/E_m is a group of residue classes mod m prime to m.) We say that a field $k \subset P_m$ is invariant with respect to group G if it is invariant with respect to automorphism $\zeta_m \to \zeta_m^n$ of P_m for any integer $n \in G$.

Theorem 1. *Let G, J be groups of rationals* mod m *prime to m and let J be a proper subgroup of G. There exist infinitely many primes in $G \setminus J$.*

Lemma 1. *Let G, J be groups of rationals* mod m *prime to m and let J be a subgroup of G of prime index. Let k be a maximal subfield of P_m invariant with respect to G. There exists a prime ideal $\mathfrak{p}$ in k prime to m such that $N\mathfrak{p}$ does not belong to J.*

Proof. Let K be a maximal subfield of P_m invariant with respect to J. We have:

$$(K : k) = (G/E_m : J/E_m) = (G : J) = l, \quad \text{where } l \text{ is a prime.}$$

Hence K/k is a cyclic extension of prime degree. Let $\mathfrak{d}$ be its relative discriminant. It is well known that $\mathfrak{d} = \mathfrak{f}^{l-1}$, where $\mathfrak{f}$ is an ideal of k.

Let A be the group of all ideal classes of $k \bmod \mathfrak{f}$ prime to $\mathfrak{f}$, $H_\mathfrak{f}$ be the group of these ideal classes of $k \bmod \mathfrak{f}$ which contain the relative norm of an ideal of K, finally, let H_1 be the group of these ideal classes of $k \bmod \mathfrak{f}$ which contain the relative norm of a principal ideal of K.

The following inequality is well known (see [1], pp. 22-24):

$$(H_\mathfrak{f} : H_1) \leqslant a \leqslant \frac{1}{l}(A : H_1),$$

where a is the number of ambiguous classes.

Hence:

$$|H_\mathfrak{f}| \leqslant \frac{1}{l}|A|. \tag{1}$$

Suppose that for every prime ideal $\mathfrak{p}$ of k prime to m we have:

$$N\mathfrak{p} \in J. \tag{2}$$

In each ideal class of $k \bmod \mathfrak{f}$ there exists an integral ideal $\mathfrak{a}$ prime to m ([1], p. 63). Let

$$\mathfrak{a} = \prod \mathfrak{p}, \quad \text{where } \mathfrak{p} \text{ prime ideals.} \tag{3}$$

Let α be an arbitrary integer of K. Since $1, \zeta_m, \ldots, \zeta_m^{\varphi(m)-1}$ form an integral basis of P_m we have:

$$\alpha = h(\zeta_m), \tag{4}$$

where h is a polynomial with rational integral coefficients.

Let $N\mathfrak{p} = p^f$, where p is a prime. By (4), (2) and the definition of K we get:

$$\alpha^{N\mathfrak{p}} \equiv h(\zeta_m^{p^f}) \equiv h(\zeta_m) \equiv \alpha \bmod p.$$

Since the above congruence holds for every integer α of K, it follows that each prime ideal factor of $\mathfrak{p}$ in K is of degree one with respect to k, thus $\mathfrak{p} = N_{Kk}\mathfrak{P}$, where $\mathfrak{P}$ is an ideal of K.

Hence by (3) $\mathfrak{a} = N_{Kk}(\prod \mathfrak{P})$ and each ideal class of $k \bmod \mathfrak{f}$ contains a relative norm of an ideal of K, i.e. $H_\mathfrak{f} = A$. The obtained contradiction with (1) proves the lemma.

LEMMA 2. *Let k be an algebraic number field. For any two integral ideals $\mathfrak{a}$ and $\mathfrak{c}$ of k there exists an integral ideal $\mathfrak{b}$ of k such that:*

$$\mathfrak{ab} = (\alpha), \quad N\alpha > 0, \quad k = Q(\alpha), \quad (\mathfrak{b}, \mathfrak{c}) = 1.$$

Proof. Clearly there exists an integral ideal $\mathfrak{b}_1$ of k such that:

$$\mathfrak{ab}_1 = (\gamma), \quad (\mathfrak{b}_1, \mathfrak{c}) = 1. \tag{5}$$

Let β be a primitive element of k. For sufficiently large rational integer n we have $N(\beta+n) = N_{kQ}(\beta+n) = n^{|k|} + \ldots > 0$.

Hence we can assume that $N\beta > 0$. We have

$$\beta - \beta_i \neq 0 \quad (i = 2, 3, \ldots, |k|).$$

(β_i's are the conjugates of β.)

Choose a rational integer x so large that

$$x \neq (\gamma_i - \gamma)/N(\mathfrak{ac})(\beta - \beta_i) \quad (i = 2, 3, \ldots, |k|), \tag{6}$$

$N\alpha = (N\mathfrak{ac})^{|k|} N\beta \cdot x^{|k|} + \ldots > 0$, where $\alpha = \gamma + xN\mathfrak{ac}\cdot\beta$. By (5) $\mathfrak{a}|\alpha$, hence $(\alpha) = \mathfrak{ab}$. The equality $\alpha = \alpha_i$ with $i > 1$ would imply

$$x = (\gamma_i - \gamma)/(N\mathfrak{ac})(\beta - \beta_i)$$

contrary to (6). Thus $k = Q(\alpha)$. If $\mathfrak{p}|\mathfrak{c}$, where $\mathfrak{p}$ is a prime ideal and $\mathfrak{p}^\nu \| \mathfrak{a}$, $\nu \geqslant 0$, then $\mathfrak{p}^\nu \| \gamma$ by (5) and $\mathfrak{p}^{\nu+1} | N\mathfrak{ac}$, thus $\mathfrak{p}^\nu \| \mathfrak{a}$, $\mathfrak{p} \nmid \mathfrak{b}$. It follows that $(\mathfrak{b}, \mathfrak{c}) = 1$ and the proof is complete.

Proof of Theorem 1. In view of the structure of the lattice of subgroups of G we can assume without loss of generality that J is a subgroup of G of prime index. Let $p_0, p_1, \ldots, p_{r-1}$ be a sequence of primes from $G \setminus J$ ($r \geqslant 0$). We shall construct a prime $p_r \in G \setminus J$ not belonging to the sequence. By Lemma 1 there exists a prime ideal $\mathfrak{p}$ such that:

$$N\mathfrak{p} \notin J, \quad (\mathfrak{p}, m) = 1. \tag{7}$$

By Lemma 2 there exists an integral ideal $\mathfrak{b}$ such that:

$$\mathfrak{p}\cdot\mathfrak{b} = (\alpha), \quad N\alpha > 0, \quad k = Q(\alpha), \quad (\mathfrak{b}, N\mathfrak{p}) = 1. \tag{8}$$

Let $u = \prod_{p_i \nmid N\mathfrak{b}} p_i$, $d = \operatorname{disc}\alpha$, $d = d_1 \cdot d_2$, where $(d_1, mN\mathfrak{b}) = 1$ and all prime factors of d_2 divide $mN\mathfrak{b}$. In virtue of the Chinese remainder theorem there exist rational integers a, b satisfying the conditions:

$$a \equiv \begin{cases} -1 \bmod m(N\mathfrak{b})^2, \\ 0 \bmod d_1 u; \end{cases} \qquad b \equiv \begin{cases} 0 \bmod m(N\mathfrak{b})^2, \\ 1 \bmod a, \ a > 0. \end{cases} \tag{9}$$

Let

$$f(x) = \prod_{i=1}^{s}(x - \alpha_i \alpha), \quad \varphi(x) = f\big(am(N\mathfrak{b})^2 x + b\big)/N\mathfrak{b}, \quad s = |k|.$$

By (8)

$$N\alpha = N\mathfrak{p}N\mathfrak{b}. \tag{10}$$

By (9)

$$f\big(am(N\mathfrak{b})^2 x + b\big) \equiv \begin{cases} 1 \bmod a, \\ N\alpha \bmod m(N\mathfrak{b})^2. \end{cases} \tag{11}$$

Hence by (10):

$$f(am(N\mathfrak{b})^2x+b) \equiv 0 \bmod N\mathfrak{b},$$

thus $\varphi(x)$ is a polynomial with rational integral coefficients. By (10) and (11):

$$\varphi(x) \equiv N\alpha/N\mathfrak{b} \equiv N\mathfrak{a} \bmod mN\mathfrak{b} \tag{12}$$

and by (7), (8), (9) and (11)

$$(\varphi(x), amN\mathfrak{b}) = (\varphi(x), admu) = 1 \quad \text{for every integer } x. \tag{13}$$

We have $D = \operatorname{disc}(a\alpha) = a^{s(s-1)}d$. Choose a rational integer x so large that $\varphi(x) > 1$ and hence $\varphi(x)$ has a prime factor. If $p \mid \varphi(x)$, p is a prime then $p \mid f(y)$ (y rational integer) and $p \nmid mD$ by (13). Let $a\alpha = h(\zeta_m)$, where h is a polynomial with rational integral coefficients. Since $k = Q(a\alpha)$ the equality $h(\zeta_m) = h(\zeta_m^n)$ implies in view of the definition of k that $n \in G$. By the theorem of Schur ([3], p. 41), $p \in G$. It follows that $\varphi(x)$ has a prime factor $p_r \in G \setminus J$. Otherwise we would have $\varphi(x) = \prod p$, $p \in J$, $\varphi(x) \in J$ and by (12) $Np \in J$ contrary to (7). By (13) $p_r \nmid uN\mathfrak{b}$ thus p_r is different from all the numbers $p_0, p_1, \ldots, p_{r-1}$. The proof is complete.

Applications. Taking in Theorem 1 for G the group of rationals congruent to 1 or $l \bmod m$, and for J the group of rationals congruent to $1 \bmod m$, where $l^2 \equiv 1 \bmod m$, $l \not\equiv 1 \bmod m$, and including the well known case $l \equiv 1 \bmod m$ we obtain:

THEOREM 2. *Let $l^2 \equiv 1 \bmod m$. The arithmetic progression $mz+l$ ($z = 0, 1, \ldots$) contains infinitely many primes.*

As a further application we have the classical ([2], Satz 147)

THEOREM 3. *Let $a_1, a_2, \ldots, a_s$ be rational integers such that $a_1^{m_1}a_2^{m_2}\ldots a_s^{m_s}$ is a square only if all m_i's are even. For any sequence $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_s$ ($\varepsilon_i = \pm 1$) there exist infinitely many primes p such that $\left(\frac{a_i}{p}\right) = \varepsilon_i$ $(1 \leqslant i \leqslant s)$.*

Proof. There exist infinitely many primes $p \equiv 1 \bmod 8a_1 \ldots a_s$. By the quadratic reciprocity law every such prime satisfies $\left(\frac{a_i}{p}\right) = 1$ $(1 \leqslant i \leqslant s)$. This settles the case $\varepsilon_i = 1$ $(1 \leqslant i \leqslant s)$. Assume now that not all ε_i's are equal 1. We take in Theorem 1 for G the group of rationals congruent mod $8a_1a_2 \ldots a_s$ to odd integers $n > 0$ satisfying

$$\left(\frac{a_1}{n}\right) = 1, \ \ldots, \ \left(\frac{a_s}{n}\right) = 1 \quad \text{or} \quad \left(\frac{a_1}{n}\right) = \varepsilon_1, \ \ldots, \ \left(\frac{a_s}{n}\right) = \varepsilon_s$$

and for J the group of rationals congruent mod $8a_1a_2 \ldots a_s$ to odd integers $n > 0$ satisfying $\left(\frac{a_i}{n}\right) = 1$ $(1 \leqslant i \leqslant s)$.

It follows easily from the quadratic reciprocity law that $J \neq G$ and by Theorem 1 there exist infinitely many primes in $G \setminus J$. These primes satisfy $\left(\frac{a_i}{p}\right) = \varepsilon_i$ $(1 \leqslant i \leqslant s)$.

References

[1] 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.

[2] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, New York 1948.

[3] I. Schur, *Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen*, S.-B. Berlin. Math. Ges. 11 (1912), appendix to Archiv der Math. und Phys. (3) 20 (1912-1913).

[4] J. Wójcik, *A refinement of a theorem of Schur on primes in arithmetic progressions II*, Acta Arith. 12 (1966), pp. 97-109.

Reçu par la Rédaction le 16. 4. 1968