where e' has no prime factor such that $d'/p^2 \equiv 0$ or $1 (\mathrm{mod}\, 4)$. Hence $e'^2 | s^2$, $e'|s$, and we can put $s = e'v$.

It may be noted that although the relation between matrices T, S is one-to-one, the relation between sets $\{WT|\ W$ any unimodular automorph of $A\}$ and $\{W_0 S|\ W_0$ any unimodular automorph of $A\}$ is σ to 1, where σ is the index of a subgroup isomorphic to the group of W's in the group of W_0's.

We would like to express our appreciation to our student, Dennis R. Estes, for various suggestions and help in the writing of this paper.

References

[1] P. Bachmann, *Grundlehren der Neueren Zahlentheorie*, 1907, p. 248.

[2] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, 1966, pp. 139-143.

[3] R. Dedekind, *Gesammelte Mathematische Werke*, vol. I.

[4] L. E. Dickson, *Introduction to the Theory of Numbers*, 1929.

[5] P. G. Lejeune Dirichlet and R. Dedekind, *Zahlentheorie*, Suppl. XI, ed. 4, 1894, p. 187.

[6] R. Fricke, *Elliptische Funktionen*, 2, 1922, p. 148.

[7] C. F. Gauss, *Disquisitiones Arithmeticae*, Arts., pp. 234-243.

[8] E. Hecke, *Vorlesungen über die Theorie der Algebraischen Zahlen*, 1923, pp. 213-217.

[9] D. Hilbert, *Die Theorie der Algebraischen Zahlkörper*, § 76.

[10] E. E. Kummer, Jour. für Mathematik, 35, p. 325.

[11] R. König, Jahresbericht d. Deutschen Math.-Vereinigung, 22, 1913, pp. 239-254.

[12] E. Landau, *Vorlesungen über Zahlentheorie*, 1927, v. 3, pp. 187-196.

[13] G. Pall, (a) Bull. Amer. Math. Soc. 54 (1948), pp. 1171-1175; (b) Trans. Amer. Math. Soc. 35 (1933), pp. 491-509.

[14] J. Sommer, *Vorlesungen über Zahlentheorie*, 1907, pp. 197-220 (French transl. by A. Lévy, Paris, 1911, pp. 205-229).

[15] H. Weber, Math. Annalen, 48 (1897), pp. 459-462; Algebra III, 1908, pp. 330-337.

[16] O. Zariski and P. Samuel, *Commutative Algebra*, I, pp. 246-247.

LOUISIANA STATE UNIVERSITY
Baton Rouge, Louisiana

Reçu par la Rédaction le 1. 12. 1967

ACTA ARITHMETICA
XV (1968)

A reduction of the Čebotarev density theorem to the cyclic case

by

C. R. MacCluer (East Lansing, Mich.)

The two most useful theorems of Algebraic Number Theory are Kummer's Theorem on prime factorizations and the Čebotarev Density Theorem. Unfortunately until now Čebotarev's Theorem has been inaccessible to the beginning student because of its difficult proof. I present here a reduction of Čebotarev's Theorem to the case of cyclic extensions, a case that can be handled by *abelian L*-series. (See [1], page 165 and 218.)

Notation. If k is a number field and $\mathfrak{a}$ a fractional ideal of k, then $\|\mathfrak{a}\|_k$ will denote the absolute norm of $\mathfrak{a}$ (over the rational number field $\boldsymbol{Q}$). If K is a finite galois extension of k, $\mathfrak{p}$ a prime ideal of k, and $\mathfrak{P}$ a prime ideal of K, then

$$\left[\frac{K/k}{\mathfrak{P}}\right] \quad \text{and} \quad \left(\frac{K/k}{\mathfrak{p}}\right)$$

will denote the Frobenius and Artin symbol respectively. If G is a group, then $C_G(\sigma)$ and $\varkappa_G(\sigma)$ will denote the centralizer and the conjugacy class of σ in G respectively. Finally if S is a subset of G, then $|S|$ will denote the cardinality of S.

Theorem (Čebotarev Density Theorem). *Let k be an algebraic number field and let K be a finite galois extension of k with galois group G over k. If σ is an element of G, then the Dirichlet density of all primes $\mathfrak{p}$ of k with*

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

is

$$|\varkappa_G(\sigma)|/(G:1).$$

Reduction to the case that K/k is cyclic. Let H denote the cyclic subgroup of G generated by σ. Suppose $\mathfrak{p}$ is a prime of k with

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

Then ($\mathfrak{p}$ is unramified in K) $\mathfrak{p}$ possesses a prime divisor $\mathfrak{P}$ in K with

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

Let us now count the number of such prime divisors $\mathfrak{P}$ of $\mathfrak{p}$ in K. All such prime divisors are certainly conjugate under G but what is important here is that they are conjugate under $C_G(\sigma)$ since

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

implies that τ is an element of $C_G(\sigma)$. Therefore $\mathfrak{p}$ has exactly $\big(C_G(\sigma):H\big)$ prime divisors $\mathfrak{P}$ in K such that

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

since H is the stabilizer = the decomposition group of $\mathfrak{P}$.

Let K_Z be the fixed field of H, i.e., the decomposition field of $\mathfrak{P}$ over k. Let

$$P = \mathfrak{P} \cap K_Z.$$

Then P gains only degree in transit from K_Z to K,

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

and

$$\left(\frac{K/K_Z}{P}\right) = \varkappa_H(\sigma) = \{\sigma\}.$$

Summing up, each prime $\mathfrak{p}$ of k with

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

has exactly $\big(C_G(\sigma):H\big)$ prime divisors P in K_Z with

$$\left(\frac{K/K_Z}{P}\right) = \{\sigma\}$$

and

$$\|P\|_{K_Z} = \|\mathfrak{p}\|_k.$$

On the other hand there may be primes P_1 of K_Z with

$$\left(\frac{K/K_Z}{P_1}\right) = \{\sigma\}$$

not arising in this way but these are all of degree larger than 1 over k. Therefore

$$\big(C_G(\sigma):H\big) \sum_{\left(\frac{K/k}{\mathfrak{p}}\right)=\varkappa_G(\sigma)} 1/\|\mathfrak{p}\|_k^s = \sum_{\left(\frac{K/K_Z}{P}\right)=\{\sigma\}} 1/\|P\|_{K_Z}^s + O(1).$$

But now let us assume that the Čebotarev Density Theorem holds for cyclic extensions and in particular for K/K_Z. Then we have that the Dirichlet density of all primes $\mathfrak{p}$ of k with

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

is exactly

$$\frac{(H:1)}{\big(C_G(\sigma):1\big)} \cdot \frac{1}{(H:1)} = \frac{1}{\big(C_G(\sigma):1\big)} = \frac{|\varkappa_G(\sigma)|}{(G:1)}.$$

Reference

[1] J. W. S. Cassels, A. Froehlich ed., *Algebraic Number Theory*, Washington 1967.

MICHIGAN STATE UNIVERSITY
East Lansing, Michigan

Reçu par la Rédaction le 27. 12. 1967