ON THE DISTRIBUTION OF ELEMENTS BELONGING TO CERTAIN SUBGROUPS OF ALGEBRAIC NUMBERS

BY
CAROLE SIROVICH

I. **Introduction.** K_0 will denote a real algebraic number field and K a real normal algebraic extension of K_0. If $\sigma_1=1, \sigma_2, \sigma_3, \ldots, \sigma_n$ are the elements of the Galois group G of K/K_0 then for $a \in K$, $Nm_{K/K_0}a=\prod_{i=1}^{n} a^{\sigma_i}$, and an integer whose norm is one is a relative unit of K/K_0. When K is regarded as a subset of a real n-dimensional vector space over K_0, the relative units are contained in a hypersurface having n asymptotic hyperplanes.

Hasse [2] has shown that in some real cyclic fields over the rationals there exists a unit with the property that $n-1$ of its conjugates and -1 generate the full group of units of K. In this paper we consider, for K cyclic over K_0, the multiplicative group generated by $n-1$ conjugates of an element in K which is not in K_0 if n is an odd prime, and has conjugates whose squares are multiplicatively independent (see Definition 2) if n is not prime. It is shown here that these groups lie close to the asymptotic hyperplanes; more precisely, any infinite set of elements of each group contains a subset whose points at infinity converge to the infinite part of one of these asymptotic hyperplanes. Furthermore, the group generated by a single element of K whose square is in no subfield containing K_0, K not necessarily cyclic over K_0, lies close to the n lines which are the intersections of $n-1$ of the asymptotic hyperplanes.

We obtain as corollaries some results concerning the finiteness of the number of elements of these groups belonging to algebraic varieties. In particular we show that any linear subvariety can contain only a finite number of powers of an element of K whose square is in no subfield containing K_0. Moreover, we obtain restrictive conditions on an algebraic variety that it contain infinitely many such points. We also show that no line can contain an infinite number of elements belonging to the group generated by $n-1$ conjugates of an element of the type being considered.

The solutions to these above mentioned diophantine problems are obtained by algebraic methods and do not rely on the Thue-Siegel-Roth theorems.

Some of the results in this paper were obtained earlier in [3]. There one of the proofs employed the Gelfond-Schneider theorem. This has recently been generalized by A. Baker [1], which provides a simplification of the proof and an extension of the result.

ACKNOWLEDGMENT. The author wishes to thank Professor Leon Ehrenpreis of New York University for his advice and encouragement in the preparation of this paper.

Received by the editors January 21, 1968 and, in revised form, August 16, 1968.

II. **The one generator case.** K can be embedded in $\boldsymbol{R}^n$ as a K_0 space by identifying with $a \in K$ the n-tuple $A=(a^{\sigma_1}, a^{\sigma_2}, \ldots, a^{\sigma_n})$. The relative units of K/K_0 are then given by those elements $(x_1, x_2, \ldots, x_n)$ of K with integer components belonging to the hypersurface of $\boldsymbol{R}^n$ given by $\prod_{i=1}^n x_i = 1$. With this embedding of K the asymptotic hyperplanes $\mathscr{H}^1, \mathscr{H}^2, \ldots, \mathscr{H}^n$, are just the coordinate hyperplanes and the intersections of $n-1$ of the hyperplanes, $H^j = \bigcap_{i \neq j} \mathscr{H}^i$, $j=1, 2, \ldots, n$ are the coordinate axes. We shall have occasion to use another representation of K as a K_0 space. If $k_1, k_2, \ldots, k_n$ is a basis for K over K_0 each $a \in K$ is represented by a unique n-tuple $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ of K_0^n where $a = \sum_{i=1}^n \alpha_i k_i$. The vectors $(k_i^{\sigma_1}, k_i^{\sigma_2}, \ldots, k_i^{\sigma_n})$ form a basis for $\boldsymbol{R}^n$ in which the point $A=(a^{\sigma_1}, a^{\sigma_2}, \ldots, a^{\sigma_n})$ is represented by the n-tuple $(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Under this change of basis the coordinate axis H^j maps into the line spanned by the jth column vector of the matrix which is inverse to the matrix whose ith row vector is $(k_1^{\sigma_i}, k_2^{\sigma_i}, \ldots, k_n^{\sigma_i})$. These column vectors are of the form $(h_1^{\sigma_j}, h_2^{\sigma_j}, \ldots, h_n^{\sigma_j})$.

The point at infinity of the line spanned by the vector X in real projective n-space P^n will be denoted by X^∞. The part at infinity of a subset S of P^n will be denoted by S_∞.

DEFINITION 1. A sequence of elements $\{X_m\}$ of $\boldsymbol{R}^n$ will be said to converge if the sequence $\{X_m^\infty\}$ of P_n converges; i.e. if there is an i_0 such that the sequences of real numbers $x_m^i/x_m^{i_0}$ converges for each i, where $X_m=(x_m^1, x_m^2, \ldots, x_m^n)$.

For the case of one generator we consider two sequences of powers of a, $\{a_m\} = \{a^{m_0(m)}\}$. When $m_0(m)$ is the sequence of positive (negative) integers we let $a^{\sigma_{j_0}}$ denote the conjugate of a of largest (smallest) absolute value. $|a^{\sigma_j}| = |a^{\sigma_{j_0}}|$ for some $j \neq j_0$ if and only if $\sigma_j \sigma_{j_0}^{-1} \in G_a$, where G_a is the subgroup of G under which a^2 is invariant. If $G_a = \{\sigma_{j_1}, \sigma_{j_2}, \ldots, \sigma_{j_r}\}$ then $a^2 \in K_a$, a subfield of K of degree n/r over K_0.

The sequence $\{a_m\}$ converges if and only if the sequence $\{A_m^\infty\}$ converges. For those a whose n conjugates have distinct squares

$$\lim a_m^{\sigma_j}/a_m^{\sigma_{j_0}} = \delta_{jj_0}$$

in which case $\{A_m^\infty\}$ converges to $H_\infty^{j_0}$. For those a whose square is in K_a, $K_0 \subseteq K_a \subset K$,

$$\lim a_m^{\sigma_j}/a_m^{\sigma_{j_0}} = \pm 1$$

if $\sigma_j = \sigma_{j_i}\sigma_{j_0}$ for $i=1, 2, \ldots, r$ and otherwise is zero and therefore $\lim A_m^\infty \in \bigcap_j \mathscr{H}_\infty^j$ where j is such that $\sigma_j \neq \sigma_{j_i}\sigma_{j_0}$. Thus we have established

THEOREM 1. *The limit of a convergent infinite sequence of powers of $a \in K$ is one of the points H_∞^j if a^2 is in no subfield of K containing K_0; if a^2 is in the subfield K_a of K corresponding to G_a then the limit is contained in $\bigcap_j \mathscr{H}_\infty^j$ where the intersection is taken over all j such that $\sigma_j \sigma_{j_0}^{-1} \notin G_a$.*

COROLLARY 1. *A linear subvariety can contain only finitely many powers of an element in K whose square belongs to no subfield containing K_0.*

Proof. Let a be any such element of K and V a minimal linear variety containing infinitely many powers of a. If the dimension of V is k then we can choose elements a^{μ_i}, $i=0, 1, \ldots, k$, in V such that $a^{\mu_i}-a^{\mu_0}$, $i=1, 2, \ldots, k$, is a linearly independent set. With respect to a basis $k_1, k_2, \ldots, k_n$ for K/K_0 these vectors have coefficients in K_0 and thus V can be given in this basis by the equations $\sum_{j=1}^{n} \alpha_{ij}\chi_j=\beta_i$, $i=1, 2, \ldots, n-k$, where the α_{ij} and β_i are in K_0.

Since V is a linear variety containing infinitely many powers of a and since V_∞ is compact, by Theorem 1, V_∞ must contain at least one of the points H^j_∞. But then $\sum_{p=1}^{n} \alpha_{ip}h^{\sigma_p j}=0$ which upon conjugation yields $\sum_{j=1}^{n} \alpha_{ij}h^{\sigma_l j}=0$ for all l. However, the vectors H^l are a linearly independent set so that the assumption is false and the corollary proved.

COROLLARY 2. *If a^2 is in no subfield of K containing K_0 then from any infinite set of powers of a, a basis for K/K_0 can be chosen.*

COROLLARY 3. *If a^2 belongs to no subfield of K containing K_0 then an algebraic variety V can contain only finitely many powers of a unless $H^j_\infty \in V_\infty$ for $j=1, 2, \ldots, n$, or the origin is a singular point of V at which the normal space to V is* 0.

Proof. If V is a minimal algebraic variety containing infinitely many of the points a^m then it is the closure in the Zariski topology of these points. In the basis $k_1, k_2, \ldots, k_n$ for K/K_0 these points have coefficients in K_0 and so are left fixed by every automorphism τ of $\boldsymbol{C}/K_0$, where $\boldsymbol{C}$ is the field of complex numbers. By the continuity of τ in this topology, V must be fixed by τ. This condition is necessary and sufficient for V to be the algebraic set of zeros of polynomials $P_i(x_1, x_2, \ldots, x_n)$ with coefficients in K_0.

If some sequence of components of a^m becomes unbounded, i.e. if $|a^{\sigma_j}|>1$ for some j, then by Theorem 1, $H^j_\infty \in V_\infty$ for some j. Since the coefficients of the P_i are in K_0 we obtain by conjugation the fact that $H^j_\infty \in V_\infty$ for all j.

If none of these sequences becomes unbounded then $\lim_{m\to\infty} a^m=0$ so that V contains the origin. By Theorem 1, a^m_∞ contains a subsequence which converges to one of the points H^j_∞. Thus for some j, H^j belongs to the tangent space to V at the origin.

If at least one of the normal vectors to V at the origin,

$$(\partial P_i/\partial x_1, \ldots, \partial P_i/\partial x_n)_{(0,0,\ldots,0)},$$

is not $(0, \ldots, 0)$ then this vector, which has components in K_0, is perpendicular to the vector H^j. This is impossible as was seen in the proof of Corollary 1.

III. **The case of more than one generator.** More generally we shall consider a sequence of elements in the group generated by $N<n$ conjugates of an element a of K, however we shall now require that K be cyclic over K_0.

$$\{a_m\} = \{(a^{\sigma_{i_1}})^{m_1(m)}(a^{\sigma_{i_2}})^{m_2(m)} \cdots (a^{\sigma_{i_N}})^{m_N(m)}\}$$

which we shall write as $a_{m_1}^{\sigma^{l_1}} a_{m_2}^{\sigma^{l_2}} \cdots a_{m_N}^{\sigma^{l_N}}$, where the $m_i(m)$ are sequences of integers, not all bounded. By compactness we can assume that the $m_i(m)$ are such that $\{a^m\}$ converges. Since the sequence $A_m = (a_m^{\sigma_1}, a_m^{\sigma_2}, \ldots, a_m^{\sigma_n})$ converges there is a j_0 such that

$$\lim_{m\to\infty} \left| \frac{a_{m_1}^{\sigma^{l_1+j}} a_{m_2}^{\sigma^{l_2+j}} \cdots a_{m_N}^{\sigma^{l_N+j}}}{a_{m_1}^{\sigma^{l_1+j_0}} a_{m_2}^{\sigma^{l_2+j_0}} \cdots a_{m_N}^{\sigma^{l_N+j_0}}} \right| = L_j \tag{1}$$

is finite for each $j=0, 1, \ldots, n-1$, where $\sigma_{i+j}=\sigma^{i+j}$, σ a generator of G.

We would like to show that at least one of the L_j must be zero, i.e. that this limit belongs to at least one of the $\mathscr{H}_j^\infty$.

Assume that all of the limits L_j of (1) are nonzero. Dividing the $j+1$st equation by the jth equation for each $j=1, 2, \ldots, n-1$ and dividing the 1st equation by the nth equation and taking logarithms we obtain

$$\lim_{m\to\infty} \sum_{i=1}^{N} m_i \log \left| \frac{a^{\sigma^{l_i+j+1}}}{a^{\sigma^{l_i+j}}} \right| = \log \frac{L_{j+1}}{L_j}$$

is finite for each $j=0, 1, \ldots, n-1$. Hence for some ν and some subsequences $m_i(m')$ of the $m_i(m)$

$$\lim_{m'\to\infty} \sum_{i=1}^{N} \frac{m_i}{m_\nu} \log \left| \frac{a^{\sigma^{l_i+j+1}}}{a^{\sigma^{l_i+j}}} \right| = 0 \quad \text{for } j = 0, 1, \ldots, n-1, \tag{2}$$

where $b=a^{\sigma_1}/a$ and $\lim m_i/m_\nu$ is finite.

Let V_i be the real n-tuple

$$(\log |b^{\sigma_i}|, \log |b^{\sigma_{i+1}}|, \ldots, \log |b^{\sigma_{i+n-1}}|), \quad i = 1, 2, \ldots, n.$$

LEMMA 1. *The vectors $V_{l_1}, V_{l_2}, \ldots, V_{l_N}$ are linearly dependent over the real numbers if and only if they are linearly dependent over the rationals.*

Proof. Let $\mathscr{L}$ be the $(n\times n)$ matrix whose $i+1$st column is the vector V_i, $i=0, 1, \ldots, n-1$. Then $V_{l_1}, V_{l_2}, \ldots, V_{l_N}$ are linearly dependent over the reals if and only if there is a real nonzero n-tuple α whose 1_kth component we shall call α_k and whose other components are zero such that $\mathscr{L}\alpha=0$.

$\mathscr{L}$ is a circulant matrix and thus has n eigenvectors $EV(s)=(1, \zeta^s, \zeta^{2s}, \ldots, \zeta^{(n-1)s})$, $s=0, 1, \ldots, n-1$, where ζ is a primitive nth root of unity. With respect to the usual inner product in C^n these eigenvectors form an orthogonal set since if $t\neq 0$, ζ^t satisfies the equation $x^{n-1}+x^{n-2}+\cdots+x+1=0$. The eigenvalue corresponding to $EV(s)$ is $ev(s)=\sum_{k=0}^{n-1} \zeta^{ks} \log |b^{\sigma_k}|$.

If rank $\mathscr{L}=M$ then $ev(s_i)\neq 0$ for $1=1, 2, \ldots, M$. Thus $\mathscr{L}\alpha=0$ if and only if α is orthogonal to each of the vectors $EV(s_i)$, $i=1, 2, \ldots, M$, or equivalently $Z\alpha'=0$ where $Z=(\zeta^{l_j s_i})$, $j=1, 2, \ldots, N$, and $i=1, 2, \ldots, M$, and $\alpha'=(\alpha_1, \alpha_2, \ldots, \alpha_N)$. If there is any nonzero solution to this last equation then there is a nonzero algebraic solution.

Suppose $\alpha_1, \alpha_2, \ldots, \alpha_N$ are algebraic and $\mathscr{L}\alpha = 0$. Then $\sum_{k=1}^{N} \alpha_k \log |b^{\sigma_{l_k}}| = 0$. The theorem of A. Baker [1] mentioned previously states that if the logarithms of nonzero algebraic numbers are linearly dependent over the algebraic numbers then they are linearly dependent over the rationals. Thus there are integers $\mu_1, \mu_2, \ldots, \mu_N$ such that $\sum_{k=1}^{N} \mu_k \log |b^{\sigma_{l_k}}| = 0$ which when exponentiated gives $\prod_{k=1}^{N} (b^{\sigma_{l_k}})^{\mu_k} = \pm 1$. By taking the absolute value of the n conjugates of this equation and the logarithm of each, we see that a necessary and sufficient condition that this equality hold is that $\sum_{k=1}^{N} \mu_k V_{l_k} = 0$. Thus the lemma is established.

DEFINITION 2. A set of numbers $a_1, a_2, \ldots, a_n$ in K will be called multiplicatively dependent if there are integers $\mu_1, \mu_2, \ldots, \mu_N$ not all zero such that $\prod_{i=1}^{N} a_k^{\mu_k} \in K_0$.

COROLLARY 4. *The vectors $V_{l_1}, V_{l_2}, \ldots, V_{l_N}$ are linearly dependent over the real numbers if and only if the squares of $a^{\sigma_{l_1}}, a^{\sigma_{l_2}}, \ldots, a^{\sigma_{l_N}}$ are multiplicatively dependent.*

Proof. Since K is real and cyclic over K_0, $\prod_{k=1}^{N} (a^{\sigma_{l_k}})^{2\mu_k} \in K_0$ if and only if $\prod_{k=1}^{N} (b^{\sigma_{l_k}})^{\mu_k} = \pm 1$. The equations obtained from this one by using the procedure above together with Lemma 1 gives the result.

COROLLARY 5. *If n is prime and $a \notin K_0$ then for $N < n$, $V_{l_1}, V_{l_2}, \ldots, V_{l_N}$ are linearly independent over the reals.*

Proof. Suppose there are integers $\mu_1, \mu_2, \ldots, \mu_N$ such that $\sum_{k=1}^{N} \mu_k V_{l_k} = 0$. Since $a \notin K_0$, rank $\mathscr{L} > 0$ and therefore $ev(s) \neq 0$ for some s. Thus $\sum_{k=1}^{N} \mu_k \zeta^{l_k s} = 0$. $s \neq 0$ since the relative norm of b over K_0 is equal to one and $ev(0) = 0$. But if n is prime the numbers $\zeta^{l_1 s}, \zeta^{l_2 s}, \ldots, \zeta^{l_N s}$ for $N < n$ and $s \neq 0$ are linearly independent over the rationals. Therefore $\mu_1 = \mu_2 = \cdots = \mu_N = 0$ and by Lemma 1 the corollary is proved.

LEMMA 2. *If $a^2 \notin K_0$ and the squares of $a^{\sigma_{l_1}}, a^{\sigma_{l_2}}, \ldots, a^{\sigma_{l_N}}$ are multiplicatively dependent then some power of the n limits in* (1) *for the sequence $\{a_{m_i}\}$ are the n limits in* (1) *for some sequence $\{a_{m_i'}\}$ in the group generated by a multiplicatively independent subset of $a^{\sigma_{l_1}}, a^{\sigma_{l_2}}, \ldots, a^{\sigma_{l_N}}$.*

Proof. Suppose $\prod_{i=1}^{N} (a^{\sigma_{l_i}})^{2\mu_i} \in K_0$ and $\mu_k \neq 0$. If L_j is jth limit in (1) for $\{a_{m_i}\}$ then $L_j^{2\mu_k}$ are the corresponding limits for $\{a_{2\mu_k m_i}\} = \{\kappa^{m_k} \prod_{i=1}^{N} a_{2(\mu_k m_i - \mu_i m_k)}^{\sigma_{l_i}}\}$ where $\kappa \in K_0$. Since κ^{m_k} does not affect the limits in (1) we see that $L_j^{2\mu_k}$ are the limits for a sequence with terms generated by $N-1$ conjugates. Thus if $a^2 \notin K_0$ we can continue to reduce the set of generators until we obtain a sequence with terms generated by a multiplicatively independent subset which has limits which are an integral nonzero power of the L_j's.

DEFINITION 3. If $a, a^{\sigma_{l_1}}, a^{\sigma_{l_2}}, \ldots, a^{\sigma_{l_N}}, \{a_{m_i'}\}$ are as in Lemma 3 and m_i' is bounded for each i then the sequence $\{a_{m_i'}\}$ will be said to be exceptional.

Applying Lemma 2 and the two corollaries to Lemma 1 to the equations in (2) we immediately deduce

THEOREM 2. *If K is cyclic over K_0, $\dim K/K_0 = n > N$, then the limit of a convergent infinite sequence of elements belonging to the group generated by N conju-*

gates of $a \in K$ is contained in $\bigcup_{j=0}^{n-1} \mathscr{H}^j_\infty$ if $n>2$ is prime and $a \notin K_0$, or if n is not prime, $a^2 \notin K_0$, and the sequence is not exceptional.

COROLLARY 6. *If K is cyclic over K_0 of dimension n then infinitely many elements belonging to the group generated by $N<n$ conjugates of $a \in K$, $a^2 \notin K_0$, cannot lie on a line unless the set contains an exceptional sequence.*

Proof. If a line L contained infinitely many such elements then, by Theorem 2, $L_\infty \in \bigcup_j \mathscr{H}^j_\infty$. Then the difference of any two elements on the line would be in $\bigcup_j \mathscr{H}^j$. But the difference belongs to K and the $\mathscr{H}^j$ contain no field elements.

In the case of one generator whose square is not in a subfield containing K_0, we saw that the set of limit points is restricted to the 0 dimensional set consisting of the points of the intersection of $n-1$ of the H^j_∞. For $n-1$ generators whose squares are multiplicatively independent the limit set is contained in the $n-2$ dimensional space $\bigcup_j \mathscr{H}^j_\infty$, K/K_0 cyclic. A problem to be considered is that of finding an upper bound less than $n-2$ for the dimension of the limit set in the case of N generators, $1<N<n-1$. More precisely, for which elements of K is the limit set contained in the $N-1$ dimensional set which is the union of the intersections of $n-N$ of the $\mathscr{H}^j_\infty$.

BIBLIOGRAPHY

1. A. Baker, *Linear forms in the logarithms of algebraic numbers*. II, Mathematika **14** (1967), 102–107.

2. Helmut Hasse, *Arithmetisch Bestimmung von Grundeiheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkorpern*, Akademie-Verlag, Berlin, 1948.

3. C. Sirovich, *On the distribution of elements of groups generated by conjugates of a number in a real cyclic algebraic number field*, Dissertation, New York University, New York, 1964.

BROWN UNIVERSITY,
PROVIDENCE, RHODE ISLAND