Reprinted from the Proceedings of the NATIONAL ACADEMY OF SCIENCES,
Vol. 38, No. 5, pp. 439–440. May, 1952

GROUP INVARIANT INTEGRATION AND THE FUNDAMENTAL THEOREM OF ALGEBRA

BY HERBERT SCARF

DEPARTMENT OF MATHEMATICS, PRINCETON UNIVERSITY

Communicated by S. Bochner, March 21, 1952

In this note we shall obtain a proof of the fundamental theorem of algebra, using the fact that a group invariant integral may be constructed on a compact group. The essential lemma embodying this fact will be the following important proposition.

LEMMA. *If a group of linear transformations* $y_i = \sum_j a_{ij}(t)x_j$ *has the property that* $|a_{ij}(t)| < M$, *then there exists a positive definite quadratic form* $\sum_{ij} g_{ij}x_ix_j$ *which is left invariant by all of the transformations of the group.*

In order to prove the fundamental theorem we shall assume, to the contrary, that there exists a polynomial $p(x)$ of degree $n > 2$, with real coefficients, leading coefficient 1, which is irreducible over the reals, and will deduce a contradiction. Then the ring $Re[x]/p(x)$, of polynomials with real coefficients, taken modulo $p(x)$ is actually a field, which shall be denoted by F. This field may be considered as a vector space of dimension n over the real numbers, and after choosing a fixed basis, which we assume done, may be represented by the points in n-space. If t is any non-zero element of F, then $y = tx$ is a non-singular linear transformation, where the multiplication used is that of the field. After deletion of 0, the remaining points of n-space operate on themselves, and therefore constitute a group space. However, it is still too early to use the lemma mentioned above, since the coefficients of the transformation, which are linear forms in the components of t, are not yet bounded. In order to obtain a bounded subgroup, we consider the set G of elements of F which have the property that $N(x) = 1$, where $N(x)$ is the norm of an element in F. The norm is a homogeneous polynomial of degree n in the n components of x. As was mentioned before, if we write the transformation $y = tx$ in the customary matrix form, then the elements of the matrix $a_{ij}(t)$ are linear forms in the components of t. Therefore to show that $a_{ij}(t)$ are bounded, it is sufficient to show that the components of t are bounded for all t in G. Assume that this is not so; then there is, in G, a sequence of elements (t_i) whose maximum component in absolute value, which we shall write as $m(t_i)$ tends to ∞. Then $t_i/m(t_i)$ has all components $\leqslant 1$, and at least one component equal to 1, in absolute value, but $N\{t_i/m(t_i)\} = N(t_i)/[m(t_i)]^n = 1/[m(t_i)^n] \rightarrow 0$. The sequence $t_i/m(t_i)$ has a limit point t in F, which is not 0, but $N(t) = 0$. This is a contradiction, and thus the lemma is applicable to G.

Let $g(x)$ be that positive definite quadratic form, normalized so that $g(1) = 1$, which has the property that $g(tx) = g(x)$ for all t and x in G. Putting $x = 1$, we see that for all t in G, $g(t) = 1 = N(t)$. Now if x is any non-zero element of F, $N\{x/N(x)^{1/n}\} = 1$, so that $g\{x/N(x)^{1/n}\} = 1$, and $g(x)^n = N(x)^2$, since $g(x)$ is homogeneous of degree 2. In particular, we shall put $x = u - r$, where $p(r) = 0$, and u is a real indeterminate. Then $N(x) = N(u - r) = p(u)$ and $g(x)$ becomes an irreducible quadratic polynomial, say $f(u)$. We obtain the relation $f(u)^n = p(u)^2$. Therefore $p(u)$ is divisible by $f(u)$ and has a quadratic factor. If $n > 2$, this contradicts the irreducibility of $p(x)$.

Acknowledgment.—I wish to thank Prof. Bochner for assistance rendered.