dependent of position) of radius \( n^{1/2}/2 \) contains at least \( N(n) \) lattice points on or within it?

II. Is it possible (for certain \( n \)) to replace the number \( \lceil n/4 \rceil + 1 \) of the theorem by a number \( M(n) \) which is greater than \( \lceil n/4 \rceil + 1 \)?

**Brooklyn, N. Y. and**

**City College of the City of New York**

**ON THE MULTIPLICATIVE GROUP OF A DIVISION RING**

**W. R. SCOTT**

Let \( K \) be a noncommutative division ring with center \( Z \) and multiplicative group \( K^* \). Hua [2; 3] proved that (i) \( K^*/Z^* \) is a group without center, and (ii) \( K^* \) is not solvable. A generalization (Theorem 1) will be given here which contains as a special case (Theorem 2) the fact that \( K^*/Z^* \) has no Abelian normal subgroups. This latter theorem obviously contains both (i) and (ii). As a further corollary it is shown that if \( M \) and \( N \) are normal subgroups of \( K^* \) not contained in \( Z^* \), then \( M \cap N \) is not contained in \( Z^* \). The final theorem is that an element \( x \) outside \( Z \) contains as many conjugates as there are elements in \( K \). This makes more precise a theorem of Herstein [1], who showed that \( x \) has an infinite number of conjugates.

Square brackets will denote multiplicative commutation. If \( S \) is a set, then \( o(S) \) will mean the number of elements in \( S \). A subgroup \( \mathcal{H} \) of \( K^* \) is subinvariant in \( K^* \) if there is a chain \( \{ N_i \} \) of subgroups such that \( \mathcal{H} \triangleleft N_0 \triangleleft \cdots \triangleleft N_i \triangleleft K^* \), where \( A \triangleleft B \) means that \( A \) is a normal subgroup of \( B \).

**Lemma.** Let \( K \) be a division ring, \( H \) a nilpotent subinvariant subgroup of \( K^* \), \( y \in H, x \in K^* \), and \( [y, x] = \lambda \in Z^* \), \( \lambda \neq 1 \). Then the field \( Z(x) \) is finite.

**Proof.** The proof of this lemma is essentially part of Hua's proof of (ii), but will be included for the sake of completeness.

Let \( f \) be any rational function over \( Z \) such that \( f(x) \neq 0 \). Then

Presented to the Society, November 23, 1956; received by the editors June 15, 1956.
\[ x_1 = [y, f(x)] = yf(x)y^{-1}f(x)^{-1} = f(yx^{-1})f(x)^{-1} = f(\lambda x)f(x)^{-1}; \]
\[ x_2 = [y, x_1] = f(\lambda^2 x)f(\lambda x)^{-2}f(x); \]
and, by induction, if \( x_n = [y, x_{n-1}] \), then
\[ x_n = \prod_{i=0}^{n} f(\lambda^i x)^{-n-i}(?) \]

Now, by the subinvariance of \( H \), \( x_1 \in N_1 \), \( x_2 \in N_2 \), \ldots, \( x_r \in H \), and since \( H \) is nilpotent, \( x_n = 1 \) for some \( n \). Letting \( f(x) = 1 + x \), we have

\[ \prod (1 + \lambda^i x)^{(?)} - \prod (1 + \lambda^i x)^{(?)} = 0, \]

where the first product is taken over those \( i \) such that \( n - i \) is even and the second over those \( i \) such that \( n - i \) is odd, \( i = 0, \ldots, n \). In the left member, the constant term is equal to 0, while the coefficient of \( x \) is

\[ \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} \lambda^i = (\lambda - 1)^n \neq 0. \]

Thus \( x \) is algebraic (of degree at most \( 2^{n-1} - 1 \)) over \( Z \). If \( c \in Z^* \), then \( [y, cx] = \lambda \), and \( cx \) is also a root of (1). Therefore \( Z \) is finite, and \( Z(x) \) is finite as asserted.

**Theorem 1.** Let \( K \) be a division ring, \( G \) and \( H \) subinvariant subgroups of \( K^* \), \( x \in G \), \( y \in H \), and \( [y, x] = \lambda \in Z^* \lambda \neq 1 \). Then one of \( G \) and \( H \) is not nilpotent.

**Proof.** Deny the theorem. By the lemma \( Z \) is finite and both \( x \) and \( y \) are algebraic over \( Z \). Since \( yx = \lambda xy \), the set \( S \) of elements of the form \( \sum z_{ij} x^i y^j \), \( z_{ij} \in Z \), is a finite noncommutative division ring.

**Theorem 2.** If \( K \) is a noncommutative division ring, then \( K^*/Z^* \) has no normal Abelian subgroups.

**Proof.** If \( N/Z^* \) is a normal Abelian subgroup, then \( N \) is a nilpotent normal subgroup of \( K^* \). The division ring generated by \( N \) is invariant, hence by the Cartan-Brauer-Hua theorem is \( K \) itself. Therefore \( N \) is non-Abelian, and there are elements \( x, y \in N \) such that \( [y, x] = \lambda \in Z^* \lambda \neq 1 \). This contradicts Theorem 1.

**Remark.** The proof of Theorem 2 depends on Wedderburn’s theorem that a finite division ring is a field. This can be avoided by the following considerations. Using the notation of the preceding proofs, \( x_1 = [y, 1 + x] \in N \), \( x_2 = [y, x_1] \in Z \), \( x_3 = [y, x_2] = 1 \), and \( n \leq 3 \). However, the coefficient of \( x^4 \) in the left member of (1) vanishes, so that \( x \) and \( y \) are of degree 2 over \( Z \), and \( o(Z) = 3 \) since it contains the distinct
elements 0, 1, and $\lambda$. Then $o(S) \leq 3^4$, and since $S$ must have room for a center and a subfield not in the center, $o(S) = 3^4$ and $Z$ is the center of $S$. Thus $S^*$ is a group of order 80 and contains an element $u$ of order 5. The centralizer $C(u)$ of $u$ in $S$ is a division ring, hence of order 3, 9, or 81, therefore by Lagrange's theorem of order 81. But then $u \in Z$, $o(Z) \geq 5$, and the contradiction proves the theorem.

**Theorem 3.** Let $K$ be a division ring and $M$ and $N$ be normal subgroups of $K^*$ not contained in $Z^*$. Then $M \cap N$ is not contained in $Z^*$.

**Proof.** Deny the theorem. Then $[M, N] \subset Z^*$. Let $y \in N$, $y \in Z^*$. Since the centralizer $C(M)$ of $M$ is an invariant division ring not $K$, by the Cartan-Brauer-Hua theorem, $C(M) = Z$. Hence $y \in C(M)$, and there is an $x$ in $M$ such that $[y, x] = \lambda \neq 1$, $\lambda \in Z^*$. The map $\sigma = [x, \cdot]$ is a homomorphism of $N$ into $Z^*$ with kernel $L \subseteq [N, N]$. Since $y \in L$, $y \in [N, N]$, and since $y$ was arbitrary, $[N, N] \subset Z^*$. Therefore $N$ is nilpotent. Similarly $M$ is nilpotent and Theorem 1 is contradicted.

**Lemma.** Let $K$ be an infinite division ring (perhaps commutative), $D$ a proper subdivision ring. Then $[K^* : D^*] = o(K)$.

**Proof.** Let $x \in K^*$, $x \in D^*$. Then the cosets $D^*(x + a)$, $a \in D$, are distinct. Hence $[K^* : D^*] \geq o(D)$. If $o(D) = o(K)$ we are done; if not, then $o(K) = o(K^*) = o(D^*) [K^* : D^*]$, hence again $[K^* : D^*] = o(K)$.

**Theorem 4** (See [1]). If $K$ is a division ring and $x$ is a noncentral element, then $x$ has $o(K)$ conjugates.

**Proof.** The centralizer $C$ of $x$ is a proper subdivision ring of $K$. Then the number of conjugates of $x$ equals $[K^* : C^*]$ which is $o(K)$ by the lemma.

**Bibliography**


University of Kansas and
Institute for Advanced Study