FINITE MULTIPLICATIVE SUBGROUPS IN DIVISION RINGS

I. N. HERSTEIN

1. **Introduction.** If G is a finite subgroup of the multiplicative group of nonzero elements of a commutative field, then it is known that G must be cyclic. This result clearly is not true for general division rings, as is shown, for instance, by the example of the group

$$G = (\pm 1, \pm i, \pm j, \pm k)$$

in the division algebra of the quaternions over the real field. One might ask, however, if there exist extensions or analogues of the theorem for commutative fields to general division rings. The results of this paper are in the direction of possible such extensions. One result we obtain is, in fact, that if K is of characteristic p, $p \neq 0$, then any finite multiplicative subgroup of the group of nonzero elements is indeed cyclic. For arbitrary K, the groups of odd order are at least metacyclic, and in the special case of the quaternions the subgroups of odd order are all cyclic.

Let K be a division ring with center Z, and let K^* be the multiplicative group of nonzero elements of K. Whenever we write $G \subset K^*$, we mean that G is a subgroup of K^* under the multiplication defined in K^*.

2. **Results on finite subgroups of K^* for general K.** Suppose that $G \subset K^*$ is both finite and Abelian. Let the elements of G be $g_1, g_2, \cdots, g_n$. Consider $T = Z(g_1, \cdots, g_n)$, the division ring obtained by adjoining $g_1, \cdots, g_n$ to Z. Since G is Abelian, T must be commutative, so T is a commutative field; moreover $G \subset T^*$. Thus, being a finite subgroup of the multiplicative group of a field, G is cyclic. So we have:

LEMMA 1. *If $G \subset K^*$ is an Abelian group of finite order, then G is cyclic.*

Let p be a prime number. If G is of order p or p^2, it is Abelian. So by Lemma 1 we obtain:

LEMMA 2. *If $G \subset K^*$ is of order p or p^2, then G is cyclic.*

Received April 5, 1952.

LEMMA 3. *If $G \subset K^*$ is of order p^r, p an odd prime, then G is cyclic.*

Proof. Our proof is by induction over r:

(1) If $r = 1$, or $r = 2$, this is merely Lemma 2.

(2) Suppose that all $G \subset K^*$ of order p^v, $v < r$, are cyclic. Let $G \subset K^*$ be of order p^r, $r > 2$. Then by the induction hypothesis all the proper subgroups of G are cyclic. Since p is an odd prime and $r > 2$, by Satz 88 [2, p. 72], G is cyclic. Thus Lemma 3 is established.

THEOREM 4. *If $G \subset K^*$ is of odd order, then G is metacyclic.*

Proof. All the Sylow subgroups of G belong to odd primes, so they are cyclic by Lemma 3. Hence G is metacyclic [3, p. 145, Theorem 11].

As a consequence of the metacyclicity of G we obtain [3, p. 145, Theorem 11]:

THEOREM 5. *If $G \subset K^*$ is of odd order, then there exist $a, b \in G$ which generate all of G, and which satisfy*

(1) $a^n = b^m = 1$ $\qquad$ *(n, m odd)*

(2) $bab^{-1} = a^r$.

3. **The case where K is of characteristic p, $p \neq 0$.** In this section we assume K is of characteristic p, $p \neq 0$. Let $P \subset Z$, Z the center of K, P the prime field of characteristic p.

THEOREM 6. *If $G \subset K^*$ is of finite order, then G is cyclic.*

Proof. Let

$$U = \left\{ x \in K \mid x = \sum_{j=1}^{n} p_j\, g_j,\ p_j \in P,\ g_j \in G \right\}.$$

Clearly U is a group under multiplication and addition. Moreover, U is finite, since P is finite. Since U is contained in K, it can have no divisors of zero. Thus U is a finite division ring. By Wedderburn's theorem, U must then be commutative; since $G \subset U^*$, we then have the result that G is cyclic.

So for division rings of nonzero characteristic, the result for commutative fields carries over in its entirety. One might well ask how much of the result carries over in the case of division rings of characteristic zero. We have not solved this completely as yet; but in the special case that K is the quaternion algebra over the real field, we obtain a fairly satisfactory answer.

4. K the real quaternions.

In this section, K will denote the division algebra of the quaternions over the real field Z (Z is then, of course, also the center of K). The principal result we obtain is:

THEOREM 7. *If $G \subset K^*$ is of odd order, then G is cyclic.*

We first establish several preliminary lemmas.

Suppose that $x \in K$. The normalizer of x, $\mathfrak{n}(x)$, is defined by

$$\mathfrak{n}(x) = \{a \in K \mid ax = xa\}.$$

Trivially, $Z \subset \mathfrak{n}(x)$; and $\mathfrak{n}(x)$ is a division algebra over the reals. Not being the reals or the quaternions, $\mathfrak{n}(x)$ must be isomorphic with the complex numbers. Thus there must be a $t \in \mathfrak{n}(x)$, with $t^2 = -1$, so that every $a \in \mathfrak{n}(x)$ can be written as $a = \alpha_0 + \alpha_1 t$, where $\alpha_i \in Z$. Let

$$C = \{y \in K \mid y = \gamma_0 + \gamma_1 i, \gamma_j \in Z\}.$$

Then C is also isomorphic to the complex numbers. There exists an isomorphism of $\mathfrak{n}(x)$ onto C which leaves the elements of Z fixed. The next two lemmas are concerned with establishing the nature of this isomorphism. Using results about division subalgebras of division algebras [1, p.42, Satz 3], we could obtain the results immediately; but, for the sake of self-containment, we establish these results here.

LEMMA 8. *If $t \in K$ is such that $t^2 = -1$, then there exists an $S \in K$ so that $StS^{-1} = i$.*

Proof. Suppose that

$$t = \tau_0 + \tau_1 i + \tau_2 j + \tau_3 k \qquad (\tau_m\text{'s in } Z).$$

Since $t^2 = -1$, it follows that $\tau_0 = 0$ and $\tau_1^2 + \tau_2^2 + \tau_3^2 = 1$. If $\tau_1 = 1$, then $t = i$ and there is nothing to prove. So we suppose that $\tau_1 \neq 1$. A simple computation then shows that $StS^{-1} = i$, where

$$S = S_0 + S_1 i + S_2 j + S_3 k,$$

and where

$$S_0 = \frac{\tau_3 - \tau_2}{2\sqrt{1-\tau_1}}\,, \quad S_1 = \frac{\tau_3 + \tau_2}{2\sqrt{1-\tau_1}}\,, \quad S_2 = S_3 = \frac{\sqrt{1-\tau_1}}{2}\,.$$

Now

$$\mathfrak{N}(x) = \{a \in K \mid a = \alpha_0 + \alpha_1 t,\ \alpha_i\text{'s in } Z,\ t^2 = -1\},$$

$$C = \{g \in K \mid g = \gamma_0 + \gamma_1 i,\ \gamma_j\text{'s in } Z\}.$$

By Lemma 8, there exists an S so that $StS^{-1} = i$, whence $S\mathfrak{N}(x)S^{-1} = C$. So we have shown:

LEMMA 9. *If $x \notin Z$, then there exists an $S \in K$ so that $S\mathfrak{N}(x)S^{-1} = C$.*

LEMMA 10. *If $a,\ b \in K$, $a^n = b^m = 1$, and $bab^{-1} = a^r$, then either $ab = ba$ or $a^{-1}b = ba$.*

Proof. If $a \in Z$, then $ab = ba$, and the result is correct. Suppose then that $a \notin Z$. Since $a \in \mathfrak{N}(a) \neq K$, by Lemma 9 there exists an $S \in K$ so that $SaS^{-1} \in C$. Thus (if we assume n is the least positive integer so that $a^n = 1$),

$$A = SaS^{-1} = \cos\frac{2\pi\lambda}{n} + i\sin\frac{2\pi\lambda}{n} \qquad [(\lambda, n) = 1]$$

is a primitive nth root of unity in C. Let

$$B = SbS^{-1} = \beta_0 + \beta_1 i + \beta_2 j + \beta_3 k,\ \beta_i \in Z.$$

From $bab^{-1} = a^r$, we obtain $BAB^{-1} = A^r$. If $\beta_2 = \beta_3 = 0$, then $AB = BA$ since in that case both A and B would be in C. So we suppose one of them, say β_2, is not zero. Then $BAB^{-1} = A^r$ yields

$$(1)\qquad (\beta_0 + \beta_1 i + \beta_2 j + \beta_3 k)\left(\cos\frac{2\pi\lambda}{n} + i\sin\frac{2\pi\lambda}{n}\right)$$

$$= \left(\cos\frac{2\pi\lambda r}{n} + i\sin\frac{2\pi\lambda r}{n}\right)(\beta_0 + \beta_1 i + \beta_2 j + \beta_3 k).$$

Computing the coefficients of j and k in (1), we obtain

$$(2a)\qquad \beta_2\left(\cos\frac{2\pi\lambda}{n} - \cos\frac{2\pi\lambda r}{n}\right) + \beta_3\left(\sin\frac{2\pi\lambda}{n} + \sin\frac{2\pi\lambda r}{n}\right) = 0,$$

$$(2\mathrm{b}) \qquad -\beta_2\left(\sin\frac{2\pi\lambda}{n} + \sin\frac{2\pi\lambda r}{n}\right) + \beta_3\left(\cos\frac{2\pi\lambda}{n} - \cos\frac{2\pi\lambda r}{n}\right) = 0.$$

Since $\beta_2 \neq 0$, we have

$$(3) \qquad \begin{vmatrix} \cos\frac{2\pi\lambda}{n} - \cos\frac{2\pi\lambda r}{n} & \sin\frac{2\pi\lambda}{n} + \sin\frac{2\pi\lambda r}{n} \\ -\left(\sin\frac{2\pi\lambda}{n} + \sin\frac{2\pi\lambda r}{n}\right) & \cos\frac{2\pi\lambda}{n} - \cos\frac{2\pi\lambda r}{n} \end{vmatrix} = 0.$$

Expanding this determinant, we have

$$(4) \qquad \cos\frac{2\pi\lambda\,(r+1)}{n} = \cos\frac{2\pi\lambda}{n}\cos\frac{2\pi\lambda r}{n} - \sin\frac{2\pi\lambda}{n}\sin\frac{2\pi\lambda r}{n} = 1.$$

Since $(\lambda, n) = 1$, from (4) we obtain $n \mid (r + 1.)$

Thus $BA = A^rB = A^{-1}B$, since $A^n = 1$; this gives correspondingly for a and b the result that $ba = a^{-1}b$, which is the lemma.

COROLLARY. *If $a^n = b^m = 1$, n and m both odd, and $bab^{-1} = a^r$, then $ba = ab$.*

For if $bab^{-1} = a^{-1}$ then $b^2a = ab^2$, and since m is odd this gives $ba = ab$.

Proof of Theorem 7. Since $G \subset K^*$ is of odd order, by Theorem 5 there exist $a, b \in G$ which generate G and which satisfy

(1) $a^n = b^m = 1$ $(n, m \text{ odd})$,

(2) $bab^{-1} = a^r$.

Thus by the corollary to Lemma 10, $ab = ba$. So G must be an Abelian group; since G is in K^*, an application of Lemma 1 yields the result that G is cyclic. This is Theorem 7.

One might hope that a more general result would hold. Such a result might be that if K is a division ring, then any finite subgroup G, $G \subset K^*$, which is of odd order, is cyclic. It would be enough to prove this for division algebras of finite order over the rationals.

REFERENCES

1. M. Deuring, *Algebren*, Chelsea, New York, 1948.

2. A. Speiser, *Die Theorie der Gruppen von endlicher Ordnung,* Third Edition, Dover, New York, 1945.

3. H. Zassenhaus, *Theory of groups,* English Translation, Chelsea, New York, 1949.

Cowles Commission for Research in Economics
and the University of Chicago