A NOTE ON SOME PROPERTIES OF FINITE RINGS

GEORGE F. LEGER, JR.1

Our first result is the determination of those finite rings $R$ which have the following property

$*(k):$ The only ideals of $R$ are $R, R^2, \ldots, R^k = (0)$.

Throughout this note the term "ideal" shall be used in place of the term "two-sided ideal."

THEOREM I. Let $R$ have property $*(k)$ and let $I[z]$ denote the ring of polynomials in the indeterminate $z$ with integral coefficients. Then there exists a prime $p$ and a polynomial $f(z) = pz - \sum_{i=1}^{k-1} a_i z^i$ with $0 \leq a_i < p$ such that $R \cong z I[z]/(f(z), z^k)$. Conversely, if $f(z)$ has this form, then $z I[z]/(f(z), z^k)$ has property $*(k)$.

Proof. Let $R$ have $*(k)$. We assert that $R$ has a prime power number of elements. If not, say $o(R) = ab$ with $(a, b) = 1$, then $A = \{r \mid ar = 0\}$ and $B = \{r \mid br = 0\}$ are two ideals of $R$ such that $A \cap B = \emptyset$, which contradicts $*(k)$. Thus $o(R) = p^n$ for some prime $p$.

We assume $k > 1$ and choose $x \in R, x \notin R^2$. Then the subring $(R^2, x)$ of $R$ generated by $R^2$ and $x$ is an ideal properly containing $R^2$ whence $(R^2, x) = R$. This gives $R = (R^2, x)^* = (R^{*+1}, x^*)$. Taking $s = k - 1, k - 2, \ldots$, we find that $R$ is the image of $z I[z]$ (if the ring of rational integers, $z$ an indeterminate) by the homomorphism $\phi$ which sends $z$ into $x$.

Now we claim that $px \in R^2$. Indeed, otherwise we should have $(R^2, px) = R$ whence there exists an integer $s$ such that $x - spx \in R^2$ which gives $x^{k-1} = spx^{k-1} = \cdots = s^k px^{k-1} = 0$ whence $R^{k-1} = (0)$, a contradiction. Thus $px = a_2 x^2 + a_3 x^3 + \cdots + a_{k-1} x^{k-1}$ with the $a_i$ rational integers, so that if we put $f(z) = pz - a_2 z^2 - a_3 z^3 - \cdots - a_{k-1} z^{k-1}$, the ideal $(z^k, f(z))$ is contained in the kernel of $\phi$. Conversely, every element of the kernel of $\phi$ is congruent modulo $(z^k, f(z))$ to a polynomial of the form $b_1 z + \cdots + b_{k-1} z^{k-1}$ with $0 \leq b_i < p$. If $b_i \neq 0$, then $b_i x$ is in $R^2$ which is impossible. Similarly each $b_i = 0$ for $1 \leq i \leq k - 1$ so that the kernel of $\phi$ is $(z^k, f(z))$, i.e. $R \cong z I[z]/(z^k, f(z))$.

Conversely let $J$ be any ideal of $z I[z]/(z^k, f(z))$ where $f(z) = pz - a_2 z^2 - \cdots - a_{k-1} z^{k-1}$ with $0 \leq a_i < p$ and let $\bar{z}$ denote the coset of $z$. Every element of $J$ has the form $b_1 \bar{z} + \cdots + b_{k+1} \bar{z}^{k-1}$ with the $b_i$...
rational integers and \( 0 \leq b_i < p \). Let \( m \) be the smallest index such that \( J \) contains an element of the form \( b_m \overline{z}^m + \cdots + b_{k-1} \overline{z}^{k-1} \) with \( b_m \neq 0 \). Multiplying this element by \( \overline{z}^{k-m-1} \), we see that \( b_m \overline{z}^{k-1} \) is in \( J \) whence \( \overline{z}^{k-1} \) is in \( J \). Multiplying by \( \overline{z}^{k-m-2} \) we see that \( b_m \overline{z}^{k-2} + b_{m+1} \overline{z}^{k-1} \) is in \( J \) whence \( \overline{z}^{k-2} \) is in \( J \). Similarly, \( \overline{z}^{k-3}, \ldots, \overline{z}^m \) are in \( J \) whence \( J = \mathbb{Z}^m \).

**Corollary.** If \( R \) has property \( \ast(k) \), then there exists a prime \( p \) such that \( o(R) = p^{k-1} \) and the following properties of \( R \) imply each other:

1. \( pR = R^2 \),
2. the additive group of \( R \) is cyclic,
3. \( R \cong \mathbb{Z}/p^k \mathbb{Z} \).

**Proof.** By Theorem I, there exists a prime \( p \) and a polynomial \( f(z) \) of the form \( f(z) = pz - \sum_{i=2}^{k-2} a_i z^i \) with \( 0 \leq a_i < p \) so that \( R \cong \mathbb{Z}[z]/(f(z), z^k) \). Now \( \mathbb{Z}[z]/(f(z), z^k) \) consists of rational integral linear combinations of the cosets \( z, z^2, \ldots, z^{k-1} \) where the coefficients, say \( b_i \), are constrained by \( 0 \leq b_i < p \). It follows that \( o(R) = p^{k-1} \).

If \( R \) has property (1), then \( a_2 = 0 \) so that the additive order of \( \overline{z} \) is \( p^{k-1} \) whence \( \overline{z} \) generates the additive group of \( R \) so that \( R \) has property (2).

To see that (2) implies (3) note that \( \overline{z}^2 = h \overline{z} \) for some integer \( h \). It is easy to see that \( h = cp \) where \( (c, p) = 1 \) whence there is an integer \( h_1 \) prime to \( p \) so that \( (h_1 \overline{z})^2 = p(h_1 \overline{z}) \). Now the map \( p^i \to p^i \overline{z} \) is a homomorphism of \( p^i \) onto \( R \) with kernel \( p^k \).

**Theorem II.** Let \( R \) be a finite ring with an identity and with a non-zero radical \( N \). Suppose further that there exists a prime \( p \) such that the only ideals of \( R \) and \( R, pR, \ldots, p^k R = (0) \) and that every ideal of \( N \) is also an ideal of \( R \). Then \( R \cong \mathbb{Z}/p^k \mathbb{Z} \).

**Proof.** Clearly \( o(R) \) is a power of \( p \). Thus \( pR \subseteq N \) and we have \( R \cong N \cong pR \) whence \( N = pR \). Let \( J \) be any ideal of \( N \); then Theorem I implies that \( J \) has the form \( p^i R \), i.e. \( N^r = p^r R = J \), so that every ideal of \( R \) is a power of \( N \). The ring \( N/N^2 \) has no ideals and hence has \( p \) elements. The mapping \( x \to px \) induces a homomorphism of \( R/N \) onto \( N/N^2 \), both considered as double modules over \( R \). As a double module, \( R/N \) is simple; hence \( R/N \cong N/N^2 \) (module isomorphic) so \( R/N \) is cyclic of order \( p \). If \( e \) is the identity of \( R \), then \( R = Ie + pR \) and by induction \( R = Ie + p^i R \), so that \( R = Ie \). Thus \( n \to ne \) is a homomorphism of \( I \) onto \( R \) with kernel \( p^k \).

**Syracuse University**