REMARKS ON A GOLDbach PROPERTY

Sun Ju Jang

Abstract. In this paper, we study Noetherian Boolean rings. We show that if $R$ is a Noetherian Boolean ring, then $R$ is finite and $R \simeq (\mathbb{Z}_2)^n$ for some integer $n \geq 1$. If $R$ is a Noetherian ring, then $R/J$ is a Noetherian Boolean ring, where $J$ is the intersection of all ideals $I$ of $R$ with $|R/I| = 2$. Thus $R/J$ is finite, and hence the set of ideals $I$ of $R$ with $|R/I| = 2$ is finite. We also give a short proof of Hayes's result: For every polynomial $f(x) \in \mathbb{Z}[x]$ of degree $n \geq 1$, there are irreducible polynomials $g(x)$ and $h(x)$, each of degree $n$, such that $g(x) + h(x) = f(x)$.

All rings are assumed to be commutative rings with identity. We use the term dimension of $R$, denoted $\dim R$, to refer to the Krull dimension of $R$. A ring $R$ is called von Neumann regular if for each $x$ in $R$, there exists $y$ in $R$ such that $x = yxy$. It is well known that $R$ is von Neumann regular if and only if $R$ is zero-dimensional and reduced if and only if $R_P$ is a field for each $P \in \text{Spec}(R)$ if and only if each ideal of $R$ is a radical ideal if and only if each principal ideal of $R$ is idempotent [4, Theorem 3.1]. In particular, $\dim R = 0$ if and only if $R/\text{nil}(R)$ is von Neumann regular (where $\text{nil}(R)$ is the nilradical of $R$) if and only if a power of each principal ideal of $R$ is idempotent - that is, if and only if, for each $x \in R$, there exists $n(x) \in \mathbb{Z}^+$ and $y \in R$ such that $x^{n(x)} = yx^{n(x)+1}$ [4, Theorem 3.4]. The class of von Neumann regular rings is closed under taking homomorphic images, quotient rings, and arbitrary products [4, Result 3.2].

$R$ is called a Boolean ring if every element is idempotent. It is well known that $R$ is a Boolean ring if and only if $R_M$ is isomorphic to $\mathbb{Z}_2$ for each maximal ideal $M$ of $R$. A Boolean ring is a von Neumann regular ring, Goldbach property.
ring with $x = x1x$. It is known that $R/\text{nil}(R)$ is Boolean if and only if $\dim R = 0$ and for each maximal ideal $M$ of $R$, $R/M \simeq \mathbb{Z}_2$ if and only if given $x \in R$, there exists a natural number $n$ with $x^n(1 + x)^n = 0$ [1, Theorem 5].

In this paper, we study Noetherian Boolean rings. We show that if $R$ is a Noetherian Boolean ring, then $R$ is finite and $R \simeq \mathbb{Z}_2^n$ for some integer $n \geq 1$. If $R$ is a Noetherian ring, then $R = J$ is a Noetherian Boolean ring, where $J$ is the intersection of all ideals of $\mathcal{I}_2 = \{I \mid I$ is an ideal of $R$ and $|R/I| = 2\}$. Thus $R/J$ is finite, and hence the set $\mathcal{I}_2$ is finite. We also give a short proof of Hayes’s result using Chinese Remainder Theorem for rings.

For future reference, we include a result from [4, Theorem 3.1(4)].

**Lemma 1.** If $R$ is a Boolean ring, then $M^2 = M$ for each ideal $M$ of $R$.

**Proof.** If $x \in M$, then $x = x^2 \in M^2$. Hence $M \subseteq M^2$, and thus $M = M^2$. □

Let $I$ and $J$ be ideals of $R$. Recall that $I$ and $J$ are comaximal if $I + J = R$. Suppose that $I$ and $J$ are comaximal. Then there exist $a \in I$ and $b \in J$ such that $a + b = 1$. For any integer $m, n (\geq 1)$,

$1 = (a + b)^{m+n}$ and $(a + b)^{m+n} \in I^m + J^n$; so $I^m + J^n = R$, and hence $I^m$ and $J^n$ are also comaximal [7, Lemma 4].

For future reference, we include the Chinese Remainder Theorem [3, Section 7.6].

**Lemma 2.** (Chinese Remainder Theorem) Let $I_1, I_2, \ldots, I_n$ be ideals of $R$. The map $R \rightarrow R/I_1 \times R/I_2 \times \cdots \times R/I_n$ defined by $r \mapsto (r + I_1, r + I_2, \ldots, r + I_n)$ is a ring homomorphism with kernel $I_1 \cap I_2 \cap \cdots \cap I_n$. If each ideals $I_i, I_j$ ($i \neq j$) are comaximal, then the map is surjective and $I_1 \cap I_2 \cap \cdots \cap I_n = I_1 I_2 \cdots I_n$, so $R/(I_1 I_2 \cdots I_n) \simeq R/(I_1 \cap I_2 \cap \cdots \cap I_n) \simeq R/I_1 \times R/I_2 \times \cdots \times R/I_n$.

If $R$ is a finite Boolean ring, then $R \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ (c.f. [3, Exercise 2, p. 267]). We next show that a Noetherian Boolean ring $R$ is finite with $R \simeq (\mathbb{Z}_2)^n$ for some integer $n \geq 1$.

**Theorem 3.** Let $R$ be a Boolean ring.
(1) $R$ is zero-dimensional reduced and for each maximal ideal $M$ of $R$, $R/M \simeq \mathbb{Z}_2$.

(2) If $R$ is Noetherian, then $R$ is a finite ring with $R \simeq (\mathbb{Z}_2)^n$ for some integer $n \geq 1$.

**Proof.** (1) Suppose that $\dim R > 0$. Then there are primes $P \subsetneq M$. Let $x \in M - P$. Then $x = x^2$, and so $x(x - 1) = 0 \in P$. Since $x \notin P$, we have $x - 1 \in P \subseteq M$. But $x \in M$, so $1 \in M$, a contradiction. Clearly $\text{nil}(R) = \{0\}$. Let $M$ be a maximal ideal of $R$. Then $R = M$ is a field and a Boolean ring; so $R = M \simeq \mathbb{Z}_2$.

(2) Suppose that $R$ is Noetherian. Then since, each ideal of $R$ contains a product of prime ideals of $R$ [3, Corollary 22, p. 685], we have $0 = P_1^{r_1}P_2^{r_2} \cdots P_n^{r_n}$. By Lemma 1, each $P_i^{r_i} = P_i$; so $0 = P_1P_2 \cdots P_n$ and $P_1, P_2, \ldots, P_n$ are distinct. Since the ideals $P_i$ and $P_j$ with $i \neq j$ are comaximal, the map $R \to R/P_1 \times R/P_2 \times \cdots \times R/P_n$, $r \to (r + P_1, r + P_2, \ldots, r + P_n)$ is an epimorphism with kernel $P_1 \cap P_2 \cap \cdots \cap P_n = P_1P_2 \cdots P_n = \{0\}$ by Lemma 2. Hence $R \simeq R/\{0\} \simeq R/P_1 \times R/P_2 \times \cdots \times R/P_n$. Now, each $R/P_i \simeq \mathbb{Z}_2$ by (1). Hence $R \simeq (\mathbb{Z}_2)^n$ for some integer $n \geq 1$.

**Corollary 4.** (c.f., [7, Lemma 7], [9, Proposition 13]) Let $R$ be a ring and let

$$\mathcal{I}_2 = \{I \mid I \text{ is an ideal of } R \text{ and } |R/I| = 2\}.$$ 

Let $J$ be the intersection of all ideals in $\mathcal{I}_2$. Then $R/J$ is a Boolean ring. Moreover, if $R$ is Noetherian, then $R/J$ is a finite ring with $|R/J| = 2^n$ for some integer $n \geq 1$ and $\mathcal{I}_2$ is finite.

**Proof.** Let $x \in R$. For each $I \in \mathcal{I}_2$, we have $x^2 - x \in I$. Thus for each $x \in R$, $x^2 - x \in \bigcap \{I \mid I \in \mathcal{I}_2\} = J$. Therefore $R/J$ is a Boolean ring. In particular, if $R$ is Noetherian, then $R/J$ is Noetherian, and so by Theorem 3, $R/J$ is a finite ring with $|R/J| = 2^n$ for some integer $n \geq 1$. Hence $\{I/J \mid |R/I| = 2\}$ is finite. Since the map $I \to I/J$ is injective, $\mathcal{I}_2$ is finite.

Let $R$ be a Noetherian ring and let $\mathcal{I}_n = \{I_a\}_{a \in A}$, where $|R/I_a| = n$. Define $J = \bigcap_{a \in A} I_a$. Then $R/J$ can be imbedded in $\prod_{a \in A}(R/I_a)$. Then $R/J$ is zero-dimensional Noetherian and hence Artinian. Hence
$J = \bigcap I_a$ has a finite subintersection, so $R/J$ is imbedded in $\prod_{i=1}^{k} (R/I_a)$, a ring of cardinality $n^k$. Therefore $R/J$ is finite and hence $\{I_a/J\}_{a \in \Lambda}$ is finite. Since the map $I_a \to I_a/J$ is injective, $\mathcal{I}_n = \{I_a\}_{a \in \Lambda}$ is finite [5, Result 3].

D. Hayes [6] was the first to observe and prove the following polynomial analogue of the celebrated Goldbach conjecture:

**Theorem 5.** For every polynomial $f(x) \in \mathbb{Z}[x]$ of degree $n \geq 1$, there are irreducible polynomials $g(x)$ and $h(x)$, each of degree $n$, such that $g(x) + h(x) = f(x)$.

To prove Theorem 5, Hayes used the following [6, Lemma]: if $p$ and $q$ are distinct odd primes, then there exist integers $c$ and $d$ such that $pc + qd = 1$, $p \nmid c$, and $q \nmid d$. Also, Hayes pointed out that more general theorem whenever $R$ is a principal ideal domain with infinitely many maximal ideals. In [7], P. Pollack showed the case that $R$ is a Noetherian domain with infinitely many maximal ideals: Suppose that $R$ is an integral domain which is Noetherian and has infinitely many maximal ideals. Then every element of $R[x]$ of degree $n \geq 1$ can be written as the sum of two irreducibles of degree $n$. He used distinct maximal ideals $P$ and $Q$ such that (1) $P^2 \neq P$ and $Q^2 \neq Q$, (2) $|R/P|, |R/Q| > 2$ [7, Theorem 5]. Noetherian condition guarantees that $I_2 = \{I \mid I$ is an ideal of $R$ and $|R/I| = 2\}$ is finite by Corollary 4, and if $M$ is maximal, then $M^2 \neq M$ [7, Lemma 6]. Also, in [8], F. Saidak gives a short proof of Hayes’s result.

In order to prove Theorem 5, we recall the remarkable criterion of Eisenstein [2].

**Lemma 6.** (Eisenstein’s criterion) If, in the integral polynomial $a_0x^n + a_1x^{n-1} + \cdots + a_n$, all of the coefficients except $a_0$ are divisible by a prime $p$, but $a_n$ is not divisible by $p^2$, then the polynomial is irreducible.

**Proof of Theorem 5.** Write $f(x) = m_0x^n + m_1x^{n-1} + \cdots + m_n$. Choose distinct odd primes $p$ and $q$ which do not divide either of $m_0$ and $m_n$. Let $R = \mathbb{Z}$, $pR = P$, and $qR = Q$. Since $P$ and $Q$ are comaximal, $P^2$ and $Q^2$ are also comaximal. Therefore the two maps $R \to R/P \times R/Q$, $r \mapsto (r + P, r + Q)$ and $R \to R/P^2 \times R/Q^2$, $r \mapsto (r + P^2, r + Q^2)$ are surjective homomorphisms by Lemma 2. Choose $\alpha \notin P$ and $\beta \notin Q$. Let $a_0$ be a preimage of $(\alpha + P, m_0 - \beta + Q)$.
Remarks on a Goldbach property

under \( R \to R/P \times R/Q \). Set \( b_0 = m_0 - a_0 \). Then \( a_0 \notin P \) and \( b_0 \notin Q \). Also, for \( i \) (\( 0 < i < n \)), let \( a_i \) be a preimage of \((0 + P, m_i + Q)\) under \( R \to R/P \times R/Q \). Set \( b_i = m_i - a_i \). Then \( a_i \in P \) and \( b_i \in Q \). Finally, let \( a_n \) be a preimage of \((p+P^2, m_n - q+Q^2)\) under \( R \to R/P^2 \times R/Q^2 \). Set \( b_n = m_n - a_n \). Then we have \( a_n \in P, a_n \notin P^2, b_n \in Q, \) and \( b_n \notin Q^2 \). If \( g(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n \) and if \( h(x) = b_0 x^n + b_1 x^{n-1} + \cdots + b_n \), then \( f(x) = g(x) + h(x) \). Lemma 6 says that \( g(x) \) and \( h(x) \) are irreducible polynomials.

**Remark 7.** (cf. [6, Theorem 1]) As the same notation above, Hayes choose \( a_n' \) and \( b_n' \) such that \( pa_n' + qb_n' = m_n \), but \( p \nmid a_n' \) and \( q \nmid b_n' \) by [6, Lemma]. Set \( a_n = pa_n' \) and \( b_n = qb_n' \). Then \( m_n = a_n + b_n \), \( p|a_n, p^2 \nmid a_n, q|b_n, \) and \( q^2 \nmid b_n \).

Acknowledgement. We would like to thank referee for several useful suggestions.

**References**


Department of Mathematics
Inha University
Incheon 402-751 Korea
E-mail: jangsj@inha.edu