Hacettepe Journal of
Mathematics & Statistics

Hacet. J. Math. Stat.
Volume 49 (6) (2020), 2071 – 2073
DOI : 10.15672/hujms.649706

Research Article

Rings with few units and the infinitude of primes

Hikmet Burak Özcan[1], Sedef Taşkın*[2]

[1] *Department of Mathematics, Faculty of Sciences, İzmir Institute of Technology, 35430, Urla/İzmir, Turkey*

[2] *Department of Mathematics, Faculty of Sciences, Dokuz Eylül University, Tınaztepe Campus, 35390, Buca/İzmir, Turkey*

Abstract

In this short note, our aim is to provide novel proofs for the infinitude of primes in an algebraic way. It's thought that the first proof for the infinitude of primes was given by the Ancient Greek mathematician Euclid. To date, most of the proofs have been based on the fact that every positive integer greater than 1 can be written as a product of prime numbers. However, first we are going to prove a ring theoretic fact that if R is an infinite commutative ring with unity and the cardinality of the set of invertible elements is strictly less than the cardinality of the ring, then there are infinitely many maximal ideals. This fact leads to an elegant proof for the infinitude of primes. In addition, under the same cardinality assumption, we consider the special case in which R is a unique factorization domain (for short UFD) and establish another ring theoretic result. Thanks to it, we give a second proof of the infinitude of primes.

Mathematics Subject Classification (2010). 16N20, 11A41, 03E10

Keywords. prime numbers, cardinality, Jacobson radical

1. Preliminaries

Throughout this note, all our rings are infinite commutative with unity. Unless otherwise stated, R denotes an infinite commutative ring with unity and the set of invertible elements of R will be denoted by $R^\times$. The **Jacobson radical** of a ring R, denoted by J, is defined to be the intersection of all the maximal ideals of R. The following lemma is well-known and characterizes the elements of the Jacobson radical J in terms of invertible elements of R.

Lemma 1.1. [1] *Let $x \in R$. Then $x \in J$ if and only if $1 - xy \in R^\times$ for all $y \in R$. In particular, $1 - x \in R^\times$ whenever $x \in J$.*

By Lemma 1.1, we see that the cardinality of the Jacobson radical can not exceed the cardinality of the set of invertible elements of the ring.

*Corresponding Author.

Email addresses: hikmetozcan@iyte.edu.tr (H.B. Özcan), sedef.taskin@deu.edu.tr (S. Taşkın)

Received: 21.11.2019; Accepted: 02.04.2020

2. Main theorems

In this section, our focus will be on the rings whose cardinality is *strictly greater* than the cardinality of the set of its invertible elements, that is $|R^\times| < |R|$. We will prove our results for such rings. Then, as a corollary, we will obtain the infinitude of primes. First, we prove our result for integral domains as the proof is easier. Then, we will generalize our result to arbitrary commutative rings.

Proposition 2.1. *If $|R^\times| < |R|$ and R is an integral domain, then there are infinitely many maximal ideals.*

Proof. Suppose that R is an integral domain with $|R^\times| < |R|$ and there are finitely many maximal ideals, and

$$M_1, \cdots, M_k$$

are all maximal ideals in R. Since R is an integral domain, all the non-zero ideals of R have the same cardinality as R. If one of the maximal ideals $M_1, \cdots, M_k$ of R is zero, then $k = 1$ and R is an infinite field, so $|R^\times| = |R|$, a contradiction. Therefore, all the maximal ideals of R are non-zero. Hence, they have the same cardinality as R. Let us fix non-zero elements x_i from each maximal ideal M_i. Then, we have that

$$x_1 \cdots x_k \in J.$$

Thus $J \neq \{0\}$, and hence J has the same cardinality as R. This is a contradiction because $|R| = |J| \leq |R^\times| < |R|$. □

Indeed, the above proposition holds for any infinite commutative ring.

Theorem 2.2. *If $|R^\times| < |R|$, then there are infinitely many maximal ideals.*

Proof. Suppose that there are finitely many maximal ideals, say $M_1, M_2, ..., M_k$. Consider the canonical epimorphism

$$\phi : R \longrightarrow \bigoplus_{i=1}^{k} R/M_i$$

defined by $\phi(r) = (r + M_1, \cdots, r + M_k)$. It is easy to see that $ker(\phi) = J$. By the first isomorphism theorem,

$$R/J \cong \bigoplus_{i=1}^{k} R/M_i.$$

Note that each quotient R/M_i is a field. Denote it by F_i. By Lemma 1.1, we have that $|J| \leq |R^\times|$ which implies that $|R/J| = |R|$. Therefore, $|F_i| = |R|$ for some field F_i. Assume without loss of generality that $|F_1| = |R|$. We observe that $(x, 1, \cdots, 1)$ is an invertible element in R/J for all non-zero $x \in F_1$. Since $|F_1| = |R|$, we have $|(R/J)^\times| = |R|$. Now, let's take $\bar{x} \in (R/J)^\times$. Then, there exists $\bar{y}$ such that $\overline{xy} = \bar{1}$ which means that $1 - xy \in J$. By Lemma 1.1, we have $xy \in R^\times$. Then there exists $z \in R$ such that $(xy)z = 1$ implying that $x \in R^\times$. Thus, the cardinality of invertible elements in R/J can not exceed the number of invertible elements in R. But we obtained above that $|(R/J)^\times| = |R|$. It is a contradiction. □

Corollary 2.3. *There are infinitely many primes in $\mathbb{Z}$.*

Proof. Since $\mathbb{Z}^\times = \{-1, +1\}$ and $\mathbb{Z}$ is infinite, there are infinitely many maximal ideals. In particular, there are infinitely many prime ideals. This implies the infinitude of primes. □

Finally, assuming the cardinality condition we will move on the case in which R is a UFD. The unique factorization of elements will play a crucial role. The following theorem immediately implies the infinitude of primes.

Theorem 2.4. *If $|R^\times| < |R|$ and R is a UFD, then there are infinitely many prime elements in R. In particular, there are infinitely many primes in $\mathbb{Z}$.*

Proof. Suppose that there are finitely many prime elements in R and $p_1, \cdots, p_k$ are all the prime elements in R. Then there are countably many elements which is of the form

$$p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k},$$

where $r_i \in \mathbb{N}$ for every i. If $|R^\times|$ is not finite, then $R^\times$ is at least countable. But this implies that R is countable and $|R| = |R^\times|$ which contradicts our assumption. Thus, R is countable and $R^\times$ is finite. Note that the product

$$p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$$

belongs to J for every $r_i \in \mathbb{N}$, because all maximal ideals contain at least one prime element. To see this, consider any maximal ideal M and take any $m \in M$. Then, we have that

$$m = u p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k},$$

where u is a unit and $r_i \in \mathbb{N}$ for every i. Since M is a maximal ideal, it is a prime ideal. Thus, either u or $p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ belongs to M. However, u is a unit and so we obtain that

$$p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k} \in M.$$

Assume, without loss of generality, that $r_1 > 0$. Then, either p_1 or $p_1^{r_1-1} p_2^{r_2} \cdots p_k^{r_k}$ belongs to M. If $p_1 \in M$, then we are done. Otherwise, we have that

$$p_1^{r_1-1} p_2^{r_2} \cdots p_k^{r_k} \in M.$$

Repeating this process, we eventually obtain that M contains at least one prime element. Now, let us take a product $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \in J$. Then,

$$1 - p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \in R^\times$$

for any $\alpha_i \in \mathbb{N}$ by Lemma 1.1. Moreover, for every $\alpha_i, \beta_i \in \mathbb{N}$ with $\alpha_i \neq \beta_i$, we have that

$$1 - p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \neq 1 - p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}.$$

Thus, we can find countably many elements in $R^\times$, which is a contradiction. As $\mathbb{Z}$ is a UFD and ±1 are the only units, $\mathbb{Z}$ contains infinitely many primes. □

Acknowledgment. We thank Dr. Haydar Göral for encouraging us to think about this problem.

References

[1] T.Y. Lam, *A First Course in Noncommutative Rings*, Springer, 1999.