WHEN DOES A QUOTIENT RING OF A PID HAVE THE CANCELLATION PROPERTY?

Gyu Whan Chang and Jun Seok Oh

Received: 16 May 2021; Revised: 12 December 2021; Accepted: 10 February 2022

Communicated by Pace Nielsen

Abstract. An ideal $I$ of a commutative ring is called a cancellation ideal if $IB = IC$ implies $B = C$ for all ideals $B$ and $C$. Let $D$ be a principal ideal domain (PID), $a, b \in D$ be nonzero elements with $a \nmid b$, $(a, b)D = dD$ for some $d \in D$, $D_a = D/aD$ be the quotient ring of $D$ modulo $aD$, and $bD_a = (a, b)D/aD$; so $bD_a$ is a nonzero commutative ring. In this paper, we show that the following three properties are equivalent: (i) $d$ is a prime element and $a \nmid d^2$, (ii) every nonzero ideal of $bD_a$ is a cancellation ideal, and (iii) $bD_a$ is a field.

Mathematics Subject Classification (2020): 13A15

Keywords: Principal ideal domain, cancellation ideal

1. Introduction

Let $S$ be a commutative semigroup under multiplication. The zero element of $S$ (if it exists) is an element $0 \in S$ such that $a \cdot 0 = 0 \cdot a = 0$ for all $a \in S$. An element $a \in S$ is said to be cancellative if $ab = ac$ implies $b = c$ for all $b, c \in S$. Clearly if $S$ has an identity, then every invertible element of $S$ is cancellative, so the cancellation property is a natural generalization of invertibility. We say that $S$ is cancellative if every nonzero element of $S$ is cancellative. Let $S^* = S \setminus \{0\}$. Then $S^*$ is not a semigroup in general, while $S$ is cancellative if and only if $S^*$ is a cancellative semigroup. The cancellation property plays an important role for the study on algebra. For example, assume that $S^*$ is a semigroup. Then (i) $S$ is cancellative if and only if $S^*$ can be embedded in a group (i.e., $S^*$ has a quotient group) \cite{5} Theorem 1.2], (ii) $S$ is torsion-free and cancellative if and only if $S^*$ admits a total order compatible with its semigroup operation \cite{5} Corollary 3.4], and (iii) several kinds of factorization properties of a semigroup (e.g., atomic, factorial, half-factorial, bounded factorization) have been studied under the assumption that it is cancellative (see \cite{3} for a survey).

This work was supported by the Incheon National University Research Grant in 2021.
Let $R$ be a commutative ring (not necessarily having an identity), $\mathcal{I}(R)$ be the set of ideals of $R$, and $\mathcal{P}(R)$ be the set of principal ideals of $R$. Then $\mathcal{I}(R)$ becomes a commutative semigroup with zero element under the usual ideal multiplication, $\mathcal{P}(R)$ is a subsemigroup of $\mathcal{I}(R)$, and if $R$ has an identity, then $\mathcal{I}(R)$ has an identity. We say that an ideal $I$ of $R$ is a cancellation ideal if $I$ is cancellative as an element of $\mathcal{I}(R)$. It is easy to see that a principal ideal $(a)$ of $R$ generated by $a \in R$ is a cancellation ideal if and only if $a$ is a regular element of $R$ (i.e., $a$ is not a zero-divisor). Furthermore, if $R$ has an identity distinct from the zero element, then a nonzero ideal $I$ of $R$ is a cancellation ideal if and only if $IR_M$ is a regular principal ideal for all maximal ideals $M$ of $R$ [1, Theorem, p. 2853], and $P(R)$ is cancellative if and only if $R$ is an integral domain, if and only if $I(R)$ is cancellative ideal if and only if $R$ is a Prüfer domain, (i.e., every nonzero finitely generated ideal of $R$ is a cancellation ideal if and only if $R$ is a Prüfer domain, (i.e., every nonzero finitely generated ideal of $R$ is invertible) [4] Theorem 24.3].

Now let $\mathbb{Z}$ be the ring of integers, $m$ and $n$ be positive integers, $\gcd(m, n)$ denote the greatest common divisor of $m$ and $n$, $\mathbb{Z}_n$ be the ring of integers modulo $n$, and $m\mathbb{Z}_n$ be the ideal of $\mathbb{Z}_n$ generated by $m$; so $m\mathbb{Z}_n$ is a commutative ring. Then $\mathcal{I}(\mathbb{Z}_n) = \mathcal{P}(\mathbb{Z}_n)$, and hence $\mathcal{I}(\mathbb{Z}_n)$ is cancellative if and only if $\mathbb{Z}_n$ is an integral domain, if and only if $n$ is a prime number. Moreover, in [2] Theorem 2.5], the authors showed that if $n \nmid m$, then every nonzero ideal in $m\mathbb{Z}_n$ is a cancellation ideal, i.e., $\mathcal{I}(m\mathbb{Z}_n)$ is a cancellative semigroup, if and only if $n \nmid \gcd(n, m)^2$, which motivated the main result of this paper.

Let $D$ be a PID, $a$ and $b$ be nonzero elements of $D$, and $d \in D$ be such that $(a, b)D = dD$. We define $D_a$ to be the quotient ring $D/aD$, $d = \gcd(a, b)$, and $bD_a = (a, b)D/aD$. Then $bD_a$ is a commutative ring, $d$ is determined only up to units, and since $\gcd(a, b) = d$, we have that $\gcd(a/d, b/d) = 1$ and $bD_a = dD_a$. In this paper, we show that every nonzero ideal of $bD_a$ is a cancellation ideal if and only if $\frac{a}{\gcd(a, b)}$ is a prime element and $a \nmid \gcd(a, b)^2$. This result is applied in two special cases, i.e., the ring of integers and the polynomial ring over a field. The former case was provided previously in [2] Theorem 2.5]; our work can be viewed as a direct generalization of the results of that paper, passing from $\mathbb{Z}$ to arbitrary PIDs.
2. Results

Let \( R \) be a commutative ring with identity. Then two ideals \( I, J \) of \( R \) are said to be \textit{comaximal} if \( I + J = R \), and we say that two elements \( a, b \) of \( R \) are \textit{comaximal} if the principal ideals \( aR \) and \( bR \) are comaximal. Clearly, \( a, b \) are comaximal if and only if \( ar + bs = 1 \) for some \( r, s \in R \).

**Lemma 2.1.** Let \( D \) be a PID and \( a, b \in D \) be nonzero elements. Then \( bD_a \) has an identity if and only if \( b \) and \( \frac{a}{\gcd(a, b)} \) are comaximal.

**Proof.** Let \( d = \gcd(a, b) \), \( a_1 = \frac{a}{d} \), and \( b_1 = \frac{b}{d} \).

\((\Rightarrow)\) Let \( bx + aD \) be the identity of \( bD_a \) for some \( x \in D \). Then

\[
(bx + aD)(b + aD) = b + aD,
\]

whence \( a \mid b(bx - 1) \). Also, \( \gcd(a_1, b_1) = 1 \) implies \( a_1 | bx - 1 \), and hence \( bx + a_1y = 1 \) for some \( y \in D \). Thus, \( b \) and \( a_1 \) are comaximal.

\((\Leftarrow)\) By assumption, \( bx + a_1y = 1 \) for some \( x, y \in D \), and hence \( bx = 1 - a_1y \).

So, for every \( z \in D \), we have

\[
(bx + aD)(bz + aD) = (1 - a_1y)(bz) + aD = (bz - a_1byz) + aD = (bz + aD) - (ab_1yz + aD) = bz + aD.
\]

Thus, \( bx + aD \) is the identity of \( bD_a \). \(\Box\)

We now give the main result of this paper.

**Theorem 2.2.** Let \( D \) be a PID and \( a, b \in D \) be nonzero elements with \( a \nmid b \). Then the following statements are equivalent:

1. \( \frac{a}{\gcd(a, b)} \) is a prime element and \( a \nmid \gcd(a, b)^2 \).
2. \( bD_a \) is a field.
3. Every nonzero ideal of \( bD_a \) is a cancellation ideal.

**Proof.** Let \( d = \gcd(a, b) \), \( a_1 = \frac{a}{d} \), and \( b_1 = \frac{b}{d} \). Clearly, \( bD_a = dD_a \), \( (a_1, b_1)D = D \), \( a_1 \) is a nonunit, and \( bD_a \neq (0) \) because \( a \nmid b \).

\((1) \Rightarrow (2)\) Note that \( bD_a \) is a commutative ring; so \( bD_a \) is a field if and only if \( bD_a \) has an identity and \( bD_a \) does not have a proper nonzero ideal.

We first show that \( bD_a \) has an identity. Note that \( a = da_1 \) and \( b = db_1 \); so \( a \nmid d^2 \) implies \( a_1 \nmid d \). Hence, \( a_1 \nmid b \) because \( \gcd(a_1, b_1) = 1 \) and \( b = db_1 \). Since \( a_1 = \frac{a}{d} \) is a prime element by assumption, it follows that \( a_1 \) and \( b \) are comaximal.

Hence, by Lemma 2.1, \( bD_a \) has an identity. Next, let \( A \) be an ideal of \( bD_a \). Then
\[ D_a A = D_a(bD_a A) = bD_a A = A \] because \( bD_a \) has an identity. Thus, \( A \) is an ideal of \( D_a \), so there exists \( e \in D \) such that
\[ a D \subseteq e D \subseteq d D \quad \text{and} \quad A = e D / a D \subseteq b D. \]

Hence, \( e = dx \) and \( a = ey \) for some \( x, y \in D \), and thus \( a = dxy \) or \( a_1 = xy \). By assumption, \( a_1 \) is a prime element of \( D \), whence either \( x \) or \( y \) is a unit of \( D \). If \( x \) is a unit, then \( e D = d D \), and hence \( A = e D / a D = d D = b D_a \). If \( y \) is a unit, then \( e D = a D \), whence \( A = e D / a D = a D / a D \) is the zero ideal of \( b D_a \). Therefore, \( b D_a \) does not have a proper nonzero ideal.

(2) \( \Rightarrow \) (3) Clear.

(3) \( \Rightarrow \) (1) If \( a \mid d^2 \), then \( (d D_a)^2 = d^2 D_a = (0) \), and since \( d D_a \) is a cancellation ideal in \( b D_a \), \( d D_a = (0) \), a contradiction. Thus, \( a \nmid d^2 \).

Next, assume to the contrary that \( a_1 = pq \) for some nonunit elements \( p, q \) of \( D \). Let \( I = pdD_a \) and \( J = qdD_a \). Then \( I \) and \( J \) are ideals of \( d D_a \). If \( I = (0) \), then \( pd + a D = a D \), and hence \( a \mid pd \). Note that \( a = a_1 d \); so \( a_1 \mid p \), and thus \( q \) is a unit, a contradiction. Similarly, we have \( J \neq (0) \). However,
\[ IJ = pdqdD_a = a_1 d^2 D_a = adD_a = (0). \]

Thus, \( I \) and \( J \) are not cancellation ideals, a contradiction. \( \square \)

As a corollary of Theorem 2.2, we have the following result.

**Corollary 2.3.** Let \( D \) be a PID and \( a \in D \) be a nonzero element. Then every nonzero ideal in \( D_a \) is a cancellation ideal if and only if \( a \) is a prime element.

We have two applications of Theorem 2.2: one is to the ring of integers and the other is to the polynomial ring over a field.

**Corollary 2.4.** Let \( n, m \in \mathbb{Z} \) be positive integers with \( n \nmid m \).

1. ([2] Theorem 2.5) Every nonzero ideal in \( m\mathbb{Z}_n \) is a cancellation ideal if and only if \( \frac{n}{\gcd(n,m)} \) is a prime number and \( n \nmid \gcd(n,m)^2 \).
2. ([2] Corollary 2.6) Every nonzero ideal in \( \mathbb{Z}_n \) is a cancellation ideal if and only if \( n \) is a prime number.

**Corollary 2.5.** Let \( F \) be a field, \( X \) be an indeterminate over \( F \), \( F[X] \) be the polynomial ring over \( F \), \( f, g \in F[X] \) be nonzero polynomials with \( f \nmid g \) in \( F[X] \), and \( (f, g)F[X] = hF[X] \) for some \( h \in F[X] \).

1. Every nonzero ideal in \( (f, g)F[X] / f F[X] \) is a cancellation ideal if and only if \( \frac{f}{h} \) is irreducible over \( F \) and \( f \nmid h^2 \) in \( F[X] \).
(2) Every nonzero ideal in \( F[X]/fF[X] \) is a cancellation ideal if and only if \( f \) is irreducible over \( F \).

**Proof.** This follows directly from Theorem 2.2 and Corollary 2.3 because an irreducible polynomial of \( F[X] \) is a prime element. \( \Box \)

**Acknowledgement.** The authors would like to thank the anonymous referee for his/her suggestions and comments.

**References**


**Gyu Whan Chang**  
Department of Mathematics Education  
Incheon National University  
22012 Incheon, Republic of Korea  
e-mail: whan@inu.ac.kr

**Jun Seok Oh** (Corresponding Author)  
Department of Mathematics Education  
Jeju National University  
63243 Jeju, Republic of Korea  
e-mail: junseok.oh@jejunu.ac.kr