THE CANCELLATION LAW FOR IDEALS IN A COMMUTATIVE RING

ROBERT W. GILMER, JR.

1. Introduction. We say that the *restricted cancellation law* for ideals (RCL) holds in the commutative ring R if from the equation $AB = AC$, where A, B, and C are ideals of R and $AB \neq (0)$, it follows that $B = C$. RCL is a weakened form of the *cancellation law* for ideals (CL): If A, B, and C are ideals of R such that $AB = AC$ and $A \neq (0)$, then $B = C$. A ring in which CL holds is an integral domain and in an integral domain, RCL is equivalent to CL.

Various forms of the cancellation law have been considered in the literature, especially by Krull (**3**, pp. 126–9; **4**) and Prüfer (**7**). This paper was originally purposed to determine whether an integral domain with unit in which CL holds is a Dedekind domain. This question is answered in the negative. We show that if RCL holds in the commutative ring R with unit, then either R is an integral domain, R is a special primary ring, or R is a primary ring in which the product of any two non-units is zero. Conversely, RCL holds in a ring of either of these latter two types. CL holds in the integral domain J with unit if and only if the quotient ring J_P of J with respect to any proper prime ideal P of J is a rank-one discrete valuation ring. The consequences of the validity of CL in an integral domain without unit are also considered.

Finally, we consider rings S for which there exists a collection $\mathfrak{S}$ of non-zero proper ideals of S such that every non-zero proper ideal of S is uniquely representable as a finite product of elements of $\mathfrak{S}$. In such an S, RCL holds. If S contains a unit and is not an integral domain, the converse is also true. Perhaps Theorem 8 is the most interesting result of the paper. It states that if S is an integral domain with unit, then S is Dedekind and $\mathfrak{S}$ is the collection of non-zero proper prime ideals of S.

2. The restricted cancellation law in a commutative ring with unit. Throughout this section R will denote a commutative ring with unit in which RCL holds and J will denote an integral domain with unit. We shall investigate the structure of R. The case when $R = J$ will be of special interest.

LEMMA 1. CL *holds in R if and only if R is an integral domain.*

LEMMA 2. *If A, B, and C are ideals of R such that $AB \subseteq AC \neq (0)$, then $B \subseteq C$.*

Proof. We have $AC = AC + AB = A(C + B) \neq (0)$ so that $C = C + B$ and $B \subseteq C$.

Received February 11, 1964.

https://doi.org/10.4153/CJM-1965-028-3 Published online by Cambridge University Press

THEOREM 1. *Either R is a one-dimensional integral domain, R is a special primary ring, or R is a primary ring with maximal ideal M in which $M^2 = (0)$. Conversely, if S is a special primary ring and T is a primary ring with maximal ideal M such that $M^2 = (0)$, then* RCL *holds in S and in T.*

Proof. We suppose P is a proper prime ideal of R and that $x \in R - P$. Then

$$[P + (x)]^4 = P^4 + P^3(x) + P^2(x^2) + P(x^3) + (x^4) = [P + (x)]^2[P^2 + (x^2)].$$

Because $x^4 \notin P$, $[P + (x)]^4 \neq (0)$ so that $[P + (x)]^2 = P^2 + (x^2)$, and hence $(x)P \subseteq P^2 + (x^2)$. Then if $p \in P$, there exist $q \in P^2$ and $r \in R$ such that $rx^2 = px - q \in P$ so that $r \in P$ and

$$(x)P \subseteq P^2 + P(x^2) = P[P + (x^2)].$$

There now arise two cases to consider:

Case I. For P a proper prime ideal of R and for $x \in R - P$,

$$P[P + (x^2)] \neq (0).$$

Case II. There exists a proper prime ideal P of R and an element $x \in R - P$ such that

$$P[P + (x^2)] = (0).$$

In the first case we may conclude that $(x) \subseteq P + (x^2)$, which will imply that P is maximal, and in the second case, there exists a prime ideal P of R such that $P^2 = (0)$. We now consider these two cases.

Resolution of Case I. In Case I, R is not an integral domain, since (0) is not a prime ideal. Further, if M is a proper prime ideal and $x \in R - M$, then $(x) \subseteq M + (x^2)$ so that $x - rx^2 = x(1 - rx) \in M$ for some $r \in R$. Hence $1 - rx \in M$ and thus $M + (x) = R$ so that M is maximal. Because M is an arbitrary proper prime ideal of R, M is also minimal. If then $m \in M$, then for some integer k and some element $t \in R - M$, $m^k t = 0$. Consequently $(m^{2k}) = (m^k)(m^k, t)$. Because $t \notin M$, $(m^k) \neq (m^k, t)$ so that $(m^{2k}) = (0)$, every element of M is nilpotent, and R is a primary ring with maximal ideal M.

If $M^2 = (0)$, the conclusion to our theorem holds. If $M^2 \neq (0)$, then $M \supset M^2 \supset M^3$. If A is the ideal generated by $M - M^2$, then $M = M^2 + A$ so that

$$M^2 = M^4 + M^2A + A^2 \subseteq M^3 + A^2.$$

Because $M^2 \supset M^3$, $A^2 \neq (0)$. Thus there exist $x, y \in M - M^2$ such that $xy \neq 0$. Now if $x^k = 0$, then

$$[M^2 + (x)]^k = \sum_{i=0}^{k} M^{2i}(x)^{k-i} = \sum_{i=1}^{k} M^{2i}(x)^{k-i} = M \sum_{j=0}^{k-1} M^{2j}(x)^{k-1-i}$$
$$= M^2[M^2 + (x)]^{k-1}.$$

https://doi.org/10.4153/CJM-1965-028-3 Published online by Cambridge University Press

But $M^2 \neq M^2 + (x)$ so that $[M^2 + (x)]^k = (0)$. This implies that $M^{2k} = (0) \subseteq (x)$. By induction, we shall show that $M \subseteq (x)$, and hence that $M = (x)$. Knowing this, it is easy to see that $(x), (x^2), \ldots, (x^k) = (0)$ are all the proper ideals of R, so that R is indeed a special primary ring. To this end, we suppose that $M^i \subseteq (x)$, where $i \geqslant 2$. Then for some ideal A of R, $M^i = A(x)$. Because $x \notin M^i$, $A \subset R$ so that $A \subseteq M$. Hence $M^i \subseteq M(x)$ and $M(x) \neq (0)$ by choice of x. By Lemma 2, $M^{i-1} \subseteq (x)$. This shows that Theorem 1 holds ir Case I.

Resolution of Case II. In this case, there exists a proper prime ideal P such that $P^2 = (0)$, so that P is the unique minimal prime ideal of R. If P is maximal, then R is a primary ring, P is its maximal ideal, and $P^2 = (0)$.

If P is non-maximal and M is a proper prime ideal distinct from P, then $M \supset P$. Thus if $t \in R - M$, $M[M + (t)] \neq (0)$ and as in Case I, M is maximal. If b is a non-unit of R, then for some maximal ideal N of R, $b \in N \supset P$. Thus $P + (b) \subseteq N$ and by the proof of Case I we must have $(b)P = P^2 + P(b^2) = (0)$. In particular if $b \notin P$, then $(b^2) = (b)[(b) + P]$ and $(b) = (b) + P$, that is, $P \subseteq (b)$. It follows that for some ideal C of R, $P = (b)C$. Because P is prime, $P = C$ and $P = (b)P = (0)$. Therefore R is a one-dimensional integral domain.

It is well known that RCL holds in S. RCL holds in T since for ideals A, B, and C of T the only way in which we can have $AB = AC \neq (0)$ is to have $A = R$, in which case $B = AB = AC = C$, or to have $B = C = R$.

We next seek to determine necessary and sufficient conditions on J in order that CL hold in J. In particular, we shall show that J need not be Dedekind in order that CL hold in J.

We first introduce some terminology.

J will be called a *Prüfer domain* if every finitely generated ideal of J is invertible. Krull has shown (**4**, p. 554) that J is Prüfer if and only if J_P is a valuation ring for each proper prime ideal P of J. Krull has also shown (**3**, p. 127) that J is Prüfer if and only if J is integrally closed and the *finite cancellation law* (FCL) holds in J: If A, B, C are ideals of J such that $AB = AC$ and if A is finitely generated and non-zero, then $B = C$.

J is said to be *almost Dedekind* if J_P is a rank-one discrete valuation ring for each proper prime ideal P of J (**2**; **8**, p. 278).

THEOREM 2. *If* FCL *holds in J, J is integrally closed.*

Remark. This result was communicated to the author by H. S. Butts.

Proof. Suppose ξ is an element of the quotient field K of J which is integral over J. Then the fractional ideal F of J generated by 1 and all positive powers of ξ is finitely generated and idempotent. For some non-zero element d of J, $dF = A$ is a finitely generated ideal of J. Further,

$$A^2 = (d^2)F^2 = (d^2)F = (d)A$$

https://doi.org/10.4153/CJM-1965-028-3 Published online by Cambridge University Press

so that $(d) = A$ since FCL holds in J. This implies, however, that $F = J$ so that $\xi \in J$ and J is integrally closed.

In view of the two results of Krull cited earlier and Theorem 2, we obtain

COROLLARY 1. *These are equivalent:*
(A) *J is a Prüfer domain,*
(B) *J_P is a valuation ring for each proper prime ideal P of J,*
(C) FCL *holds in J.*

THEOREM 3. CL *holds in J if and only if J is almost Dedekind.*

Proof. We first suppose that CL holds in J. If P is a proper prime ideal of J, J_P is a valuation ring by Corollary 1. By Theorem 1, J_P has rank one. Now $P \subset J$ so that $P^2 \subset JP = P$ since CL holds in J. Because P^2 has radical P, a maximal ideal, P^2 is primary for P. Consequently,

$$P^2J_P = [PJ_P]^2 \subset PJ_P.$$

It is easily shown that if $m \in PJ_P - P^2J_P$, then $PJ_P = (m)$. Therefore J_P is a rank-one discrete valuation ring and J is almost Dedekind.

Conversely, if J is almost Dedekind and $\{M_\lambda\}$ is the collection of maximal ideals of J, then $AB = AC$ implies that

$$(AJ_{M_\lambda})(BJ_{M_\lambda}) = (AJ_{M_\lambda})(CJ_{M_\lambda}) \text{ for each } \lambda.$$

Because CL holds in a Dedekind domain, $BJ_{M_\lambda} = CJ_{M_\lambda}$ for each λ. It follows that

$$B = \bigcap_{\lambda} BJ_{M_\lambda} = \bigcap CJ_{M_\lambda} = C.$$

Therefore CL holds in J.

In a previous paper the author has shown that J is almost Dedekind if and only if J has dimension less than two and primary ideals of J are prime powers **(2)**. Nakano has given in **(5)** an example of an integral domain with unit with these last two properties which is not a Dedekind domain.

3. The cancellation law in integral domains without unit.

An integral domain in which CL holds need not contain a unit, as the domain of even integers illustrates. However, if D is a domain without unit, if e is the identity of the quotient field K of D, and if $D^* = D[e]$, then we have:

THEOREM 4. CL *holds in D if and only if* CL *holds in D^*.*

Proof. Because ideals of D are also ideals of D^*, CL holds in D if it holds in D^*. Conversely, suppose CL holds in D and $A \neq (0)$, B, and C are ideals of D^* such that $AB = AC$. If d is a non-zero element of d, then dD^* is an invertible ideal of D and

$$(AdD^*)(BdD^*) = (AdD^*)(CdD^*)$$

so that $BdD^* = CdD^*$. Since dD^* is invertible, $B = C$, and CL holds in D^*.

https://doi.org/10.4153/CJM-1965-028-3 Published online by Cambridge University Press

THEOREM 5. *If* CL *holds in D, then D is an ideal of finite index in D^* (i.e., D^*/D is a finite ring). Conversely, if J is an integral domain with unit e in which* CL *holds and if A is an ideal of J of finite index in which* CL *holds, then $J = A^* = A[e]$.*

Proof. We have $D^*/D \simeq Z/(s)$ for some integer s. If CL holds in D, CL holds in D^* so that D^* has dimension less than two. It follows that $Z/(s)$ has dimension zero. Consequently, $s > 0$.

We obviously have $A \subseteq A^* \subseteq J$. If CL holds in A, CL holds in A^* so that A^* is integrally closed by Theorem 2. But A has finite index in J so that, if $x \in J$, there exist distinct positive integers k and t such that $x^k - x^t \in A$. Then x is integral over A^* and hence in A^*.

In **(2)**, the author has shown that if the integral domain J with unit is almost Dedekind, if K is the quotient field of J, and if J' is a domain such that $J \subseteq J' \subseteq K$, then J' is almost Dedekind. By use of this result, we can prove one part of Theorem 3 without the assumption that the domain under consideration contains a unit.

THEOREM 6. *If P is a non-zero proper prime ideal of the integral domain D in which* CL *holds, then D_P is a rank-one discrete valuation ring.*

Proof. If e is the identity of the quotient field K of D, then CL holds in $D^* = D[e]$ by Theorem 4. Now $D^* \subseteq D_P \subset K$ so that CL holds in D_P also. By Theorem 3,

$$D_P = (D_P)_{PD_P}$$

is a rank-one discrete valuation ring.

If D is a domain without unit such that D_P is a rank-one discrete valuation for every proper prime ideal P of D, CL need not hold in D. For example, (0) may be the only proper prime ideal of D so that the hypothesis is trivially satisfied **(1)**. Less-trivial examples are provided by the following lemma.

LEMMA 3. *If A is an ideal of the Dedekind domain J, then for each non-zero proper prime ideal P of A, A_P is a rank-one discrete valuation ring.*

Proof. We first note that P is also an ideal of J. This is true because $JP \subseteq JA = A$ so that JP is an ideal of A. Further,

$$(JP)^2 = P(JP) \subseteq PA \subseteq P$$

so that $JP \subseteq P \subseteq JP$. Hence $P = JP$ and is an ideal of J. Because J is Dedekind, $P = AB$ for some ideal B of J. If

$$A = P_1^{e_1} \ldots P_k^{e_k}$$

is a factorization of A into distinct prime ideals of J, we shall show that for an ideal B of J, AB is prime in A only if B is a prime ideal of J distinct from each P_i, $1 \leqslant i \leqslant k$.

https://doi.org/10.4153/CJM-1965-028-3 Published online by Cambridge University Press

First, if B is not prime in J, then $B = CD$ for some ideals C and D of J, both of which properly contain B. Then AC and AD are ideals of A, $(AC)(AD) \subseteq AB$, but neither AC nor AD is contained in AB. Moreover, if $1 \leqslant i \leqslant k$, then $A^2 \subseteq AP_i$ but $A \not\subseteq AP_i$. This proves our earlier claim: if P is a prime ideal of A, then $P = AB$ for some prime ideal B of J such that $B \notin \{P_1, \ldots, P_k\}$. The converse is also true since for any such prime ideal B, $AB = A \cap B$. To complete the proof, it suffices to show that

$$J_B = A_P = A_{A-(A\cap B)} = A_{A-B}.$$

Clearly $A_P \subseteq J_B$. If, however, $x/y \in J_B$ where $y \in J - B$ and if $a \in A - B$, then $x/y = xa/ya$, $xa \in A$, and $ya \in A - B$. Thus $x/y \in A_P$. This completes the proof of the lemma.

If K is a finite field, if X is an indeterminate over K, and if $J = K[X]$, then J is Dedekind. If $A = (X^2)$, A is an ideal of J of finite index and A_P is a rank-one discrete valuation ring for each proper prime ideal P of A. The domain $A^* = A[e]$, where e is the identity of K, is not integrally closed (X is integral over A^*, but not in A^*). Hence CL does not hold in A^*, and therefore not in A.

RCL seems to be a weak condition in rings without unit. For example, RCL holds in any ring R such that $R^2 = (0)$.

4. Rings with unique ideal factorization. As an application of the previous three sections, we consider a commutative ring S with unit in which there exists a collection $\mathfrak{S}$ of non-zero proper ideals such that every non-zero proper ideal of S may be expressed uniquely as a product of elements of $\mathfrak{S}$. It is easy to see that uniqueness of representation implies that RCL holds in S. In view of Theorem 1 we then easily obtain:

THEOREM 7. *If S has proper divisors of zero, then either:*

(1) *S is a special primary ring and $\mathfrak{S}$ contains only the maximal ideal of S, or*

(2) *S is a primary ring with maximal ideal M, $M^2 = (0)$, and $\mathfrak{S}$ is the collection of all non-zero proper ideals of S.*

Of special interest is the following theorem.

THEOREM 8. *If S is an integral domain, then S is Dedekind and $\mathfrak{S}$ is the collection of non-zero proper prime ideals of S.*

Proof. If S is a field, both conclusions follow. If S is not a field, Theorem 1 implies that S is one-dimensional. To show that S is Dedekind, it suffices to show that every proper non-zero prime ideal of S is invertible (**6**). We first show that an invertible ideal S_0 in $\mathfrak{S}$ is prime. Thus if $xy \in S_0$, then $(x)(y) = (xy) = S_0 A$ for some ideal A of S, since S_0 is invertible. From the uniqueness of representation, S_0 must occur as a factor either of (x) or of (y). Hence $x \in S_0$ or $y \in S_0$ and S_0 is prime. Now if p is a non-zero element of P

https://doi.org/10.4153/CJM-1965-028-3 Published online by Cambridge University Press

and if $(p) = S_1 S_2 \dots S_k$ is the factorization of (p) into elements of $\mathfrak{S}$, then each S_i is an invertible element of $\mathfrak{S}$ and therefore maximal. Because $p \in P$, $P = S_i$ for some i. Hence $P \in \mathfrak{S}$ and P is invertible. It follows that S is Dedekind, and consequently every element of $\mathfrak{S}$ is invertible, therefore prime by our previous argument. This completes the proof of the theorem.

References

1. R. W. Gilmer, *Commutative rings containing at most two prime ideals*, Mich. Math. J., *10* (1963), 263–8.
2. ——— *Integral domains which are almost Dedekind*, to appear in Proc. Amer. Math. Soc.
3. W. Krull, *Idealtheorie* (New York, 1948).
4. ——— *Beiträge zur Arithmetik kommutativer Integritätsbereiche*, Math. Z. *41* (1936), 545–69.
5. N. Nakano, *Idealtheorie in einem speziellen unendlichen algebraischen Zahlkörper*, J. Sci. Hiroshima Univ., *16* (1953), 425–39.
6. ——— *Über die Umkehrbarkeit der Ideale im Integritätsbereiche*, Proc. Imperial Acad. Tokyo, *19* (1943), 230–4.
7. H. Prüfer, *Untersuchungen über die Teilbarkeitseigenschaften in Körpern*, J. reine angew. Math. *168* (1932), 1–36.
8. O. Zariski and P. Samuel, *Commutative algebra*, vol. 1 (Princeton, 1958).

Florida State University,
Tallahassee, Florida

https://doi.org/10.4153/CJM-1965-028-3 Published online by Cambridge University Press