

Unique Factorization in Integral Domains

11/14/06 Radford

Throughout R is an integral domain unless otherwise specified. Let A and B be sets. We use the notation $A \subseteq B$ to indicate that A is a subset of B and we use the notation $A \subset B$ to mean that A is a proper subset of B .

The group of elements in R which have a multiplicative inverse (the group of units of R) is denoted R^\times . Since R has no zero divisors cancellation holds.

$$\text{If } a, b, c \in R \text{ and } a \neq 0 \text{ then } ab = ac \text{ implies } b = c. \quad (1)$$

To see this note $ab = ac$ is equivalent to $a(b - c) = 0$ which implies $b - c = 0$ when $a \neq 0$.

For $a \in R$ let

$$(a) = Ra = \{ra \mid r \in R\}$$

be the ideal generated by a . An ideal I of R is *principal* if $I = (a)$ for some $a \in R$.

1 Associates, the Relation Divides, Greatest Common Divisors

Elements $a, b \in R$ are *associates* if $b = ua$ for some $u \in R^\times$. Since R^\times is a group, $a \sim b$ if and only if a and b are associates defines an equivalence relation on R . Note that R^\times acts on R by left multiplication. The equivalence class of $a \in R$ is thus the R^\times -orbit of a .

Lemma 1 *Let $a, b \in R$. Then:*

$$(1) \ (a) = (b) \text{ if and only if } a \text{ and } b \text{ are associates.}$$

- (2) *The product of ideals (a) and (b) and their set product are the same;*
 $(a)(b) = (ab)$.
- (3) $(a)(b) \subseteq (a), (b)$.

PROOF: To show part (1) we may assume $a \neq 0$. Suppose $(a) = (b)$. Since $a \in Ra = Rb$ there is an $r \in R$ such that $a = rb$. Thus since $b \neq 0$ and $(b) = (a)$ there is an $s \in R$ with $b = sa$. Therefore $a = rb = r(sa)$ from which $a1 = a(rs)$ follows. Cancellation (1) gives $1 = rs$ which means $r, s \in R^\times$ since R is commutative. Therefore a, b are associates.

Conversely, suppose that a, b are associates. Then $b = ua$ for some $u \in R^\times$. This means $(b) \subseteq (a)$ since $Rb = Rua \subseteq Ra$. Since b, a are associates $(a) \subseteq (b)$ from which $(a) = (b)$ follows. We have established part (1).

To show part (2) we first note that $RR = R$ since $RR \subseteq R = R1 \subseteq RR$. Thus multiplication of sets yields $(Ra)(Rb) = RaRb = RRab = Rab$ which means the set product of (a) and (b) is (ab) which is an ideal of R . This is enough for part (2). Part (3) follows from part (2) since $Rab \subseteq Rb$ and $Rab = Rba \subseteq Ra$. \square

Suppose $a, b \in R$. Then $b|a$, or b divides a , if $a = bc$ for some $c \in R$. Thus the set of elements which b divides is (b) . The notion of divides can be expressed in terms of set inclusion.

Lemma 2 *Suppose $a, b \in R$. Then the following are equivalent:*

- (1) $b|a$.
- (2) $(a) = (b)(c)$ for some $c \in R$.
- (3) $(a) \subseteq (b)$.

PROOF: Part (1) implies part (2) by part (2) of Lemma 1. Part (2) implies part (3) by part (3) of the same. Part (3) implies part (1) as $a \in (a)$. \square

By virtue of the preceding lemma divides is a reflexive and transitive relation. As a consequence of the lemma and part (1) of Lemma 1, if b divides a then any associate of b divides a and b divides any associate of a . Note that b divides a and a divides b if and only if a and b are associates.

Suppose that $a, b, d \in R$. Then d is a *greatest common divisor* of a and b if d divides a and b , and if $e \in R$ divides a and b then e divides d .

In light of Lemma 2 d divides a, b if and only if $(a), (b) \subseteq (d)$, or equivalently $(a) + (b) \subseteq (d)$. Thus:

Lemma 3 *Let $a, b, d \in R$. Then d is a greatest common divisor of a and b if and only if $(a) + (b) \subseteq (d)$ and whenever $e \in R$ satisfies $(a) + (b) \subseteq (e)$ then $(d) \subseteq (e)$. \square*

Suppose $a, b \in R$ has a greatest common divisor d . By the preceding lemma and part (1) of Lemma 1 the greatest common divisors of a and b are the associates of d .

2 The Monoid of Non-Zero Principal Ideals

Let \mathcal{R} denote the set of *non-zero* principal ideals of R . Since R is an integral domain \mathcal{R} is a monoid under set multiplication with identity element $(1) = R$ by part (b) of Lemma 1.

Lemma 4 *Let $(a), (b), (c) \in \mathcal{R}$. Then:*

- (1) $(a) = R$ if and only if $a \in R^\times$.
- (2) $(a)(b) = (a)(c)$ implies $(b) = (c)$
- (3) $(a) = (a)(b)$ implies $(b) = (1)$.

PROOF: Since $R = (1)$, $(a) = R$ if and only if $a, 1$ are associates by part (1) of Lemma 1. But $a, 1$ are associates if and only if $a = u1 = u$ for some $u \in R^\times$. We have established part (1). To see part (2), we use Lemma 1 to note that $(a)(b) = (a)(c)$ if and only if $(ab) = (ac)$ if and only if $ac = u(ab) = a(ub)$ for some $u \in R^\times$. The latter implies $c = ub$ by cancellation, and thus $(b) = (c)$. Part (3) follows by part (2) since $(a) = (a)(1)$. \square

The appropriate notions of prime ideal in \mathcal{R} and maximal ideal in \mathcal{R} are key to the arithmetic of R . An element $(p) \in \mathcal{R}$ is a \mathcal{R} -*prime ideal* if $(p) \neq (1)$ and whenever $(a), (b) \in \mathcal{R}$ satisfy $(a)(b) \subseteq (p)$ then $(a) \subseteq (p)$ or $(b) \subseteq (p)$. An element $p \in R$ is *prime* if p is a non-zero non-unit and whenever $a, b \in R$ and $p|ab$ then $p|a$ or $p|b$.

Remark 1 $a \in R$ is a non-zero non-unit if and only if $(a) \in \mathcal{R}$ and $(a) \neq R$; see part (1) of Lemma 4.

Lemma 5 Let $p \in R$. Then the following are equivalent:

- (1) (p) is prime ideal of R .
- (2) (p) is a \mathcal{R} -prime ideal.
- (3) p is prime.

PROOF: Part (1) implies part (2) by definition of prime ideal. To show part (2) implies part (3), suppose that (p) is a \mathcal{R} -prime ideal. Then p is a non-zero non-unit Remark 1. Let $a, b \in R$ and suppose $p|ab$. We wish to show $p|a$ or $p|b$. Since $p|0$ we can assume $a, b \neq 0$. Therefore $(a), (b) \in \mathcal{R}$. By part (2) of Lemma 1 and Lemma 2 observe that $(a)(b) \subseteq (p)$. Since (p) is a \mathcal{R} -prime ideal either $(a) \subseteq (p)$ or $(b) \subseteq (p)$. Therefore $p|a$ or $p|b$. We have shown part (2) implies part (3).

To complete the proof we need only show that part (3) implies part (1). Suppose that p is prime. Then $R \neq (p) \in \mathcal{R}$ by Remark 1. Let A, B be ideals of R such that $AB \subseteq (p)$. To show that (p) is a prime ideal of R we need only show that $A \not\subseteq (p)$ implies $B \subseteq (p)$.

Let $a \in A$ and $b \in B$. Then $ab \in (p)$, or equivalently $p|ab$. Since p is prime $p|a$ or $p|b$. Suppose that $A \not\subseteq (p)$. Then $a \notin (p)$ for some $a \in A$. Let $b \in B$. Since $p|a$ is false necessarily $p|b$. Therefore $b \in (p)$. We have shown $B \subseteq (p)$. \square

Remark 2 By the preceding lemma associates of prime elements are prime elements.

An element $(m) \in \mathcal{R}$ is a \mathcal{R} -maximal ideal if $(m) \neq R$ and whenever $(a) \in \mathcal{R}$ and $(m) \subseteq (a)$ then $(m) = (a)$ or $(a) = R$. An element $m \in R$ is *irreducible* if m is a non-zero non-unit and $m = ab$, where $a, b \in R$, implies a or b is a unit.

Lemma 6 Let $m \in R$. Then the following are equivalent:

- (1) (m) is a \mathcal{R} -maximal ideal.

(2) m is irreducible.

PROOF: Suppose that (m) is a \mathcal{R} -maximal ideal. Now m is a non-zero non-unit by Remark 1. Suppose $a, b \in R$ satisfy $m = ab$. Then $(m) = (a)(b) \subseteq (a), (b)$ by parts (2) and (3) of Lemma 1. Since $(m) \in \mathcal{R}$ necessarily $(a), (b) \in \mathcal{R}$. Thus $(m) = (a)$, in which case $(b) = (1)$ and b is a unit by Lemma 4, or $(a) = R$, in which case a is a unit by the part (1) of the same. Therefore part (1) implies part (2).

Suppose that m is irreducible. Then $R \neq (m) \in \mathcal{R}$ by Remark 1. Let $(m) \subseteq (a)$ where $(a) \in \mathcal{R}$. Then $a|m$ which means $ab = m$ for some $b \in R$. Thus a is a unit, in which case $(a) = R$ by part (1) of Lemma 4, or b is a unit, in which case $(m) = (a)$ by part (1) of Lemma 1. We have shown part (2) implies part (1). \square

Remark 3 *By the preceding lemma associates of irreducible elements are irreducible elements.*

Corollary 1 *\mathcal{R} -prime ideals are \mathcal{R} -maximal ideals. Thus prime elements of R are irreducible.*

PROOF: Suppose that (p) is a \mathcal{R} -prime ideal and $(p) \subseteq (a)$, where $(a) \in \mathcal{R}$. Then $(p) = (a)(b)$ for some $b \in R$ by Lemma 2. Thus $(p) \subseteq (a), (b)$ by part (3) of Lemma 1. Since $(a)(b) \subseteq (p)$, either $(a) \subseteq (p)$ in which case $(a) = (p)$ or $(b) \subseteq (p)$ in which case $(b) = (p)$ and thus $(a) = R$ by part (3) of Lemma 4. Therefore (p) is a \mathcal{R} -maximal ideal. Lemmas 5 and 6 complete the proof. \square

3 Euclidean and Principal Ideal Domains

R is a *Euclidean Domain* if there is a function $N : R \rightarrow \mathbf{Z}^{\geq 0}$ such that for all $a, b \in R$, where $b \neq 0$, there are $q, r \in R$ which satisfy

$$a = qb + r, \quad \text{where } r = 0 \text{ or } N(r) < N(b).$$

Proposition 1 *Suppose that R is a Euclidean Domain. Then all ideals of R are principal.*

PROOF: \square

An integral domain whose ideals are principal is a *Principal Ideal Domain*.

Suppose that R is a Principal Ideal Domain. Let $a, b \in R$. Then the ideal $(a) + (b) = (d)$ for some $d \in R$. Therefore d is a greatest common divisor of a and b by Lemma 3. Since $d \in (a) + (b)$ it follows that $d = ra + sb$ for some $r, s \in R$.

By Corollary 1 prime elements of R are irreducible. Conversely, irreducible elements are prime.

To see this, suppose that $m \in R$ is irreducible. Then (m) is a \mathcal{R} -maximal ideal. Since R is a Principal Ideal Domain, \mathcal{R} is the set of all non-zero ideals of R . Therefore (m) is a maximal ideal of R and as such is a prime ideal of R . By Lemma 5 m is a prime element of R .

Principal Ideal Domains belong to the very important class of commutative rings whose ideals are finitely generated.

4 Noetherian Rings

In this section R is a ring. The ring R is *Noetherian* if all ideals of R are finitely generated. R satisfies the *ascending chain condition* if every ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

of R terminates; that is $I_n = I_{n+1} = I_{n+2} = \cdots$ for some $n \geq 1$. The ring R satisfies the *maximum condition on ideals* if any non-empty set \mathcal{I} of ideals of R has a maximal element I ; that is if $J \in \mathcal{I}$ and $I \subseteq J$ then $I = J$.

Theorem 1 *Let R be a commutative ring. Then the following are equivalent:*

- (1) *R satisfies the maximum condition on ideals.*
- (2) *R is Noetherian.*
- (3) *R satisfies the ascending chain condition.*

PROOF: Part (1) implies part (2). Suppose that R satisfies the maximum condition on ideals and let I be an ideal of R . Let \mathcal{I} be the set of all finitely generated ideals which are contained in I . Since $(0) \in \mathcal{I}$, by assumption there is a maximal element $(\{a_1, \dots, a_r\})$ in \mathcal{I} . Let $a \in I$. Then $(\{a_1, \dots, a_r\}) \subseteq$

$(\{a_1, \dots, a_r, a\}) \subseteq I$ means $(\{a_1, \dots, a_r\}) = (\{a_1, \dots, a_r, a\})$. Therefore $a \in (\{a_1, \dots, a_r\})$. We have shown that $I = (\{a_1, \dots, a_r\})$.

Part (2) implies part (3). Suppose that R is Noetherian and let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ be an ascending chain of ideals in R . Then $I = \bigcup_{n=1}^{\infty} I_n$ is an ideal of R . Therefore $I = (\{a_1, \dots, a_r\})$ for some $a_1, \dots, a_r \in I$. It is easy to see that $a_1, \dots, a_r \in I_n$ for some $n \geq 1$. Therefore

$$I = (\{a_1, \dots, a_r\}) \subseteq I_n \subseteq I$$

which implies $I = I_n$. Since $I_n \subseteq I_m \subseteq I$ for all $m \geq n$ it follows that $I_m = I_n$ for all $m \geq n$.

Part (3) implies part (1). Suppose that R satisfies the ascending chain condition on ideals and let \mathcal{I} be a non-empty set of ideals of R . Suppose that \mathcal{I} has no maximal element. Then for every $I \in \mathcal{I}$ there exists a $J \in \mathcal{I}$ such that $I \subset J$. Thus there exists an ascending chain of ideals $I_1 \subset I_2 \subset I_3 \subset \dots$ of ideals in \mathcal{I} . This contradiction shows that \mathcal{I} must have a maximal element after all. \square

5 Unique Factorization Domains

An integral domain R is a *Unique Factorization Domain* if every non-zero non-unit $a \in R$ can be written as $a = m_1 \cdots m_r$ as a product of irreducibles, and if $a = m'_1 \cdots m'_{r'}$ is another such product then $r = r'$, and after possible reordering of factors, m_i and m'_i are associates for all $1 \leq i \leq r$. In light of parts (1) and (2) of Lemma 1, R is a unique factorization domain if and only if every $(a) \in \mathcal{R} \setminus \{(1)\}$ is a product of maximal ideals $(a) = (m_1) \cdots (m_r)$ in \mathcal{R} , and this product is unique up to reordering of factors.

Prime and irreducible are the same in a unique factorization domain.

Lemma 7 *Let R be a Unique Factorization Domain. Then the \mathcal{R} -prime ideals and \mathcal{R} -maximal ideals are the same. Thus the prime and the irreducible elements of R are the same.*

PROOF: \mathcal{R} -prime ideals are \mathcal{R} -maximal ideals by Corollary 1. Suppose that (m) is an \mathcal{R} -maximal ideal and suppose that $(a)(b) \subseteq (m)$, where $(a), (b) \in \mathcal{R}$. We need to show that $(a) \subseteq (m)$ or $(b) \subseteq (m)$. If $(a) = R$ then $(b) \subseteq (m)$ and likewise if $(b) = R$ then $(a) \subseteq (m)$. Thus we may assume $(a), (b) \neq R$.

Now $(m)(c) = (a)(b)$ for some $(c) \in \mathcal{R}$ by Lemma 2. Since $(a), (b) \neq R$ it follows that (a) and (b) can be written as a product of \mathcal{R} -maximal ideals. Since $(c)(m) = (a)(b)$ necessarily (m) must be one of them. Therefore $(a) \subseteq (m)$ or $(b) \subseteq (m)$ by part (3) of Lemma 1. \square

Theorem 2 *Every Principal Ideal Domain is a Unique Factorization Domain.*

PROOF: Let R be a Unique Factorization Domain. We first show that every $(a) \in \mathcal{R}$, $(a) \neq R = (1)$, is a product of \mathcal{R} -maximal ideals. To do this it suffices to show that the set S of all elements of $\mathcal{R} \setminus \{(1)\}$ which are not such a product is empty.

Suppose that $S \neq \emptyset$. Since R is Noetherian S has an element (a) maximal with respect to inclusion. Now (a) is not a \mathcal{R} -maximal ideal. Therefore a is not irreducible by Lemma 6. Note that a is non-zero non-zero divisor. Thus $a = bc$, where b, c are not units. By Lemma 4 we have $(a) = (b)(c) \subseteq (b), (c)$ and $(b), (c) \neq R$. Therefore $(a) \subset (b), (c)$ which means $(b), (c) \notin S$. Hence (b) and (c) are products of \mathcal{R} -maximal ideals whence $(a) = (b)(c)$ is also, a contradiction. This means that S is empty after all.

To show uniqueness, suppose $(a) \in \mathcal{R} \setminus \{(1)\}$ is written as products of \mathcal{R} -maximal ideals.

$$(a) = (m_1) \cdots (m_r) = (m'_1) \cdots (m'_{r'}).$$

Then $(m'_1) \cdots (m'_{r'}) \subseteq (m_r)$ by part (3) of Lemma 1. Since (m_r) is a \mathcal{R} -prime ideal by Lemma 7, $(m'_i) \subseteq (m_r)$ for some $1 \leq i \leq r'$. Since (m_r) and (m'_i) are both \mathcal{R} -maximal ideals it follows that $(m_r) = (m'_i)$. Therefore

$$(m_1) \cdots (\widehat{m_r}) = (m'_1) \cdots (\widehat{m'_i}) \cdots (m'_{r'})$$

by part (2) of Lemma 4, where “hat” means factor omitted. By induction on r we conclude that $r = r'$ and, after reordering if necessary, $(m_1) = (m'_1), \dots, (m_r) = (m'_r)$. \square