FACTORIAL DOMAINS

CLIFFORD S. QUEEN

(Communicated by Wolmer V. Vasconcelos)

Abstract. We give a simple characterization of factorial domains. We also characterize almost factorial domains and Krull domains with finite cyclic class group.

1. Introduction

Let $A$ be an integral domain and $K$ its field of fractions. We say that $A$ is a factorial domain if there exists a subset $P$ of $A$ not containing 0 such that any nonzero $a$ in $A$ can be written uniquely up to order as a product

$$a = u \prod_{p \in P} p^{n(p)}$$

where $u$ is a unit of $A$ and the $n(p)$ are nonnegative integers with $n(p) = 0$ for all but finitely many $p$.

The two most well-known examples of factorial domains are $\mathbb{Z}$, the ring of integers, and $F[X]$, the ring of polynomials in one variable $X$ over a field $F$. Both of these rings are principal ideal domains (PIDs) and all such rings are known to be factorial (see [6]). Let $Q$ denote the field of rational numbers. In 1928 Hasse proved (see [4]) the following result:

**Theorem 1.** $A$ is a PID if and only if there is a map $N : K \rightarrow Q$ satisfying the following properties:

1. $N(x) \geq 0$ for all $x$ in $K$ and $N(x) = 0$ if and only if $x = 0$.
2. $N(xy) = N(x)N(y)$ for all $x$ and $y$ in $K$.
3. $N(a) \in \mathbb{Z}$ for all $a \in A$.
4. For $a$ in $A$, $N(a) = 1$ if and only if $a$ is a unit of $A$.
5. Given an $x$ in $K$ such that $x$ is not in $A$ there exist $a$ and $b$ in $A$ with $0 < N(ax - b) < 1$.

We prove a more general result (Theorem 2) in section 2. However a sketch of the proof of Theorem 1 is as follows: Suppose $A$ is an integral domain and there is a map $N : K \rightarrow Q$ satisfying the above four properties. To show that $A$ is a PID let $\mathcal{I}$ be a nonzero ideal in $A$ and $N(d)$ minimal over all nonzero elements $d$ of $\mathcal{I}$. We claim that $\mathcal{I} = Ad = (d)$, since if $e$ is in $\mathcal{I}$ and $d$ does not divide $e$, then $e/d$ is not in $A$ and so there exist $a, b \in A$ so that $0 < N((e/d)a - b) < 1$. Thus $ea - bd$ is a nonzero element of $\mathcal{I}$ and $N(ea - bd) < N(d)$, which is impossible.

Received by the editors February 18, 1994 and, in revised form, June 4, 1994.

1991 Mathematics Subject Classification. Primary 13M15.

©1996 American Mathematical Society
Next suppose that $A$ is a PID. To construct a map $N : K \rightarrow Q$ satisfying the
four properties of our theorem, let $P$ be a set consisting of one irreducible element
from each associate class of irreducible elements. Then set $N(0) = 0$ and if $a$ is a
nonzero element of $A$ we set $N(a) = 2^{w(a)}$, where $w(a)$ is the number of factors of
elements of $P$ in a factorization of $a$, counting multiplicity. Finally, if $x$ is a nonzero
element of $K$, then there exist $a, b \in A$ such that $ab \neq 0$ and $x = a/b$ and so we
set $N(x) = N(a)/N(b)$. One then completes the proof by showing that $N$ satisfies
properties (1)–(5) above.

Of course a factorial domain need not be a PID. Examples are the ring of polynomials in one variable over a field. We achieve one objective of this paper in section 2 by
proving Theorem 2, which is a characterization of factorial domains that general-
izes Theorem 1. In section 3 we generalize Theorem 1 in yet another direction by characterizing Krull domains with finite cyclic class groups.

2. FACTORIAL DOMAINS

Let $A$ be an integral domain and $K$ its field of fractions. Recall that an ideal of
$A$, usually referred to as a fractional ideal, is an $A$-module in $K$ of the form $xI$,
where $I$ is an $A$-module contained in $A$ and $x$ is in the multiplicative group of $K$,
denoted by $K^*$. A divisorial ideal $A$ is an intersection of principal ideals, i.e. there
is a subset $S$ of $K^*$, such that
$$I = \bigcap_{x \in S} Ax.$$ If $I$ and $J$ are nonzero ideals, then the following are a list of known results whose
proofs can be found in Fossum (see [2]):

1. All divisorial ideals are of the form $(A : I) = \{x \in K | xI \subseteq A\}$.
2. If $I \subseteq J$, then $(A : J) \subseteq (A : I)$.
3. $(A : (A : I))$ is the smallest divisorial ideal containing the ideal $I$.

If $a, b \in A$ and $b \neq 0$, then $b$ divides $a$ (in notation $b|a$) means there exists $c \in A$
so that $a = bc$. Now the units of $A$ are simply those $u$ in $A$ so that $u|1$. Further
we say that a nonunit $b$ properly divides $a$ if $a = bc$ and $c$ is not a unit of $A$. A
nonzero element $c$ of $A$ is determined up to a unit multiple as the greatest common
divisor of two elements $a$ and $b$ of $A$, if $c|a, c|b$ and for any $d \in A$ such that $d|a$
and $d|b$, then $d|c$. Our notation is $c = \gcd(a, b)$. It is shown in Jacobson (see [6])
that $A$ is a factorial domain if and only if any two nonzero elements of $A$ have a
gcd and the ascending chain condition holds for integral principal ideals of $A$. This
last condition is referred to as ACCP and simply means that there are no infinite
ascending chains of integral principal ideals.

Definition 1. A mapping $N : K \rightarrow Q$ is said to be a norm on the pair $(A, K)$ if
the following properties hold:

1. $N(x) \geq 0$ for all $x \in K$ and $N(x) = 0$ if and only if $x = 0$.
2. $N(xy) = N(x)N(y)$ for all $x$ and $y$ in $K$.
3. $N(a) \in \mathbb{Z}$ for all $a \in A$.
4. For $a$ in $A$, $N(a) = 1$ if and only if $a$ is a unit of $A$.

Theorem 2. An integral domain $A$ is a factorial domain if and only if there is
a norm $N$ on the pair $(A, K)$ satisfying the following condition: Given $a, b \in A$
such that \( a \) does not divide \( b \) and \( b \) does not divide \( a \), there exists a nonzero \( c \in (A : (A : (a, b))) \) with \( N(c) < \min(N(a), N(b)) \).

**Proof.** Suppose that there is a norm \( N \) on the pair \((A, K)\) satisfying the above condition. As we saw above it suffices to prove that any two nonzero elements of \( A \) have a gcd and that ACCP holds for \( A \).

\((\gcd)\) Let \( a, b \in A \) with \( ab \neq 0 \). Let \( c \) be a nonzero element of \((A : (A : (a, b)))\) of smallest norm, \( N(c) \). We claim that \((A : (A : (a, b))) = cA\). Suppose \( e \in (A : (A : (a, b))) \) and \( c \) does not divide \( e \); then \( e \) cannot divide \( c \) because \( N(c) \leq N(d) \) and if \( e|c \), then \( N(c/e) = 1 \), i.e. \( e \) would be a unit times \( c \), which is not possible by our assumption. Now there exist a nonzero \( f \in (A : (A : (e, c))) \) such that \( N(f) < \min(N(e), N(c)) = N(c) \). However because \((e, c) \subseteq (A : (A : (a, b)))\), we have that \((A : (A : (A : (a, b)))) \subseteq (A : (e, c)) \) and thus

\[
(A : (A : (e, c))) \subseteq (A : (A : (A : (a, b)))) = (A : (A : (a, b))),
\]

contradicting the minimality of \( N(c) \). Now to show that \( e = \gcd(a, b) \), we note that \( c|a \) and \( c|b \). Next if \( d \in A \) such that \( d|a \) and \( d|b \), i.e. \( (a, b) \subseteq Ad \), then since \( Ad \) is divisorial and \((A : (A : (a, b)))\) is the smallest divisorial ideal containing \((a, b) \), we have that \( cA = (A : (A : (a, b))) \subseteq Ad \), i.e. \( d|c \).

\((\text{ACCP})\) If we had an infinite sequence of \( a_1, a_2, \ldots \) so that \( a_{i+1} \subseteq Aa_i \), for \( i \geq 1 \), then we would have an infinite strictly descending chain of positive integers \( N(a_1) > N(a_2) > \ldots \), which is clearly impossible.

Now suppose that \( A \) is a factorial domain. Let \( P \) consist of one irreducible element from each associate class of irreducible elements. Then if \( a \) is a nonzero element of \( A \), we write

\[
a = u \prod_{p \in P} p^{n(p)}
\]

where \( u \) is a unit of \( A \) and the \( n(p) \) are nonnegative integers with \( n(p) = 0 \) for all but finitely many \( p \). Here we set \( N(a) = 2^{\sum_{p \in P} n(p)} \). We set \( N(0) = 0 \) and extend \( N \) by multiplicativity to all of \( K \). Now it is easy to see that \( N \) is a norm on the pair \((A, K)\).

Next suppose \( a, b \in A \) such that \( a \) does not divide \( b \) and \( b \) does not divide \( a \). If \( c = \gcd(a, b) \), then \( cA = (A : (A : (a, b))) \) and since \( c \) properly divides \( a \) and \( b \), we must have that \( N(c) < \min(N(a), N(b)) \).

\(\square\)

### 3. Krull Domains

Let \( D(A) \) denote the collection of nonzero divisorial ideals of \( A \) in \( K \). We partially order \( D(A) \) by set-theoretic containment and introduce a binary operation as follows: If \( \mathcal{I}, \mathcal{J} \in D(A) \), then \( \mathcal{I} \circ \mathcal{J} = (A : (A : (\mathcal{I}, \mathcal{J}))) \). Now according to Fossum in ([2]) this order and binary operation makes \( D(A) \) a lattice-ordered commutative monoid with \( A \) as identity. Further, if \( x \in K^* \) and \( \mathcal{I} \in D(A) \), then \( \mathcal{I} \cdot Ax = Ix \) and in fact the principal ideals \( P(A) \) form a subgroup of \( D(A) \). Let \( D(A)^+ \) denote the integral divisorial ideals and \( CL(A) = D(A)/P(A) \) the monoid of divisorial ideal classes. We call \( A \) a Krull domain if, under the above defined binary operation, \( D(A) \) is a group and the elements of \( D(A)^+ \) satisfy the ascending chain condition, i.e. there is no infinite sequence of elements of \( D(A)^+ \), \( \{\mathcal{I}_i\}_{i=1}^{\infty} \), where \( \mathcal{I}_{i+1} \) properly contains \( \mathcal{I}_i \).

Suppose \( A \) is a Krull domain. Let \( \mathfrak{P} \) denote the set of prime divisorial ideals in \( D(A)^+ \); then it is known (see [9]) that \( D(A) \) is the free abelian group on the
elements of \( \mathfrak{I} \). So in particular if \( \mathcal{I} \) is in \( D(A) \) we can write
\[
\mathcal{I} = \prod_{\mathfrak{P} \in \mathfrak{I}} \mathcal{P}^{(v_\mathfrak{P}(\mathcal{I}))}
\]
where the \( v_\mathfrak{P}(\mathcal{I}) \)'s are integers uniquely determined by \( \mathcal{I} \) and \( \mathcal{P} \) and are zero for all but finitely many \( \mathcal{P} \). Our notation needs a little explanation: We write \( \prod \mathcal{P} \) and \( \mathcal{P}^{(n)} \), for \( n \) an integer, to indicate that our binary operation is \( \circ \). We can now define a function on \( D(A) \) as follows: Set \( N(\mathcal{I}) = 1 \) and if \( \mathcal{I} \neq A \) is in \( D(A) \) we set \( N(\mathcal{I}) = 2^{l(\mathcal{I})} \), where \( l(\mathcal{I}) = \sum_{\mathfrak{P} \in \mathfrak{I}} v_\mathfrak{P}(\mathcal{I}) \). Now let \( Q^+ \) and \( Z^+ \) denote the positive rationals and the positive integers respectively. We have defined a map \( N : D(A) \to Q^+ \). It follows then that \( N \) satifies the properties:

1. For \( \mathcal{I}, \mathcal{J} \) in \( D(A) \), \( N(\mathcal{I} \circ \mathcal{J}) = N(\mathcal{I})N(\mathcal{J}) \).
2. If \( \mathcal{I} \) is \( D(A)^+ \), then \( N(\mathcal{I}) \) is in \( Z^+ \) and \( N(\mathcal{I}) = 1 \) if and only if \( \mathcal{I} = A \).

**Definition 2.** Now let \( A \) be any integral domain. A mapping \( N : D(A) \to Q^+ \) is called a norm map on \( D(A) \) if it satisfies the following properties:

1. For \( \mathcal{I}, \mathcal{J} \) in \( D(A) \), \( N(\mathcal{I} \circ \mathcal{J}) = N(\mathcal{I})N(\mathcal{J}) \).
2. If \( \mathcal{I} \) is \( D(A)^+ \), then \( N(\mathcal{I}) \) is in \( Z^+ \) and \( N(\mathcal{I}) = 1 \) if and only if \( \mathcal{I} = A \).

**Definition 3.** A Krull domain is said to be almost factorial if \( CL(A) \) is a torsion group, i.e. every element of \( CL(A) \) is of finite order.

A generalization of Theorem 2 is the following.

**Theorem 3.** An integral domain \( A \) is an almost factorial domain if and only if there is a norm \( N \) on \( D(A) \) with the property: Given \( \mathcal{I} \neq A \) in \( D(A)^+ \), there exist a positive integer \( k \) and an element \( x \) in \( K^* \) so that \( \mathcal{I}^{(k)}x \) is in \( D(A)^+ \) and \( N(\mathcal{I}^{(k)}x) < N(\mathcal{I}) \).

**Proof.** Suppose \( A \) is an almost factorial domain. We saw above that there is a norm on \( D(A) \). Let \( N \) be any norm on \( D(A) \). If \( \mathcal{I} \neq A \) is in \( D(A) \), then there exists a positive integer \( k \) so that \( \mathcal{I}^{(k)} = (y) = Ay \) is a principal ideal, \( y \) a nonzero element of \( A \). Hence \( \mathcal{I}^{(k)}y^{-1} = A \) is in \( D(A)^+ \) and \( N(A) = 1 < N(\mathcal{I}) \).

Now suppose that \( A \) is an integral domain and there is a norm \( N \) on \( D(A) \). This alone guarantees the ascending chain condition on \( D(A)^+ \), since if we have an infinite chain of elements of \( D(A)^+ \), \( \{\mathcal{I}_i\}_{i=1}^\infty \), where \( \mathcal{I}_{i+1} \) properly contains \( \mathcal{I}_i \), then \( \{N(\mathcal{I}_i)\}_{i=1}^\infty \) would be an infinite descending chain of positive integers, which is impossible. Next we assume the property: Given \( \mathcal{I} \neq A \) in \( D(A)^+ \), there exist a positive integer \( k \) and an element \( x \) in \( K^* \) so that \( \mathcal{I}^{(k)}x \) is in \( D(A)^+ \) and \( N(\mathcal{I}^{(k)}x) < N(\mathcal{I}) \). We will show that \( CL(A) \) is a torsion group from which it follows that \( D(A) \) is a group and thus \( A \) is a Krull domain and every element of \( CL(A) \) has finite order. Proceeding by induction we note first that \( A \) is principal and we suppose that \( \mathcal{I} \) is in \( D(A)^+ \), \( \mathcal{I} \neq A \) and for any \( \mathcal{J} \) in \( D(A)^+ \) such that \( N(\mathcal{J}) < N(\mathcal{I}) \), we have that some power of \( \mathcal{J} \) is principal. Then there exist a positive integer \( k \) and an element \( x \) in \( K^* \) so that \( \mathcal{I}^{(k)}x \) is in \( D(A)^+ \) and \( N(\mathcal{I}^{(k)}x) < N(\mathcal{I}) \). Hence there is a positive integer \( m \) so that \( (\mathcal{I}^{(k)}x)^{(m)} = (z) \) is a principal ideal, i.e. \( \mathcal{I}^{(km)} = (zx^{-m}) \). \( \square \)

**Theorem 4.** Suppose \( A \) is an integral domain, \( N \) is a norm map on \( D(A) \) and there is a class \( C \) in \( CL(A) \) with the following property: given \( \mathcal{I} \) in \( D(A)^+ \) with \( \mathcal{I} \neq A \), there exists \( \mathcal{J} \) in \( C \) such that \( \mathcal{I} \circ \mathcal{J} \) is in \( D(A)^+ \) and
\[
N(\mathcal{I} \circ \mathcal{J}) < N(\mathcal{I}).
\]

Then \( A \) is a Krull domain and \( CL(A) \) is a finite cyclic group.
Proof. As we saw in Theorem 3, the existence of a norm map on $D(A)$ guarantees the ascending chain condition on the elements of $D(A)^+$. To show that $D(A)$ is a group it suffices to show that $CL(A) = \{C^{(k)}\}_{k=1}^{\infty}$, because in particular the principal class is of the form $C^{(-k)}$ for some positive integer $k$, i.e. $CL(A)$ is a finite cyclic group from which it follows that $D(A)$ is a group.

If $I \neq A$ is in $D(A)^+$ we need to show that there is a positive integer $k$ so that $I$ is in $C^{(-k)}$ and we will proceed by induction on $N(I)$. If any $J \neq A$ in $D(A)^+$ is in $C^{(-k)}$ for some positive integer $k$ whenever $N(J) < N(I)$, then choose $B$ in $C$ so that $I \circ B$ is in $D(A)^+$ and $N(I \circ B) < N(I)$. Now if $I \circ B = A$, then $I$ is in $C^{(-1)}$ but if $I \circ B \neq A$, then by the induction hypothesis there exists a positive integer $k$ so that $I \circ B$ is in $C^{(-k)}$ and thus $I$ is in $C^{(-k-1)}$. \qed

Theorem 5. If $A$ is a Krull domain with a prime divisorial ideal in every divisorial ideal class, then $CL(A)$ is a finite cyclic group if and only if there is a norm $N$ on $D(A)$ and a class $C$ in $CL(A)$ with the following property: given $I$ in $D(A)^+$ with $I \neq A$, there exists $J$ in $C$ such that $I \circ J$ is in $D(A)^+$ and

$$N(I \circ J) < N(I).$$

Proof. Theorem 3 gives the proof of this equivalence in one direction. Suppose that $A$ is a Krull domain with a prime divisorial ideal in every divisorial ideal class and that $CL(A)$ is a finite cyclic group. If $n$ is the order and $C$ a generator of $CL(A)$, then $CL(A) = \{C^{(0)}, C^{(2)}, C^{(3)}, \ldots, C^{(n-1)}\}$. If $P$ is a prime divisorial ideal and $P$ is in $C^{(k)}$, $0 \leq k \leq n-1$, then we set $N(P) = 2^{n-k}$. Now setting $N(A) = 1$ and extending $N$ to all of $D(A)$ by multiplicativity, it is clear that $N$ is a norm on $D(A)$. Suppose that $I$ is in $D(A)^+$ and $I \neq A$; then we can write $I = I_0 \circ P$, where $I_0$ is in $D(A)^+$ and $P$ is a prime divisorial ideal. If $P$ is in $C^{(k)}$, $0 \leq k \leq n-2$, we choose a prime divisorial ideal $Q$ in $C^{(k+1)}$; then we have that $P^{(k)} \circ Q$ is in $C$, $I \circ P^{(k)} \circ Q$ is in $D(A)^+$ and $N(I \circ P^{(k)} \circ Q) = N(I_0 \circ Q) < N(I)$. Finally if $P$ is in $C^{(n-1)}$, then $P^{(n-1)}$ is in $C$, $I \circ P^{(n-1)} = I_0$ is in $D(A)^+$ and $N(I_0) < N(I)$. \qed

Recall that a Dedekind domain is an integral domain $A$ with the property that $I(A : I) = A$ for every nonzero ideal $I$ of $A$. In this case $D(A) = M(A)$ is a group and the binary operation $\circ$ is just ideal multiplication.

Corollary 1. If $A$ is the ring of integers in an algebraic number field, then $CL(A)$ is a finite cyclic group if and only if there is a norm $N$ on $M(A)$ and a class $C$ in $CL(A)$ with the following property: given $I$ in $M(A)^+$ with $I \neq A$, there exists $J$ in $C$ such that $I \circ J$ is in $M(A)^+$ and

$$N(I \circ J) < N(I).$$

Proof. This result follows from Theorem 5, since a generalization of Dirichlet’s theorem on primes in an arithmetic progression is that (see [5]) there is a prime ideal in every ideal class. \qed

If $A$ is a Krull domain, then it is known (see [2]) that the polynomial domain in one variable $X$ over $A$, denoted by $A[X]$, is not only a Krull domain but every element of $CL(A[X])$ contains a prime divisorial ideal of $A[X]$.

Corollary 2. If $A$ is an integral domain, then $A$ is a Krull domain with $CL(A)$ finite cyclic if and only if there is a norm map $N$ on $D(A[X])$ and a class $C$ in
Let \(I\) be in \(D(A[X])\) with the property: given \(I\) in \(D(A[X])^+\) with \(I \neq A[X]\), there exists \(J\) in \(C\) such that \(I \circ J\) is in \(D(A[X])^+\) and

\[N(I \circ J) < N(I)\]  

**Proof.** It is proven in Fossum (see [2]) that \(A[X]\) is a Krull domain if and only if \(A\) is a Krull domain. Further if \(A\) is a Krull domain, then \(CL(A)\) is isomorphic to \(CL(A[X])\). Now, by Theorem 14.3 on page 63 of Fossum (see [2]), if \(A\) is a Krull domain, then there is a prime divisorial ideal of \(A[X]\) in every element of \(CL(A[X])\). Thus our result follows from Theorems 4 and 5 above. \(\square\)

If \(A\) is a factorial domain or an almost factorial domain, then it is clear from the proofs of Theorems 2 and 3 that any norm on \(D(A)\) will satisfy the condition of those theorems. However if \(A\) is a Krull domain with a prime divisorial ideal in every divisorial ideal class, then it is not true that any norm on \(D(A)\) will satisfy the condition of Theorem 5.

**Example 1.** Let \(A = \mathbb{Z}[\sqrt{34}]\). Of course \(A\) is a Dedekind domain and \(CL(A)\) is cyclic of order 2 (see [1]). Further because \(A\) is the ring of integers in an algebraic number field there is a prime ideal in every ideal class. We claim that the usual norm map on \(D(A) = M(A)\) does not satisfy the condition of Theorem 5. To that end we note that the \(Z\)-module \([3, 4 + \sqrt{34}]\) is a nonprincipal ideal and so it determines a class \(C\) that generates \(CL(A)\) as a cyclic group. The ideal \(I = (6 + \sqrt{34}) = A(6 + \sqrt{34})\) is principal but it is not equal to \(A\). If there were an ideal \(B\) in \(C\) so that \(IB\) is in \(M(A)^+\) and \(N(IB) < N(I)\), then \(B = [3, 4 + \sqrt{34}]x, x\) is in \(K^*, (6 + \sqrt{34})[3, 4 + \sqrt{34}]x \subseteq A\) and \(|N(x)| < 1/3\). Because \((6 + \sqrt{34})[3, 4 + \sqrt{34}] = [6, 4 + \sqrt{34}]\), we have that \(x\) is a nonzero element of \((A : [6, 4 + \sqrt{34}]) = \{1, (4 - \sqrt{34})/6\}\), in which case \(6x\) is in \([6, 4 - \sqrt{34}]\) and \(|N(6x)| < 12\). However we must then have that \(|N(6x)| = 6\) and so it follows that \([6, 4 - \sqrt{34}] = (6x)\), i.e. \([6, 4 - \sqrt{34}]\) is a principal ideal, which we know is not true.

**References**


*Department of Mathematics, Christmas-Saucon Hall, Lehigh University, 14 E. Packer Avenue, Bethlehem, Pennsylvania 18015
E-mail address: csq@lehigh.edu*