ISRAEL JOURNAL OF MATHEMATICS, Vol. 37, No. 4, 1980

HALF-FACTORIAL-DOMAINS

BY
ABRAHAM ZAKS

ABSTRACT
Let R be a commutative domain with 1. We term R an HFD (Half-Factorial-Domain) provided the equality $\Pi_{i=1}^{n} x_i = \Pi_{j=1}^{m} y_j$ implies $m = n$, whenever the x's and the y's are non-zero, non-unit and irreducible elements of R. The purpose of this note is to study HFD's, in particular, Krull domains that are HFD's, and to provide examples of HFD's, that contradict a conjecture of Narkiewicz.

1. Introduction

Let R be a commutative domain with 1. For an element $r \in R$, $r \neq 0$, we say that $r = x_1 \cdots x_n$ is a factorization of r into a product of irreducible factors, if for $i = 1, \cdots, n$, $x_i \in R$ is not a unit and x_i cannot be written as a product of two non-units in R. Recall that r is a prime element in R if Rr is a prime ideal in R.

For a Krull domain R, we denote by $C(R)$ its divisor class group. We identify the height one prime ideals p with their images in $C(R)$. Let $\mathcal{P}$ denote the set of height one prime ideals then $R = \bigcap_{p \in \mathcal{P}} R_p$. We say that R^* is a subintersection if $R^* = \bigcap_{p \in \mathcal{P}^*} R_p$, and $\mathcal{P}^* \subset \mathcal{P}$. Nagata's Theorem states that the natural map of $C(R)$ into $C(R^*)$ is a group epimorphism whose kernel is generated by those prime p for which $p \in \mathcal{P} - \mathcal{P}^*$ [6]. This result applies in particular to any flat overring R_* of R, that is, any ring R_* between R and its field of quotient that is flat as an R-module [6]. In particular, for any multiplicatively closed subset S of R, with $0 \notin S$, the natural map of $C(R)$ into $C(R_S)$ is a group epimorphism whose kernel is generated by those prime ideals p of height one for which $p \cap S \neq \emptyset$.

Let F be a free abelian group on the generators $f_1, f_2, \cdots, f_n, \cdots$. Let H be a subset consisting of elements $m_1 f_1 + \cdots + m_n f_n$ with $m_i \geqq 0$. Under the condition (*) "for each finite set $m_1, \cdots, m_s$ of non-negative integers, there exist nonnegative integers $m_{s+1}, \cdots, m_t$ such that $m_1 f_1 + \cdots + m_t f_t \in H$."

Received November 6, 1978 and in revised form May 8, 1979

There exists a Dedekind domain with non-zero prime ideals $p_1, p_2, \cdots$ such that the map $f_i \to p_i$ for $i = 1, 2, \cdots$, induces a group isomorphism of F/G onto $C(R)$, where G is the group generated by H in F [6]. In particular, the relation $p_1^{m_1} \cdots p_n^{m_n} = Rx$, for some $x \in R$, $x \neq 0$, holds iff $m_1 f_1 + \cdots + m_n f_n \in H$. Such a Dedekind domain is termed a realization of (F, H).

In [9] the following was stated (C_2 is the cyclic group of order 2): "... one can obtain an example of a Dedekind domain in which every element has factorizations of the same length, but the class group has the form $C_2 \times C_2$. It is easy to see that every such example must have its class -group of the form $C_2 \times \cdots \times C_2$ (provided it is finite), but the converse does not obviously hold. Thus we have:

Problem 6. Characterize Dedekind domains in which every element has all its factorizations of the same length...".

The ring R is called an HFD if for every non-zero, non-unit element r in R, any two factorizations into irreducible factors have the same number of terms.

Some results concerning Dedekind HFD's were announced in [11].

In this paper, we extend the results to Krull domains, and we extend and generalize some of the results announced. In particular, we provide examples of Dedekind HFD's with various class group.

In section 2 we generalize some results concerning divisors in a Krull domain. The study of HFD's in section 4 yields criteria for a Krull domain to be an HFD and these are given via conditions on the scattering of the height one primes of R in $C(R)$. We obtain a result similar to that of Carlitz [2], namely: for a Krull domain R, we have $C(R) = Z/2Z$ or else R is a UFD iff $R[x]$ is an HFD. We also obtain a result similar to Narkiewicz's conjecture under two additional hypotheses: (i) for every height one prime ideal p there exists a height one prime ideal q for which $p \cap q \equiv R$, and (ii) $C(R)$ is a torsion group. Then R is an HFD iff $C(R)$ is an elementary 2-group.

We are mainly concerned in this note with HFD's that are Krull domains, but there exist HFD's that are not Krull domains. Some general conditions for a ring to be an HFD are given in section 3.

We provide various examples in section 5 of HFD's that are Krull domains. These examples reflect upon the results cited in section 4, showing that most of them are the best possible.

2. Divisors

Let R be a Krull domain with quotient field K. Let K^* denote the set of units of K. Let div a denote the divisor class of the R-ideal a in K, and let

$\operatorname{div} x = \operatorname{div}(Rx)$ for any $x, x \in K^*$. Let $p^{(n)}$ denote the nth symbolic power of the prime ideal p in R (set $p^{(0)} = R$).

Recall that for a height one prime p in R, $p^{(n)}$ is a divisorial ideal for every positive integer n. We identify $p^{(n)}$ with its image in the divisor class group $C(R)$.

Notice that we use " = " for equality in the ring, in the set of R-ideals in K etc., without specifying, whenever it is clear from the context where the equality holds. We use " ≡ " for equality in $C(R)$.

The following are known for Krull domains R

P1: $\operatorname{div}(ab) = \operatorname{div} a + \operatorname{div} b$.

P2: $\operatorname{div}(a : b) = \operatorname{div} a - \operatorname{div} b$, and $(a : b)$ is divisorial if a is.

P3: $\operatorname{div} a = n_1 p_1 + \cdots + n_t p_t$ iff $a = \bigcap_{i=1}^{t} p_i^{(n_i)}$, whenever a is a divisorial ideal.

P4: For every $x \in K^*$, Rx is a divisorial ideal.

P5: For every divisorial ideal a and for every element $x, x \in K^*$, ax is a divisiorial ideal (as $ax = a : (R : x)$.

Observe that for some pair of non-zero elements x, y in R, the inclusion $Rx \subset Ry$ holds, iff there exists an element z in R such that $Rx = (Ry)(Rz)$, and $Rx = Ry$ iff $x = uy$ where u is an invertible element in R.

P6: Notice that if a, b, c are distinct height one prime ideals, and i, j, k, h integers, then $\operatorname{div}[a^{(i)} \cap c^{(k)})(b^{(j)} \cap c^{(h)})] = \operatorname{div}(a^{(i)} \cap b^{(j)} \cap c^{(h+k)})$.

In particular, if $a^{(i)} \cap c^{(k)}$ and $b^{(j)} \cap c^{(h)}$ are principal ideals, then $(a^{(i)} \cap c^{(k)}) \cdot (b^{(j)} \cap c^{(h)}) = a^{(i)} \cap b^{(j)} \cap c^{(k+h)}$.

LEMMA 1.2. *Let $p^{(m)} \cap q^{(n)}$ be a principal ideal in R, where p and q are height one primes in R and m, n are positive integers. Then $(p^{(m)} \cap q^{(n)})^k = p^{(mk)} \cap q^{(nk)}$.*

PROOF. Since $p^{(m)} \cap q^{(n)}$ is a principal ideal, it is a divisorial ideal as well as its powers. The result follows from P1 and P3.

Notice that it is not necessary to assume that $p \neq q$, and that the same line of proof yields:

PROPOSITION 2.2. *Let $p_1, \cdots, p_t$ be height one primes and $n_1, \cdots, n_t$ be positive integers so that $p_1^{(n_1)} \cap \cdots \cap p_t^{(n_t)}$ is a principal ideal. Then $(p_1^{(n_1)} \cap \cdots \cap p_t^{(n_t)})^k = p_1^{(n_1 k)} \cap \cdots \cap p_t^{(n_t k)}$.*

The arithmetic of principal ideals of R is similar to their arithmetic properties in Dedekind domains, namely:

LEMMA 3.2. *Let p and q be different height one primes in R, such that for some positive integers m and n both $p^{(m)}$ and $q^{(n)}$ are principal ideals. Then $p^{(m)} \cap q^{(n)} = p^{(m)} . q^{(n)}$.*

PROOF. This again follows from P1 and P3 observing that $p^{(m)}\cdot q^{(n)}$ is divisorial by P4.

The same type argument is also valid to obtain, using induction on t:

LEMMA 4.2. *Let $p_1,\cdots,p_t$ be a finite set of different height one primes in R, and let $n_1,\cdots,n_t$ be a set of positive integers, such that $p_i^{(n_i)}$ is a principal ideal for every i, $i=1,\cdots,t$. Then $\bigcap_{i=1}^t p_i^{(n_i)}=\prod_{i=1}^t p_i^{(n_i)}$.*

LEMMA 5.2. *Let p be a height one prime and n a minimal positive integer for which $p^{(n)}$ is a principal ideal.*

If $p^{(n)}=Rx$, then x is an irreducible element in R.

Remark that such an n exists iff p has finite order in $C(R)$ in which case it equals the order of p in $C(R)$.

PROOF. We prove it by contradiction: if $x=yz$ with y,z non-invertible elements in R then we have $Rx=(Ry)(Rz)$; by P4 all these principal ideals are divisorial. As $Rx=p^{(n)}$ it follows by P3 and P1 that $Ry=p^{(k)}$ and $Rz=p^{(m)}$ with $k+m=n$, $k\neq 0$, $m\neq 0$. This contradicts the minimality of n.

Let $p_1,\cdots,p_t$ be a finite set of different height one primes in R and let $n_1,\cdots,n_t$ be positive integers. For a set of non-negative integers $m_1,\cdots,m_t$ we say that $\bigcap_{i=1}^t p_i^{(m_i)}$ is a subintersection of $\bigcap_{i=1}^t p_i^{(n_i)}$ whenever $m_i\leqq n_i$. We say that the subintersection is proper if for some j, $1\leqq j\leqq t$, $m_j\neq n_j$, and not all the m_j's are zero.

PROPOSITION 6.2. *Let $p_1,\cdots,p_t$ be a finite set of different height one primes in R and $n_1,\cdots,n_t$ a set of positive integers so that $a=p_1^{(n_1)}\cap\cdots\cap p_t^{(n_t)}$ is a principal ideal, say $a=Rr$ for some element r in R. Then r is irreducible iff no proper subintersection is a principal ideal.*

PROOF. The proof follows from P1, P3 and P4 observing that (i) r is irreducible iff $Rr=Rb\cdot Rc$ implies $Rb=Rr$ or $Rc=Rr$ and (ii) a subintersection of Rr is principal, say Rb, iff $rb^{-1}\in R$.

Following Lemma 4.2 and the remarks following Lemma 3.2, we may derive using P1 and P3:

PROPOSITION 7.2. *Let $p_1,\cdots,p_t$ be a finite set of distinct height one primes in R, and let $n_1,\cdots,n_t$, $m_1,\cdots,m_t$ be a set of non-negative integers, so that $a=\bigcap_{i=1}^t p_i^{(n_i)}$ and $b=\bigcap_{i=1}^t p_i^{(m_i)}$ are both principal ideals. Then $ab=\bigcap_{i=1}^t p_i^{(n_i+m_i)}$.*

The result naturally extends to a product of finitely many principal ideals.

Passing to $C(R)$ we observe that

LEMMA 8.2. *Let p, q_1, q_2 be different height one primes in R such that $q_1 \equiv q_2 \equiv p$. then $q_1 \cap q_2 \equiv p^{(2)}$.*

PROOF. Since $q_1 \cap q_2$ and $p^{(2)}$ are both divisorial ideals the result is a straightforward consequence of the hypothesis.

3. General criteria

We state various criteria for a domain to be an HFD. We are mainly concerned with Krull domains.

From the definition, it follows that every UFD is an HFD.

Let S be the multiplicative closed subset of R generated by all non-zero elements of R that are not units, that is, $S = \{s \mid s \in R,\ Rs \neq 0 \text{ and } Rs \neq R\}$.

We say that R *admits a length function* if a map l exists, $l : S \to Z^+$ such that for every pair of elements s, t in S we have $l(st) = l(s) + l(t)$.

A straightforward reasoning, based upon the definition of an HFD, yields:

LEMMA 1.3. *A domain R is an* HFD *iff R admits a length function with the property that* $\operatorname{Im} l = Z^+$ *and $l(x) = 1$ iff x is an irreducible element.*

Before proceeding with the study of Krull domains that are HFD's it will be worth noticing that HFD's exist that are not Krull domain.

EXAMPLE. Let $R = Z[\sqrt{-3}]$, then R is not a Krull domain, but R is a subring of the principal ideal domain $A = Z[(1+\sqrt{-3})/2]$. Observe that for every a in A we have either $a \in R$, or $a(1+\sqrt{-3}/2) \in R$, or $a(1-\sqrt{-3}/2) \in R$ while $(1+\sqrt{-3})/2$ and $(1-\sqrt{-3})/2$ are invertible elements in A. The conclusion that R is an HFD follows from the following observations: Firstly, $r \in R$ is irreducible iff $\|r\| = (r_1^2 + 3r_2^2)$, where $r = r_1 + r_2\sqrt{-3}$, cannot be written non-trivially as $(u^2+3v^2)(x^2+3y^2)$ for integers x, y. Secondly, $u \in A$ is a unit iff $\|u\| = 1$.

Remark that $\| \quad \|_A$ and $\| \quad \|_R$ both coincide on elements of R, as they are both induced by the norm of the complex numbers.

Thirdly, if $a \in A$, then for some unit u in A we have $ua \in R$.

Consequently these imply that if r is irreducible in R, it remains irreducible in A.

In particular, since A is a P.I.D. it follows that R is an HFD.

More generally, if we have a subring R in a UFD A, then R is an HFD if irreducible elements in R remain irreducible in A. This is the case if A admits a norm $\| \quad \|$ under which $\|u\| = 1$ iff u is a unit in A, and for every element in A there exists a unit u such that $ua \in R$. Summarizing we get:

LEMMA 2.3. *Let R be a subring of an* HFD, *A. If every irreducible element in R, is irreducible in A, then R is an* HFD. *This in particular is the case when A admits a "norm" $| \quad |$ such that*

(i) *$r \in R$ decomposes iff $|r| = m + n$ where m, n are positive integers and there are elements s, t of R whose norms are $|s| = m$, $|t| = n$.*

(ii) *For every $a \in A$ there exists a unit u in A such that $ua \in r$, and*

(iii) *$|a| = 1$ iff a is a unit in A.*

REMARK. Every UFD admits a norm that satisfies (iii); just set $l(x) = 0$ if x is a unit in R, and $l(x)$ equals the number of factors in a decomposition of x into irreducible factors. Then $2^{l(x)} = |x|$ is a norm on R.

A natural question thus arises:

Is every HFD a subring of a UFD, such that every irreducible element in the HFD remains irreducible in the UFD?

Coming back to the Krull-domain case, a natural way to construct a length function for R in case $C(R)$ is a torsion group is the following: let $O(\mathbf{p})$ for any height one prime be the order of $\mathbf{p}$ in $C(R)$. For a divisorial ideal $\mathbf{a} = \bigcap_{i=1}^{t} \mathbf{p}_i^{(n_i)}$ set $L(\mathbf{a}) = \Sigma n_i / O(\mathbf{p}_i)$. Since for principal ideals we have $L(Rxy) = L(Rx) + L(Ry)$, setting $l(z) = L(Rz)$ for every z in R yields a function from S into the rationals. For the rest we always assume that R is a Krull domain.

THEOREM 3.3. *Let $C(R)$ be a torsion group. Then R is an* HFD *iff under the function l as defined, $l(r) = 1$ iff r is an irreducible element in R.*

PROOF. Since $l(rs) = l(r) + l(s)$ for every pair of elements r, s in S, then $l(r) = 1$ iff r is an irreducible element in R is a sufficient condition, by Lemma 1.3, for R to be an HFD. Conversely, let R be an HFD, and let $\mathbf{a} = \mathbf{p}_i^{(n_i)} \cap \cdots \cap \mathbf{p}_t^{(n_t)}$ be a principal ideal, where $\mathbf{p}_i$ are height one primes of order $O(\mathbf{p}_i)$ and n_i are positive integers. If $\mathbf{a} = Ru$, and if k is the least common multiple of all the $O(p_i)$'s, then $Ru^k = \mathbf{p}_1^{(n_1k)} \cap \cdots \cap \mathbf{p}_t^{(n_tk)}$ (see Propsoition 2.2). Each $\mathbf{p}_i^{(n_ik)}$ is a principal ideal, say Rv_i, and since R is an HFD v_i is the product of precisely $n_ik / O(\mathbf{p}_i)$ factors, in any factorization of v_i into irreducible factors. If u is the product of q irreducible elements in R, then the following equality results:

$$kq = (n_1k / O(\mathbf{p}_1)) + \cdots + (n_tk / O(\mathbf{p}_t)),$$

whence

$$q = (n_1 / O(\mathbf{p}_1)) + \cdots + (n_t / O(\mathbf{p}_t)).$$

By definition

$$l(u) = L(Ru) = (u_1/O(p_1)) + \cdots + (u_t/O(p_t)).$$

Thus, in particular, $L(u)$ equals the *integer* q, where q is the number of irreducible elements in any factorization of u into irreducible elements. In particular, $l(r) = 1$ iff r is an irreducible element in R.

This result may also be stated as follows:

THEOREM 3′.3. *Let $C(R)$ be a torsion group. Then R is an* HFD *iff the domain of the function l as defined above is Z^+, and if $l(r) > 1$, then a proper subintersection of $Rr = p_1^{(n_1)} \cap \cdots \cap p_t^{(n_t)}$ exists which is a principal ideal.*

Remark that this in particular implies that if $Rr = p_1^{(n_1)} \cap \cdots \cap p_t^{(n_t)}$ then $(n_1/m_1) + \cdots + (n_t/m_t)$ is an integer, where $m_i = O(p_i)$, and there exist integers $0 \leqq n_i' \leqq n_i$, such that $(n_1'/m_1) + \cdots + (n_t'/m_t) = 1$.

Recall that we termed [11] the set of positive integers $m_1, \cdots, m_t$ a *splittable* set if whenever positive integers $n_1, \cdots, n_t$ exist so that $\Sigma_{i=1}^t (n_i/m_i)$ is an integer, there exist positive integers $n_1', \cdots, n_t'$ such that $0 < n_i' \leqq n_i$, and $\Sigma_{i=1}^t (n_i'/m_i) = 1$. Modify this by requiring that the n_i''s are non-negative integers.

There arises naturally the question:

Is every finite set of positive integers, a splittable set?

The following examples show that not all finite sets are splittable sets:

(a) $(2,3,5,30): \frac{1}{2} + \frac{2}{3} + \frac{4}{5} + \frac{1}{30} = 2$ and no subsum adds up to 1.

(b) $(2,3,5,7,210): \frac{1}{2} + \frac{2}{3} + \frac{2}{5} + \frac{3}{7} + \frac{1}{210} = 2$ and no subsum adds up to 1.

In these cases we have sets consisting of primes and their least common multiple. One can produce more examples of this type.

If the set consists of different prime numbers, it is always a splittable set. Other splittable sets are $\{q^{n_1}, \cdots, q^{n_t}\}$ where q is a prime number.

This suggests the following problem:

PROBLEM. Which sets are splittable sets?

LEMMA 4.3. *For each n, the set $\{m! \mid 2 \leqq m \leqq n\}$ is a splittable set.*

PROOF. By induction on n: For $n = 2$, it is obvious.

For $n > 2$, notice that if $A = \Sigma_{i \geqq 2} a_i/i!$ is an integer, then $n!A = \Sigma_{i \geqq 2} a_i(n!/i!)$.

In particular, n divides a_n. We may thus write

$$A = \sum_{(n-2) \geqq i \geqq 2} a_i/i! + (a_{n-1} + a_n')/(n-1)! \qquad \text{where } na_n' = a_n, \quad a_n' \in Z^+.$$

The induction applies to this expression of $A : A_1 + A_2$, $A_j = \Sigma_{(n-2)\geqq i>2} a_{ji}/i!$, $0 \leqq a_{ji} \leqq a_i$ for $i = 2,\cdots,(n-2)$ and $0 \leqq a_{j(n-1)} \leqq a_{n-1} + a'_n$ for $j = 1,2$ such that $A_1 = 1$. We will end the proof when we show that we may choose $a_{1(n-1)} = b_1 + c_1$, $a_{2(n-1)} = b_2 + c_2$ with $0 \leqq b_j \leqq a_{n-1}$, $0 \leqq c_j \leqq a'_n$ for $j = 1,2$.

As $a_{1(n-1)} + a_{2(n-1)} = a_{n-1} + a'_n$ we have:

$$\text{If} \quad a_{1(n-1)} > a_{n-1} \quad \text{then} \quad a_{2(n-1)} < a'_n.$$

Take $c_2 = a_{2(n-1)}$, $b_2 = 0$, $b_1 = a_{n-1}$, $c_1 = a_{1(n-1)} - a_{n-1}$. Then the required inequalities hold for b_1, b_2, c_2 obviously, and

$$c_1 = a_{1(n-1)} - a_{n-1} = (a_{n-1} + a'_n - a_{2(n-1)}) - a_{n-1} = a'_n - a_{2(n-1)} \leqq a'_n.$$

If $a_{1(n-1)} \leqq a_{n-1}$, take $b_1 = a_{1(n-1)}$, $c_1 = 0$, $b_2 = a_{2(n-1)} - a'_n$, $c_2 = a'_n$ then the required inequalities hold obviously for b_1, c_1, c_2 and

$$b_2 = a_{2(n-1)} - a'_n = (a_{n-1} + a'_n - a_{1(n-1)}) - a'_n = a_{n-1} - a_{1(n-1)} \leqq a_{n-1}.$$

To complete the proof, let a_{ji} for $j = 1,2$, and $i = 2,\cdots,(n-2)$ be as above and set $a_{1(n-1)} = b_1$, $a_{1n} = c_1 n$, $a_{2(n-1)} = b_2$, $a_{2n} = c_2 n$.

Observe that a subset of a splittable set is itself splittable.

Note the following equivalent statement of this result:

LEMMA 4'.3. *Let $f(x)$ be a polynomial of degree n. Let $f(0), f'(0),\cdots, f^{(n)}(0)$, $f(1)$ be positive integers. Then there exists m polynomials of degree n, $f_1(x),\cdots,f_m(x)$ such that $f_i(0), f'_i(0),\cdots, f_i^{(n)}(0)$ are positive integers, and $f_i(1) = 1$ for all $i = 1,\cdots,m$ and $f(x) = f_1(x) + \cdots + f_m(x)$.*

In case $C(R)$ is not a torsion group, still one gets similar results to Theorems 3.3 and 3'.3, except that for elements p in $C(R)$ that are not torsion elements one cannot predict $L(p)$.

To this extent, let G denote the free group on the height one primes, and D its subgroup consisting of principal divisors. For an HFD R, we always have the function $l : D \to Z$, which extends to $L : G \to Q$, where Q denotes the rational integers. Obviously l is induced by L, and whenever p in G is a torsion element in $C(R)$, say of order n, then $L(p) = 1/n = 1/O(p)$.

Summarizing, we get:

THEOREM 5.3. *Let R be a Krull domain, then R is an* HFD *if there exists a group homomorphism $L : G \to Q$ that induces a length function on R such that $l(x) = 1$ iff x is irreducible.*

4. Krull domains

In this section we study Krull domains that are HFD's.

We start by pointing out a class of Krull domains that are always HFD. In the sequel, its importance beyond that of providing examples of HFD's that are not UFD's will become clear.

THEOREM 1.4. *Let R be a Krull domain with $C(R) \approx Z/2Z$. Then R is an* HFD.

PROOF. By the hypothesis, for every pair of non-principal height one primes p_1 and p_2 we have $p_1 \equiv p_2$. By Lemma 8.2 it follows that $p_1 \cap p_2$ is a principal ideal for every pair of distinct non-principal height one prime ideals. By Proposition 6.2, if $a = p_1^{(n_1)} \cap \cdots \cap p_t^{(n_t)}$ is a principal ideal, where $p_1, \cdots, p_t$ is a finite set of distinct height one primes in R, and $n_1, \cdots, n_t$ are positive integers, and if $a = Rr$, then for r to be irreducible it is necessary that one of the following holds: (i) $t = 1$, $n_1 = 1$, (ii) $t = 1$, $n_1 = 2$, or (iii) $t = 2$, $n_1 = n_2 = 1$. In case (i) $Rr = p_1$, that is r is a prime element. In case (ii) $Rr = p_1^{(2)}$ where p_1 is a non-principal height one prime. In case (iii) $Rr = p_1 \cap p_2$ where p_1 and p_2 are non-principal height one prime. Consider any element s in R, and consider the representation of Rs as an intersection, say $Rs = q_1^{(m_1)} \cap \cdots \cap q_i^{(m_i)}$, where $q_1, \cdots, q_i$ are different height one primes in R and $m_1, \cdots, m_i$ are positive integers. By the representation of Rr for irreducible elements r in R and by Proposition 7.2 applied to a product of finitely many principal ideals, it results that any factorization of s into irreducible, non-units in R has the same number of factors: in fact, if the q's are so arranged that $q_1 \cdots q_j$ are principal primes and $q_{j+1} \cdots q_i$ are non-principal primes (with the obvious conventions as for $j = 0$ and $j = i$), then the number of factors in any irreducible factorization of s is $m_1 + \cdots + m_j + \frac{1}{2}(m_{j+1} + \cdots + m_i)$.

In particular this yields that R is an HFD as stated.

By ([5], [7], [8]), flat overrings of R within K are localizations in case $C(R) = Z/2Z$. Furthermore, every localization of R within K is a Krull domain A with $C(A)$ a factor group of $C(R)$. Let R be a Krull domain whose class group is isomorphic to $Z/2Z$. Let S be the multiplicative set in R, generated by 1 and all the prime elements in R, then R_S is a Krull domain with class group isomorphic to $Z/2Z$, and R_S has no prime elements. Consequently, for every proper flat overring T of R_S, $C(T) = \{1\}$, thus providing examples of:

EXISTENCE THEOREM. *There exist Krull domains R that are* HFD *but are not* UFD, *such that every proper flat overring of which is a* UFD.

Passing from the Krull-domain R to the ring of polynomials in one variable $R[x]$, it is known that $C(R) = C(R[x])$, and that in every class of $C(R[x])$ there lies a height one prime ideal of $R[x]$ (e.g. [6]).

Since irreducible elements of R remain irreducible in $R[x]$, it follows that if $R[x]$ is an HFD then R is an HFD.

Our next task is to study the converse, that is: let R be an HFD. Is $R[x]$ an HFD?

Observe the resemblance of the result to that of Carlitz ([2]). It seems that the crux lies in the fact that both in rings of integers of algebraic number fields, and in $R[x]$, every class of the divisor class group contains a prime ideal.

THEOREM 2.4. *Let R be a Krull domain. The ring* $R[x]$ *is an* HFD *iff* $C(R)$ *is either* $\{1\}$ *or else* $Z/2Z$.

PROOF. If $C(R) = \{1\}$ then R is a UFD, whence $R[x]$ is a UFD, and every UFD is obviously an HFD.

If $C(R) = Z/2Z$ then $C(R[x]) = Z/2Z$ and by Theorem 1.4 $R[x]$ is an HFD.

Conversely, let $R[x]$ be an HFD. If R is a UFD we are done. If not, then $C(R[x])$ is either (a) a torsion group, but not an elementary 2-group, (b) an elementary 2-group, or else (c) not a torsion group. We will prove that cases (a) and (c) are impossible, and in case (b) $C(R)$ has a unique summand. This will establish our claim.

Case a. Let $\boldsymbol{p}$ be an height one prime ideal in $R[x]$ that is not a principal ideal and whose order in $C(R[x])$ is n, $n > 2$. In $R[x]$ we may find a height one prime $\boldsymbol{q}$ so that in $C(R[x])$ we have $\boldsymbol{q} \equiv \boldsymbol{p}^{(n-1)}$. Consequently, the divisorial ideal $\boldsymbol{p} \cap \boldsymbol{q}$ is a principal ideal, say $\boldsymbol{a} = \boldsymbol{q} \cap \boldsymbol{p}$, $\boldsymbol{a} = R[x]r$ for some element r in $R[x]$. By Proposition 6.2 r is an irreducible element. Since the order of $\boldsymbol{p}$ in $C(R[x])$ is n, the order of $\boldsymbol{q}$ is n. In particular, the principal ideals $\boldsymbol{p}^{(n)}$ and $\boldsymbol{q}^{(n)}$ are generated by irreducible elements in $R[x]$. By Lemmas 1.2 and 3.2 $R[x]r^n = (R[x]s)(R[x]t)$, where $\boldsymbol{p}^{(n)} = R[x]s$ and $\boldsymbol{q}^{(n)} = R[x]t$. Hence $r^n = (u\, s)t$ where u is a unit in $R[x]$. Since us is irreducible in $R[x]$ and $n \geqq 2$ this contradicts the hypothesis that $R[x]$ is an HFD.

Case b. Suppose $C(R[x])$ is not isomorphic to $Z/2Z$. Then in $R[x]$ we can find non-principal height one primes $\boldsymbol{p}$, $\boldsymbol{q}$ such that $\boldsymbol{p} \neq \boldsymbol{q}$ in $C(R[x])$. In particular $\boldsymbol{p} \cap \boldsymbol{q}$ is not a principal ideal. Let $\boldsymbol{a}$ be a height one prime ideal in $R[x]$ such that $\boldsymbol{a} = \boldsymbol{p} \cap \boldsymbol{q}$ in $C(R([x])$. Then we have the following principal ideals, $\boldsymbol{p}^{(2)}$, $\boldsymbol{q}^{(2)}$, $\boldsymbol{a}^{(2)}$, $\boldsymbol{a} \cap \boldsymbol{p} \cap \boldsymbol{q}$. All of these principal ideals are generated by irreducible elements. Consider the equality $(\boldsymbol{a} \cap \boldsymbol{p} \cap \boldsymbol{q})^2 = \boldsymbol{a}^{(2)} \cdot \boldsymbol{p}^{(2)} \cdot \boldsymbol{q}^{(2)}$ that follows from Propositions 2.2 and 4.2. If $\boldsymbol{a}^{(2)} = R[x]a$, $\boldsymbol{p}^{(2)} = R[x]p$, $q^{(2)} = R[x]q$, $\boldsymbol{a} \cap \boldsymbol{p} \cap \boldsymbol{q} = R[x]b$, where a, b, p, q are irreducible elements in $R[x]$, then $b^2 = (ua)\,p \cdot q$ where u is a unit in $R[x]$, and this contradicts the hypothesis that $R[x]$ is an HFD. Whence, if $C(R[x])$ is an elementary 2-group, then necessarily it is isomorphic to $Z/2Z$.

Case c. Let g be an element in $C(R[x])$ of infinite order. Let $\boldsymbol{p}$, $\boldsymbol{q}$ be height one primes in $R[x]$ such that $\boldsymbol{p} \equiv g$ and $\boldsymbol{q} \equiv -g$ in $C(R[x])$. Then $\boldsymbol{p} \cap \boldsymbol{q}$ is a principal ideal that is generated by an irreducible element in $R[x]$. Let $\boldsymbol{a}$, $\boldsymbol{b}$ be height one primes in $R[x]$ so that $\boldsymbol{a} \equiv \boldsymbol{p}^{(2)}$, $\boldsymbol{b} \equiv \boldsymbol{q}^{(3)}$ in $C(R[x])$. Then $\boldsymbol{b} \cap \boldsymbol{a} \cap \boldsymbol{p}$ is a principal ideal, and by Proposition 6.2 it is generated by an irreducible element y, $y \in R[x]$. Consider $Ry^3 = (Ry)^3$ which decomposes into $Ry^3 = \boldsymbol{b}^{(3)} \cap \boldsymbol{a}^{(3)} \cap \boldsymbol{p}^{(3)}$. Notice that both $\boldsymbol{b} \cap \boldsymbol{p}^{(3)}$ and $\boldsymbol{b}^{(2)} \cap \boldsymbol{a}^{(3)}$ are principal ideals. By Proposition 6.2 $\boldsymbol{b} \cap \boldsymbol{p}^{(3)}$ is generated by an irreducible element s, $s \in R[x]$. Also Proposition 6.2 applies to $\boldsymbol{b}^{(2)} \cap \boldsymbol{a}^{(3)}$, as no subintersection can be zero in $C(R[x])$, whence $\boldsymbol{b}^{(2)} \cap \boldsymbol{a}^{(3)} = R[x]t$, where t is an irreducible element in $R[x]$. Consequently $y^3 = (us)t$ for some unit u in $R[x]$, and this contradicts the hypothesis of R being an HFD. Q.E.D.

Our next result comes very close to Narkiewicz's conjecture, provided the additional hypothesis, namely, the existence of primes that are inverses to given primes in $C(R)$:

THEOREM 3.4. *Let R be a Krull domain such that for every height one prime $\boldsymbol{p}$, there exists a height one prime $\boldsymbol{q}$ such that $\boldsymbol{p} \cap \boldsymbol{q} \equiv R$. Then the following are equivalent*:

(i) *R is an* HFD.

(ii) *$C(R)$ is a direct sum of a free group and an elementary* 2*-group, and for every height one prime $\boldsymbol{q}$, if $\boldsymbol{q}$ is non-principal and $\boldsymbol{q} \equiv \boldsymbol{q}_1^{(n_1)} \cap \cdots \cap \boldsymbol{q}_t^{(n_t)}$ for some height one primes $\boldsymbol{q}_1, \cdots, \boldsymbol{q}_t$ then $\boldsymbol{q} \equiv \boldsymbol{q}_1$ for some i.*

PROOF. (i) $\Rightarrow$ (ii). Let $\boldsymbol{p}$ be a height one prime of finite order in $C(R)$. Let m be its order. If $\boldsymbol{p} \cap \boldsymbol{q} \equiv R$, $\boldsymbol{q}$ a height one prime, then the order of $\boldsymbol{q}$ is m. Since R is an HFD we must have $1/m + 1/m = 2/m$ an integer. Whence $m = 1$ or $m = 2$. Thus every torsion element in $C(R)$ is a 2-torsion element.

Suppose that $\boldsymbol{p}_1, \cdots, \boldsymbol{p}_s$ are height one primes and $\boldsymbol{p}_1^{(n_1)} \cap \cdots \cap \boldsymbol{p}_s^{(n_s)}$ is a principal ideal that is generated by an irreducible element. Let $\boldsymbol{q}_1, \cdots, \boldsymbol{q}_s$ be height one primes such that $\boldsymbol{p}_i \cap \boldsymbol{q}_i$ is a principal ideal for $i = 1, \cdots, s$. We may assume that $s \neq 1$. Whence all $\boldsymbol{p}_i$ are non-principal primes. Then $\boldsymbol{q}_1^{(n_1)} \cap \cdots \cap \boldsymbol{q}_s^{(n_s)}$

is a principal ideal generated by an irreducible element.† Consequently there results a principal ideal generated by a product of two irreducible elements, namely $(p_1^{(n_1)} \cap \cdots \cap p_s^{(n_2)}) \cdot (q_1^{(n_1)} \cap \cdots \cap q_s^{(n_s)})$, which also can be represented as a product of principal ideals in the following way: $(p_1 \cap q_1)^{n_1} \cdots (p_s \cap q_s)^{n_s}$. Since R is an HFD, necessarily $n_1 + \cdots + n_s = 2$. As $s \neq 1$ we must have $s = 2$ and $n_1 = n_2 = 1$.

Hence every height one prime is either of order two or of infinite order. For every height one prime p, let $\mathcal{Q}_p$ be the set of all height one primes q such that $p \cap q$ or $p \cap q \equiv R$.

Pick one p in each class $\mathcal{Q}_p$ (except the class of R), then these p's generate $C(R)$ and there are no non-trivial relations among them. In particular, $C(R)$ is the direct sum of the free group generated by the p's whose order is infinite, and the elementary 2-group generated by the rest of the p's. Furthermore, every height one prime in R is equivalent in $C(R)$ to some p, or $-p$. In particular, if $q \equiv q_1^{(n_1)} \cap \cdots \cap q_s^{(n_s)}$ then for q' with $q' \cap q \equiv R$ we have $R \equiv q' \cap q_1^{(n_1)} \cap \cdots \cap q_s^{(n_s)}$, if $q' \neq q_i$ for $i = 1, \cdots, s$. If q is non-principal, then necessarily for some i $q' \cap q_i$ is a principal ideal, whence $q \equiv q_i$.

If $q' = q_i$ for some i, say $i = 1$, then $q_1^{(n_1+1)} \cap \cdots \cap q_s^{(n_s)} \equiv R$. In case q is of finite order, $q \equiv q_1$. In case q is of infinite order, q' is such too, and at least one of the q's with $2 \leqq j \leqq s$ must be such that $q_j \cap q_1 \equiv R$. In particular, $q \equiv q_j$.

Summarizing, $C(R)$ is a direct sum of a free group and an elementary 2-group, and whenever $q \equiv q_1^{(n_1)} \cap \cdots \cap q_s^{(n_s)}$ where q is a non-principal ideal, then $q \equiv q_i$ for some i, $1 \leqq i \leqq s$. That is, $C(R)$ has a set of generators $\{p\}$ consisting of height one prime ideals of R, the only relations among these p's are the ones arising from $p^{(2)} \equiv R$ for the torsion elements, and for every height one prime q in $C(R)$ if $q \not\equiv R$ then there exists a prime p such that $q \equiv p$ or $q \equiv -p$.

(ii) $\Rightarrow$ (i). Let x be an irreducible element and assume Rx is not a prime ideal. Let $Rx = p_1^{(n_1)} \cap \cdots \cap p_s^{(n_s)}$ for some height one primes $p_1 \cdots p_s$. If some p, say p_1, has order 2, then $n_1 = 1$ or $n_1 = 2$. If $n_1 = 1$ then from $p_1 p_2^{(n_2)} \cap \cdots \cap p_s^{(n_s)}$ it follows that $Rx = p_1 \cap p_2$ and if $n_1 = 2$ then $Rx = p_1^{(2)}$. If p_1 has infinite order, and if q is a height one prime such that $p_1 \cap q \equiv R$, then $p_1 \cap q \equiv p_1^{(n_1)} \cap \cdots \cap p_s^{(n_s)}$ where $q \equiv p^{(n_1-1)} \cap \cdots \cap p_s^{(n_s)}$, and q being non-principal implies $q \equiv p_i$ for some $i \geqq 2$. Since x is irreducible, this necessarily implies $s = 2$, and $n_1 = n_2 = 1$.

Thus, for every irreducible element x, Rx is a prime ideal or $Rx = p^{(2)}$ or else $Rx = p \cap q$ where p and q are height one primes. Consequently, if we let

† If the q_i's are not distinct, say $q_1 = q_2$, then take $q_1^{(n_1+n_2)}$, and a similar proof using P6 establishes the result.

$L(p) = 1/2$ for every height one prime that is not a principal ideal, the function $l(x)$ achieves only integral values and $l(x) = 1$ iff x is an irreducible element, whence by Theorem 3.3 R is an HFD as stated. Q.E.D.

In the two extreme cases we get:

COROLLARY 4.4. *Let R be a Krull domain such that for every height one prime p there exists a height one prime q such that $p \cap q \equiv R$. If R is an* HFD, *and $C(R) = Z$ then a height one prime p exists such that for each height one prime q in R, either $p \equiv q$, or $p \cap q \equiv R$, or $q \equiv R$.*

COROLLARY 5.4. *Let R be a Krull domain such that for every height one prime p there exists a height one prime q such that $p \cap q \equiv R$. If R is an* HFD *with torsion class group, then $C(R)$ is an elementary 2-group.*

Note that $C(R)$ being an elementary 2-group is not a sufficient condition to imply that R is an HFD.

In Section 5 we will privide an example of a Dedekind domain R that is an HFD in which for each non-zero prime ideal p there exists a prime ideal q such that $p \cap q \equiv R$. As for Krull domains, R is an HFD whenever $C(R) = Z/2Z$.

A related problem is: Does there exist a Krull domain R that is not a Dedekind domain such that R is an HFD and $C(R) \neq 0$ or $Z/2Z$.

We end this section with some cases of special interest. From here on, unless otherwise specified, we assume $C(R)$ to be a cyclic group, generated by some prime p, and R to be a Krull domain.

If $C(R)$ is a torsion group, that is in particular a finite group, and q any prime of height one in R, then for some integer k, $q \equiv p^{(k)}$. Assume k to be the smallest possible, and suppose $q \not\equiv R$. Let the order of $C(R)$ be n, then $0 < k \leqq n$.

Observe that $p^{(n-k)} \cap q$ is a principal ideal, say Rx, with x an irreducible element in R. In case R is an HFD, we must necessarily have $1/m + (n-k)/n = 1$, where m is the order of q in $C(R)$. This last equality implies $n = km$. We have thus established:

THEOREM 6.4. *Let $C(R)$ be a finite cyclic group of order n, generated by some prime p. If R is an* HFD, *then for every height one prime q in R, if $q \neq R$, then $q \equiv p^{(k)}$ for some integer k such that $k \mid n$.*

REMARK 1. If $C(R)$ is torsion free, examples 4–6 suggest that no analogues to Theorem 1 exist in this case.

REMARK 2. The converse of Theorem 6.4 does not hold in general, e.g. example 10. However, if $n_1 < \cdots < n_t = n$ are the orders of prime ideals in

$C(R)$, and if $\{n_1, \cdots, n_t\}$ is a splittable set, then the converse will hold, too. In particular, if the set of all factors of n is a *splittable* set, then the converse holds.

In fact, we could study any pair of height one primes p, q in R, provided that q belongs to the subgroup generated by p in $C(R)$, as long as p has finite order. Thus obtaining:

PROPOSITION 7.4. *Let p be a height one prime of finite order in $C(R)$, say n, and let q be a height one prime in R such that $q \equiv p^{(k)}$ for some integer k. Then $q \equiv p^{(k_0)}$, where $0 \leqq k_0 \leqq n$ and either $k_0 = 0$ or else $k_0 \mid n$.*

A converse for this proposition, in case $C(R)$ is a torsion group, will depend as above on certain sets being *splittable* sets.

In particular, we may derive the following:

THEOREM 8.4. *Let $C(R)$ be a cyclic q-group for some prime number q, or Z_{q^∞}, then R is an* HFD *iff for every pair of height one primes p_1, p_2 that are not principal primes, there exists an integer n, $n \geqq 0$, such that $p_1 \equiv p_2^{(q^n)}$ or else $p_2 \equiv p_1^{(q^n)}$.*

Note that the Z_{q^∞} case fits in as its proper subgroups are cyclic q-groups and the converse holds as the set of factors of q^n is a splittable set for each n, and finally, every cyclic q-group $C(R)$ has necessarily some prime p as its generator.

To this extent note that there exist Dedekind domains R with $C(R)$ a cyclic q group or Z_{q^∞} for which all proper overrings are HFD but R itself is not an HFD. However, we have:

COROLLARY 9.4. *Let $C(R)$ be a cyclic q-group. If R is an* HFD *then every overring of R is an* HFD.

If we let $C(R) = Z_{q^\infty}$, and R is an HFD, then every flat overring of R is an HFD, but not every flat overring of R is a localization. A natural problem arises:

PROBLEM. Is every overring of R an HFD, if R is an HFD and $C(R) = Z_{q^\infty}$?

The answer is affirmative for Dedekind domains as its overrings are flat.

One can produce examples of Dedekind domains R, with a finite class group, such that every proper overring is a PID, but R itself is not an HFD. In fact, whenever $C(R)$ is a group of order q, for some prime q, and if we let S denote the multiplicative set of prime elements, then $C(R) = C(R_S)$. Every proper overring T of R_S is necessarily a PID, since $C(R_S)$ is a simple group and the epimorphism $C(R_S) \to C(T)$ has no trivial kernel.

If $C(R)$ is of order n, not a prime integer, a similar example results upon starting with a Dedekind domain whose primes are scattered in all classes $g_1, \cdots, g_k$ of elements of $C(R)$ that generates $C(R)$, and only in those.

However, if R is an HFD and its flat overrings are UFD's then necessarily

(i) $C(R)$ is a cyclic group, and

(ii) R has no prime elements, or else $C(R) = 0$.

Since if flat overrings are UFD, and if $C(R)$ is a finite group, then for any height one prime p there exists an integer m such that $p^{(m)} = Ra$. Since $C(R[1/a]) = 0$, whence p generates $C(R)$. Since this holds for every height one prime, and since R is an HFD, it follows that $p \equiv q$ for every pair of height one prime ideals. Obviously, if $p \equiv q$ for every pair of height one prime ideals then $C(R)$ is a finite cyclic group (e.g. consider $Rx = p_1^{(n_1)} \cap \cdots \cap p_t^{(n_t)}$) generated by p. It follows that every flat overring is a localization whence a UFD, since the kernel of the epimorphism $C(R) \to C(R_S)$ contains some q. From $p \equiv q$ it also follows that R is an HFD. Consequently we established:

Proposition 10.4. *The Krull domain R is a* HFD *and its proper flat overrings are* UFD's *iff all height one prime ideals are equal in $C(R)$.*

Note that such a result cannot hold if $C(R) = Z_{q^\infty}$. To this extent note that for every subgroup H of $C(R)$ that is generated by some height one prime ideals in R, one easily constructs an overring R^* of R (whence a flat overring in case R is a Dedekind domain) for which the epimorphism $C(R) \to C(R^*)$ has H as its kernel. In particular for $C(R^*) = 0$ to hold, it follows that $H = C(R)$. Let g be a generator for $C(R)$, let p, q be any pair of height one prime ideals in R for which $p \equiv mg$ and $q \equiv -ng$, where m, n are positive integers. Since $p^{(n)} \cap q^{(m)} \equiv R$ it follows that a localization R^* of R exists for which the kernel H of the epimorphism $C(R) \to C(R^*)$ is generated by p and q. For $C(R^*)$ to be zero, it is necessary that $(m, n) = 1$. If there exists in R height one primes $p' \equiv m'g$, $q' \equiv -n'g$ with $m \neq m'$ and $n \neq n'$, it will follow that R is not an HFD, as the equalities $nL_1 + mL_2 = 1$, $n'L_1 + mL_4 = 1$, $nL_3 + m'L_2 = 1$ and $n'L_3 + m'L_4 = 1$ cannot be solved simaltaneously. However, if we always have $n' = n$, they have the solution: $L_2 = L_4 = 0$, $L_1 = L_3 = 1/n$. Such rings exist (see examples 5 and 6) and they provide examples of (a) rings R for which proper flat overrings are UFD, and R itself is an HFD when $n = 1$ and $m = m' = 1$, and (b) rings R for which proper flat overrings are HFD and R itself is an HFD when $n = n'$, $m = m'$ and $(n, m) = 1$.

However, in case R is a Dedekind domain, then for every height one prime ideal p set $R^* = \bigcap_{p \in \mathcal{P}^*} R_p$ where $\mathcal{P}^* = \mathcal{P} - \{p\}$. The kernel of the epimorphism $C(R) \to C(R^*)$ is generated by p. If flat overrings are UFD, then $C(R^*) = 0$, whence p is a generator. Since every overring of a Dedekind domain is flat, every overring is a subintersection (see [6]). In particular this implies that every height one prime p is a generator for $C(R)$. We have thus established:

PROPOSITION 11.4. *The Dedekind domain R is an* HFD *and its proper flat overrings are* UFD's *iff for every pair of height one prime ideals p and q either $p \equiv q$ or else $p \cap q \equiv R$. If for some height one prime p, $p \cap q \equiv R$ and $p \not\equiv R$, then $C(R)$ is isomorphic to Z.*

5. Examples

The purpose of this section is to provide examples of HFD's that are Dedekind domains with various possible class groups, from which one may derive the extent to which the results in the previous sections are best possible ones.

We are not going to specify the reason for each example. Thus it will be left in part for the interested reader to draw the conclusions.

For the rest of this section, let F denote a free group on a countable number of generators $\{f_1, f_2, \cdots\}$, let G denote the non-negative subset of F consisting of all finite sums $n_1 f_1 + \cdots + n_k f_k$ with $n \geqq 0$, and let H be a subset of G, such that:

(*) For each finite set $m_1, \cdots, m_s$ of non-negative integers, there exist non-negative integers $m_{s+1}, \cdots, m_t$ such that $m_1 f_1 + \cdots + m_t f_t \in H$.

Let K denote the subgroup in F generated by H.

By ([4], [8]), there exists a Dedekind domain R with countably many non-zero primes $\{p_1, p_2, \cdots\}$ such that there is an isomorphism of F/K onto $C(R)$ given by $f_i \to p_i$. In other words, the p's generate $C(R)$ and the group of relations is generated by those $p_1^{n_1} \cdots p_k^{n_k}$ such that $n_1 f_1 + \cdots + n_k f_k \in H$. Such an R is said to realize (F, H) (see ([6]), also consult there for possible generalizations for the non-countable situation).

We start with examples of Dedekind domains that are not HFD, such that their overrings are PID.

EXAMPLE 1. Let q be a prime number. Let $H = \{n_1 f_1 + \cdots + n_k f_k \mid q \mid \Sigma_i n_i\}$.

H satisfies (*), as can easily be verified.

Let R be a Dedekind domain that realizes (F, H).

Let $\{p_1, p_2, \cdots\}$ be the non-zero primes of R. In $C(R)$ we have the following equalities:

$$R \equiv p_1^q \equiv p_1^{q-1} p_{kq+1} \quad \text{or} \quad p_1 \equiv p_{kq+1} \quad \text{for } k \geqq 1.$$

$$R \equiv p_i^q \equiv p_i^{q-1} p_{kq+i} \quad \text{or} \quad p_i \equiv p_{kq+i} \quad \text{for } k \geqq 1 \quad \text{and} \quad i \geqq 1.$$

$$R \equiv p_1^{q-i} p_i \equiv p_1^q \quad \text{or} \quad p_1^i \equiv p_i \quad \text{for } i \geqq 1.$$

Consequently, p_1 generates $C(R) = F/K = Z/qZ$, and to each class i of $C(R)$ there belongs some prime, namely p_i.

Localize R at the multiplicative set generated by its prime elements to obtain $T = R_s$ (in fact, as no p_i is a principal ideal, S is void and $T = R$).

$C(T) = C(R) = Z/qZ$, and in T there exist no prime elements. Consequently, every overring T' of T is a localization of T, and the natural epimorphism $C(T) \to C(T')$ is not a monomorphism. Consequently every overring of T is a PID, while T is an HFD iff $q = 2$.

EXAMPLE 2. Another type of example of the same nature can be achieved. Let q be a prime number, let m be a positive integer, and let

$$H = \left\{ n_1 f_1 + \cdots + n_k f_k \mid q^m \mid \left(\sum_{2i \leqq k} n_{2i} - \sum_{2i+1 \leqq k} n_{2i+1} \right) \right\}.$$

H is easily verified to satisfy (*).

Let R be a Dedekind domain that realizes (F, H). Let $\{p_1, p_2, \cdots\}$ be the set of non-zero primes of R. In $C(R)$ we have the following inequalities:

$$R \equiv p_1^{q^m} \equiv p_1^{q^m - 1} p_{2i+1} \quad \text{or} \quad p_1 \equiv p_{2i+1} \quad \text{for } i \geqq 0.$$

$$R \equiv p_1^{q^m} \equiv p_1^{q^m + 1} p_{2i} \quad \text{or} \quad p_1 p_{2i} \equiv R \quad \text{for } i > 0.$$

In particular $p_2 \equiv p_{2i}$ for $i > 0$. Thus, for each prime p in R either $p \equiv p_1$ or else $p \equiv p_2$. Furthermore, $p_1 p_2 \equiv R$, and $p_1^{q^m} \equiv R$. It follows that $C(R) = Z/q^m Z$.

As in the previous example one deduces that:

Every overring of R is a PID, and R is an HFD iff $q = 2$ and $m = 1$.

EXAMPLE 3. Next we provide an example of a Dedekind HFD whose class group is isomorphic to Z_{q^∞}. For this example it will be easier to express H if we denote the elements of F by a double-indexing set $\{f_{ij}\}$ $i, j = 1, 2, \cdots$.

Let

$$H = \left\{ n_{11} f_{11} + \cdots + n_{st} f_{st} \mid q \mid \sum_{i=1}^{t} (n_{1i} \cdots + (-1)^{r+1} q^{-r+1} n_{ri} \cdots + (-1)^{s+1} q^{-s+1} n_{si}) \right\}.$$

A straightforward reasoning yields that H satisfies (*).

Let the Dedekind domain R realize (F, H), let $\{p_{ij}\}$ be its set of non-zero prime ideals (the double indexing is to match that of the $\{f_{ij}\}$). We have the following relations:

$$p_{is} \equiv p_{it} \quad \text{for all } i \geqq 1 \text{ and all pairs of } (s,t), \quad s \geqq 1, \quad t \geqq 1.$$

$$p_{is}^{q^k} \equiv p_{(i+k)s} \quad \text{for all } i \geqq 1 \text{ and all } s \geqq 1 \text{ and all } k \geqq 1.$$

Consequently, $C(R)$ is isomorphic to Z_{q^∞}, and for each pair of prime ideals p_1, p_2 a non-negative integer k exists such that $p_1 \equiv p_2^{q^k}$ or else $p_2 \equiv p_1^{q^k}$ ($p_1 \equiv p_{i1}$ and $p_2 \equiv p_{j1}$ for suitable $i, j \geqq 1$). This ring is an HFD, and every localization of it is an HFD.

The following three examples are of Dedekind domains that are HFD, whose class group is Z, in which prime ideals p exist for which $p \cdot p' \not\equiv R$ for every prime ideal p' in R.

EXAMPLE 4. Let n be a fixed positive integer.

Let $H = \{n_1 f_1 + \cdots + n_k f_k \mid \Sigma_{2i+1 \leq k} n_{2i+1} = n \, \Sigma_{2i \leq k} n_{2i}\}$.

One verifies that H satisfies (*).

Let R be a Dedekind domain that realizes (F, H). The following hold in $C(R)$:

$$R \equiv p_1^n p_2 \equiv p_1^{n-1} p_{2k+1} p_2, \quad \text{whence } p_1 \equiv p_{2k+1} \quad \text{for } k \geqq 0.$$

$$R \equiv p_1^n p_2 \equiv p_1^n p_{2k} \quad \text{whence } p_2 \equiv p_{2k} \quad \text{for } k > 0.$$

p_1 has infinite order in $C(R)$.

Consequently, $C(R)$ is isomorphic to Z, and for each non-zero prime p we have $p \equiv p_1$ or else $p \equiv p_2$. Observe that only if $n = 1$ then for every non-zero prime ideal p there exist a prime ideal p' such that $p \cdot p' \equiv R$.

$L(p_{2k+1}) = 1/2n$, $L(p_{2k}) = 1/2$ give rise to a length function on R.

If R^* is any proper overring of R, then $C(R^*)$ is necessarily 0 or Z/nZ and in both cases R^* is an HFD, while if R^* is a proper localization, then $C(R^*) = 0$.

This example can be generalized as follows:

EXAMPLE 5. Let $H = \{n_1 f_1 + \cdots + n_k f_k \mid s \, \Sigma_{2i \leq k} n_{2i} = t \, \Sigma_{2i+1 \leq k} n_{2i+1}\}$ where (s, t) is a pair of relatively prime positive integers. For the rest of this example, we may assume $s > 1$, $t > 1$.

It is a straightforward argument to verify that H satisfies (*).

Let R denote a Dedekind domain that realizes (F, H).

Let $\{p_i\}$ be its set of non-zero primes. The following hold:

$$R \equiv p_1^s p_2^t \equiv p_1^{s-1} p_2^t p_{2i+1}, \quad \text{whence } p_1 \equiv p_{2i+1} \quad \text{for } i \geqq 0.$$

$$R \equiv p_1^s p_2^t \equiv p_1^s p_2^{t-1} p_{2i}, \quad \text{whence } p_2 \equiv p_{2i} \quad \text{for } i > 0.$$

Let $as + bt = 1$, then $p_1^b p_2^{-a} = I$ is an element in $C(R)$.

$$I^s \equiv p_1^{bs} p_2^{-as} \equiv p_1^{bs} p_2^{-1+bt} \equiv p_1^{bs} p_2^{+bt} p_2^{-1} \equiv (p_1^s p_2^t)^b p_2^{-1} \equiv p_2^{-1}.$$

$$I^t \equiv p_1^{bt} p_2^{-at} \equiv p_1^{1-as} p_2^{-at} \equiv p_1 p_1^{as} p_2^{at} \equiv p_1 (p_1^{-s} p_2^{-t})^a \equiv p_1.$$

Therefore, I generates $C(R)$. Furthermore, $I^k \neq 0$ for every positive integer k, because $nf_1 \notin H$ for every positive integer n, and so $p_1^n \not\equiv R$. Consequently, $C(R) = Z$.

We claim that R is an HFD:

Let $L(p_{2i+1}) = 1/2s$ for $i \geqq 0$, $L(p_{2i}) = 1/2t$ for $i > 0$.

Observe that $p_1^{n_1} \cdots p_k^{n_k} \equiv R$ iff $p_1^u p_2^v$ R where $u = \Sigma_{2i+1 \leqq k} n_{2i+1}$ and $v = \Sigma_{2i \leqq k} n_{2i}$. Thus $ut = vs$, and as $(s, t) = 1$, we have a positive integer w such that $u = ws$ and $v = wt$. Consequently, $p_1^u p_2^v = (p_1^s p_2^t)^w \equiv R$. Whence if $Rr = p_1^{n_1} \cdots p_k^{n_k}$, then $l(r) = w$ is a well-defined length function, and if $w > 1$ then r necessarily decomposes. By Lemma 1.3 it results that T is an HFD.

Remark that in this case proper localizations are all HFD, with class group cyclic of order s or t.

Both in examples 5 and 6, every non-zero prime p satisfies either $p \equiv p_1$ or else $p \equiv p_2$.

EXAMPLE 6. Let $H = \{n_1 f_1 + \cdots + n_k f_k \mid \Sigma_{2i+1 \leqq k} n_{2i+1} = \Sigma_{2i \leqq k} i n_{2i}\}$.

One verifies that H satisfies $(*)$.

Let R be a Dedekind domain that realizes (F, H). Then the following relations hold among its prime ideals $\{p_i\}$:

$$R \equiv p_1^2 p_2 = p_1 p_{2i+1} p_2, \quad \text{whence } p_1 \equiv p_{2i+1} \quad \text{for } i \geqq 0.$$

In $C(R)$, p_1 has infinite order.

$$R \equiv p_1^j p_{2j} \quad \text{whence } p_{2j} \equiv p_1^{-j} \quad \text{for} \quad j > 0.$$

Consequently, $C(R)$ is an infinite group with p_1 as a generator.

CLAIM. *R is an* HFD.

Let $Rr = p_1^{n_1} \cdots p_k^{n_k}$, with non-negative integers $n_1, \cdots, n_k$. Then $\Sigma_{2i+1 \leqq k} n_{2i+1} = \Sigma_{2j \leqq k^j} n_{2j}$. Let $n_{2j} \neq 0$ for some j. Then there exists $0 \leqq n'_{2i+1} \leqq n_{2i+1}$ such that $\Sigma_{2i+1 \leqq k} n'_{2i+1} = j$. Set $n''_{2i+1} = n_{2i+1} - n'_{2i+1}$, then

$$\left(\prod_{2i+1 \leqq k} p_{2i+1}^{n'_{2i+1}} \cdot p_{2j}\right) \cdot \left(\prod_{2i+1 \leqq k} p_{2i+1}^{n''_{2i+1}} \cdot \prod_{\substack{2j \leqq k \\ i \neq j}} p_{2i}^{n_{2i}} \cdot p_{2j}^{n_{2j}-1}\right) = Rr$$

yields a decomposition for R. Defining $l(r) = \Sigma_{2i \leqq k} n_{2i}$ will provide a well-defined length function such that $l(r) = 1$ iff r is indecomposable.

By Lemma 1.3 it results that R is an HFD as stated.

For this ring R, every overring S has the property that in $C(S)$, there exists a prime ideal in every class of $C(S)$. In particular, except when $C(S) = (0)$ and $Z/2Z$, it is not an HFD.

Remark that in this case the length function does not arise from a function L on primes whose values are positive rational integers, because $L(p_1^j p_{2j})$ has to be 1 for every j, that is $jL(p_1) + L(p_{2j}) = 1$, and with rational integers, these equalities imply $L(p_1) = 0$, $L(p_{2j}) = 1$ for all positive integers j.

In example 5 we have seen how to obtain a Dedekind HFD with cyclic (finite) class group. Another way to get a Dedekind HFD with cyclic p-group as its class group is described in the following example.

EXAMPLE 7. Let k be a non-perfect field of characteristic $q \neq 0$, and let K be its separable closure. Let $a(x)$ be any irreducible polynomial over K, then $\|a(x)\| = q^n$ for some non-negative integer n. Let $\|a(x)\| \neq 1$, that is $n \geqq 1$. Then

$$R = K\left[\frac{1}{a(x)}, \cdots, \frac{x^{q^n-1}}{a(x)}\right] \text{ is a Dedekind domain with } C(R) = Z/q^nZ,$$

and R is an HFD [12].

Observe that n can be chosen arbitrarily.

Thus, this provides examples of Dedekind domains with class-group cyclic of order q^n, for every prime q, and these Dedekind domains are all HFD. Let p be a generating prime for $C(R)$ and denote by g its class. The result follows since the prime ideals are scattered in the $(1+N)$ classes: g, g^q, $g^{q^{n-1}}$, 1.

In example 3 we have obtained Dedekind HFD's whose class groups were the divisible indecomposable torsion groups. Next we study the divisible indecomposable torsion free case.

EXAMPLE 8. We denote the elements of F by $g_1, \cdots, g_m, \cdots, f_1, \cdots, f_n, \cdots$. Let

$$H = \left\{ \sum_{i=1}^{h} m_i g_i + \sum_{j=1}^{k} n_j f_j \,\middle|\, \sum_{i=1}^{h} m_i = \sum_{j=1}^{k} n_j j! \right\}.$$

One easily verifies that H satisfies (*).

Let R be a Dedekind domain that realizes (F, H). Let $\{q_i, p_j\}$ be the prime ideals of R, where the q_i correspond to g_i and p_j to f_j. Then the following relations among the prime ideals hold:

(i) $q_1 \equiv q_i$ for every i, since both $q_1 p_1$ and $q_i p_1$ are principal ideals.

(ii) $q_1^{k!} p_k \equiv R$ for each k, whence in $C(R)$, q_1 is divisible by every integer.

Furthermore, $C(R)$ itself is a divisible group.

(iii) For positive integers, $m_1, \cdots, m_k$, $n_1, \cdots, n_k$, $q_1^{m_1} \cdots q_h^{m_h} p_1^{n_1} \cdots p_k^{n_k}$ is a principal ideal iff $\Sigma_{i=1}^{h} m_i = \Sigma_{j=1}^{k} n_j j!$. In particular, q_1 is an element of infinite order, whence $C(R)$ is isomorphic to the additive group of the rational integers (Q).

If we let $L(q_i) = 0$ for each $i \geqq 1$ and $L(p_j) = 1$ for each $j \geqq 1$, then the induced function $l(x) = n_1 + \cdots + n_k$ on the elements x of R such that $x \neq 0$, $Rx \neq P$, $Rx = q_1^{m_n} \cdots q_n^{m_n} p_1^{n_1} \cdots p_k^{n_k}$ is a length function, whence R is an HFD.

Thus R is an HFD whose class group is isomorphic to Q.

We have provided so far examples of Dedekinds HFD's whose class group is (i) cyclic group (finite or infinite), (ii) Z_{q^∞} for every prime q, and (iii) Q.

In the next example we'll suggest a way of building up a Dedekind domain R whose class group is a countable direct sum of groups $\{G_i\}$, such that R is an HFD.

Example 9. We denote the elements of F by $\{f_{ij}\}$. We consider $F_k = \{f_{ik}\}$, and we let H_k be a subset of F_k so that the ring R_k that realizes (F_k, H_k) will be an HFD with G_k as its class group, where G_k is either a cyclic group, or Z_{q^∞}, or Q.

Let $H = U_k H_k$, then H satisfies (*) and one verifies that R is an HFD whose class group is the direct sum of the G_i's. Note that a similar construction leads to a similar result for the finite direct sum of G_i's.

In particular, one can obtain an HFD whose class group is a direct sum of a countably generated free group and a countably generated elementary 2-group. In this case one can easily verify that we can still get an HFD upon imposing the extra condition for every prime p there exists a prime q so that $pq \equiv R$.

There remains still to verify whether:

Problem A. Is every abelian group the class group of a Dedekind HFD?

As one observes, most examples were of Dedekind domains. The only other Krull type examples are those where the class group is $Z/2Z$.

Naturally there arises the question:

Problem B. Do there exist Krull HFD's that are not Dedekind domains, whose class group contains more than 2 elements?

We end this section with the construction of a Dedkind domain R and a function L on its maximal primes into Q that induces the function l on $S = \{x \mid x \neq 0, Rx \neq R\}$. The function l naturally satisfies $l(xy) = l(x) + l(y)$ for $x, y \in S$; furthermore $l : S \to Z^+$ and if $l(r) = 1$ for $r \in S$, then r is irreducible.

However, the converse does not hold, that is, there are irreducible elements $r \in R$ for which $l(r) \neq 1$. This ring is not an HFD. Compare this example with Theorem 3'.3.

EXAMPLE 10. Start with a non-splittable set, say $\{3, 5, 7, 105\}$. Define

$$H = \{n_1 f_1 + \cdots + n_k f_k \mid \Sigma(n_{4i}/105 + n_{4i+1}/3 + n_{4i+2}/5 + n_{4i+3}/7) \in Z^+\},$$

then H satisfies (*), it has prime ideals p_1, p_2, p_3, p_4 such that $p_1 \equiv p_4^{35}$, $p_2 \equiv p_4^{21}$, $p_3 \equiv p_4^{15}$, $p_4^{105} \equiv R$, and every prime p belongs to the class of some of these p_i.

The ideal $p_1^2 p_2^3 p_3^5 p_4^2$ is a principal ideal, as $\frac{2}{3} + \frac{3}{5} + \frac{5}{7} + \frac{2}{105} = 2$.

As $C(R)$ is cyclic, and the expression $\frac{2}{3} + \frac{3}{5} + \frac{5}{7} + \frac{2}{105} = 2$ does not decompose to subsums that add up to one each, it follows that $p_1^2 p_2^3 p_3^5 p_4^2 = Rx$, where x is an irreducible element. Let x_1, x_2, x_3, x_4 be the irreducible elements that satisfy $p_1^3 \equiv Rx_1$, $p_2^5 \equiv Rx_2$, $p_3^7 \equiv Rx_3$, $p_4^{105} = Rx_4$, we have: $Rx^{105} = Rx_1^{70} x_2^{63} x_3^{75} x_4^2$ whence we get a decomposition of x^{105} on one hand into 105 irreducible terms, while on the other hand we get $70 + 63 + 75 + 2 = 210$ terms. Therefore, R is not an HFD.

The function l induced by L achieves the following values on the above irreducible elements: $l(x_1) = l(x_2) = l(x_3) = l(x_4) = 1$, and $l(x) = 2$.

Notice that $C(R)$ is cyclic, generated by p_4, and for every prime p, $p \equiv p_4^m$ with $m \mid C(R)$.

REFERENCES

1. M. Bass, *Algebraic K-theory*, Benjamin Inc., 1968.
2. L. Carlitz, *A characterization of algebraic number field with class number two*, Proc. Amer. Math. Soc. **11** (1960), 391–392.
3. L. Claborn, *Specified relations in the ideal group*, Michigan Math. J. **15** (1960), 249–255.
4. L. Claborn, *Every abelian group is a class group*, Pacific J. Math. **18** (1966), 219–222.
5. E. D. Davis, *Overrings of commutative rings II*, Trans. Amer. Math. Soc. **110** (1964), 196–212.
6. R. M. Fossum, *The Divisor Class Group of a Krull Domain*, Springer-Verlag, 1973.
7. R. Gilmer and J. Ohm, *Integral domains with quotient overrings*, Math. Ann. **153** (1964), 813–818.
8. O. Goldman, *On a special class of Dedekind domains*, Topology 3 Suppl. **1** (1964), 113–118.
9. W. Narkiewicz, *Some unsolved problems*, Bull. Soc. Math. France **25** (1971), 159–164.
10. B. Wajnryb and A. Zaks, *On the flat overrings of an integral domain*, Glasgow Math. J. **12** (1971), 162–165.
11. A. Zaks, *Half-factorial domains*, Bull. Amer. Math. Soc. **82** (1976), 721–724.
12. A. Zaks, *Dedekind k-subalgebras of k(x)*, Com. Algebra **5** (1977), 347–364.

DEPARTMENT OF MATHEMATICS
TECHNION — ISRAEL INSTITUTE OF TECHNOLOGY
HAIFA, ISRAEL