Math 531 Tom Tucker

How can we identify a DVR? The following will help.

A couple remarks first:
1. If $I$ and $J$ are principal then so is $IJ$. In particular, any power of
a principal ideal is principal.
2. Notation: for any ideal $I$ of $R$, we say $I^0 = R$.

**Proposition 5.1.** Let $R$ be a Noetherian local domain of dimension 1
with maximal ideal $\mathcal{M}$ and with $R/\mathcal{M} = k$ its residue field. Then the
following are equivalent

1. $R$ is a DVR;
2. $R$ is integrally closed;
3. $\mathcal{M}$ is principal;
4. there is some $\pi \in R$ such that every element $a \in R$ can be written
   uniquely as $u \pi^n$ for some unit $u$ and some integer $n \geq 0$.
5. every nonzero ideal is a power of $\mathcal{M}$;

**Proof.** (1 $\Rightarrow$ 2) Suppose that $b \in K \setminus R$. Then $v(b) < 0$, so for any
monic polynomial in $b$ with coefficients in $R$, we have

$$v(b^n + a_n b^{n-1} + \cdots + a_0) = v(b^n) < 0,$$

which means that $b^n + a_n b^{n-1} + \cdots + a_0 \neq 0$.

(2 $\Rightarrow$ 3) Let $a \in \mathcal{M}$. There is some $n$ for which $\mathcal{M}^n \subset (a)$ (by “Poor
Man’s Factorization” in Noetherian rings) but $\mathcal{M}^{n-1}$ is not contained
in $(a)$ (note $n-1$ could be zero). Let $b \in \mathcal{M}^{n-1} \setminus (a)$ and let $x = a/b$. We
can show that $\mathcal{M} = Rx$. This is equivalent to showing that $x^{-1} \mathcal{M} = R$.

Note that since $(b)$ is not in $(a)$, $b/a = x^{-1}$ cannot be in $R$. Hence, it
cannot be integral over $R$. By Cayley-Hamilton, $x^{-1} \mathcal{M} \neq \mathcal{M}$ since $\mathcal{M}$
is finitely generated as an $R$-module and $x^{-1} \notin R$ and $R$ is integrally
closed. Since $x^{-1} \mathcal{M}$ is an $R$-module and $x^{-1} \mathcal{M} \subset R$ (this follows from
the fact that $b \mathcal{M} \subset \mathcal{M}^n \subset (a)$), this means that $x^{-1} \mathcal{M}$ is an ideal of
$R$ not contained in $\mathcal{M}$. So $x^{-1} \mathcal{M} = R$, as desired.

(3 $\Rightarrow$ 4) Let $\pi$ generate $\mathcal{M}$. Now, let $a \in R$. We define $w(a)$ to be
the smallest $n$ for which $\mathcal{M}^n \subset Ra$; such an $n$ exists by “Poor
Man’s Factorization” in Noetherian rings. We will show by induction that
that $a$ can be written as $u \pi^{w(a)}$ for some unit $u$. The case $w(a) = 0$ is
trivial, since $w(a) = 0$ means $a$ is a unit. If $w(a) \geq 1$, then $a \in \mathcal{M}$.

Then we can write $a = \pi b$ for some $b$. Since, any element in $\mathcal{M}^n$, which
is simply the set of $z \pi^n$ for $z \in R$, can be written as $xa$ for some $x \in R$,
any element $z \pi^{w(a)-1}$ in $\mathcal{M}^{w(a)-1}$ can be written as $xb$ for that same
$x$. Hence $w(b) \leq w(a) - 1$. By the same reasoning, $w(b) \geq w(a) - 1$.

Hence $w(b) = w(a) - 1$. So we can write $b$ uniquely as $u \pi^{w(b)}$ for some
unit $u$, which gives $a = u \pi^{w(a)}$ uniquely.
(4 ⇒ 5) Let \( I \) be an ideal of \( R \). Since \( I \) is finitely generated, it has generators \( m_1, \ldots, m_n \) which can all be written as \( u_i \pi_i^{t_i} \). Then the \( i \) for which \( t_i \) is smallest will generate \( I \) from above.

(5 ⇒ 1) Let \( a \in R \). Then \( Ra = M^n \) for some unique \( n \). Letting \( v(a) = n \) gives the desired valuation.

\[ \square \]

Example 5.2. The ideal \( P \) generated by 2 and \( \sqrt{5} - 5 \) in \( \mathbb{Z}[\sqrt{5}] \) is prime but \( \mathbb{Z}[\sqrt{5}] \setminus P \) is not a DVR. More on this later.

Recall, a Dedekind domain is a Noetherian domain \( R \) such that \( R \) is a DVR for every nonzero prime \( P \) of \( R \). The ideal structure is a bit more complicated than that of a DVR. Recall that in any noetherian ring \( R \) for every ideal \( I \) we can write \( \prod_{i=1}^{n} P_i \subset I \) with \( P_i \supset I \). We’ll prove that in a Dedekind domain we can write get an inequality and get it uniquely.

One more thing: we’ll want to work in Noetherian domains of (Krull) dimension 1 more generally, as you’ll see later. So we’ll try to state results for them when possible.

To understand how to factorize an ideal \( I \), we’ll want to understand \( R/I \). To help us with this we’ll want the Chinese remainder theorem.

The Chinese remainder theorem really consists of writing 1 in a lot of different ways. Let’s prove the following easy Lemma.

Lemma 5.3. Let \( I \) and \( J \) be ideals in \( R \). Suppose that \( I + J = 1 \). Then

1. \( I \cap J = IJ \); and
2. for any positive integers \( m, n \), we have \( I^m + J^n = 1 \).

Proof. Since \( I + J = 1 \), we can write \( a + b = 1 \) for \( a \in I \) and \( b \in J \). Now 1. follows from the fact that for if \( x \in I \cap J \), then \( x = (a + b)x = ax + bx \in IJ \), so \( I \cap J \subset IJ \). The reverse inclusion \( IJ \cup I \cap J \) is obvious. To prove 2., we simply write \( (a + b)^2 = 1 \), and note that the expansion of \( (a + b)^2(\text{m+n}) \) consists entirely of elements in either \( I^{m+n} \subset I^m \) or \( J^{m+n} \subset J^n \).  

\[ \square \]

Lemma 5.4. Let \( I \) and \( J \) be ideals of \( R \) and suppose that \( I + J = 1 \). Then the natural map

\[ \phi : R \longrightarrow R/I \oplus R/J \]

is surjective with kernel \( IJ \).

Proof. The kernel is \( I \cap J \) which equals \( IJ \) from the Lemma above. Now, to see that it is surjective, write \( a + b = 1 \) with \( a \in I \) and \( b \in J \).
Then \( b = 1 - a \) and \( \phi(b) = (1, 0) \) and \( \phi(a) = (0, 1) \). Since \( \phi(R) \) is clearly a \( R/I \oplus R/J \) module and \( R/I \oplus R/J \) is generated by \( (1, 0) \) and \( (0, 1) \) as an \( R/I \oplus R/J \) module, \( \phi \) must be surjective. □

**Lemma 5.5.** If \( I + J_1 = 1 \) and \( I + J_2 = 1 \), then \( I + J_1J_2 = 1 \).

**Proof.** Writing \( a + b = 1 \) for \( a \in I \) and \( b \in J_1 \) and writing \( a' + b' = 1 \) for \( a \in I \) and \( b \in J_2 \), we see that
\[
1 = (a + b)(a' + b') = aa' + ab' + ba' + bb' \subseteq I + J_1J_2.
\]

□

**Proposition 5.6.** (*Chinese Remainder theorem*) Let \( R \) be a ring and let \( I_1, \ldots, I_n \) be a set of ideals of \( R \) such that \( I_j + I_k = 1 \) for \( j \neq k \). Then the natural map
\[
R \longrightarrow \bigoplus_{j=1}^{n} R/I_j
\]
is surjective with kernel \( I_1 \cdots I_n \).

**Proof.** We proceed by induction on \( n \). If \( n = 1 \), then the result is obvious. Otherwise, write \( I := I_1 \) and \( J := I_2 \cdots I_n \). Applying the lemmas above, \( I + J = 1 \) and the natural map
\[
R \longrightarrow R/I \oplus R/J
\]
is surjective with kernel \( IJ \). Since the natural map
\[
R \longrightarrow \bigoplus_{j=2}^{n} R/I_j
\]
is surjective with kernel \( I_2 \cdots I_n \) by the inductive hypothesis, we are done. □