LECTURE 17: CHARACTERIZATION OF NORMAL RINGS; DEDEKIND RINGS

Theorem 0.1. *A ring R is a DVR if and ony if it is a local one-dimensional Noetherian normal domain.*

Proof. The forward inclusion is easy: we know that a DVR is local normal domain (since it is a valuation ring). The maximal ideal of R is a principal ideal, so it has height one.

For the converse, write $K = Q(R)$ and $\mathfrak{m}$ for the maximal ideal of R. According to Nakayama, $\mathfrak{m} \neq \mathfrak{m}^2$ and so we can choose an element $x \in \mathfrak{m} \setminus \mathfrak{m}^2$. Since R has only two prime ideals, 0 and $\mathfrak{m}$, we conclude that $\mathfrak{m}$ is an associated prime of R/xR, that is there exists $y \in R$ such that $\mathfrak{m} = \mathrm{Ann}_R(\hat{y}) = (Rx :_R y)$. Let $a = y/x \in K$ and note that $\mathfrak{m} \cdot a \subseteq R$, which implies that $a \in \mathfrak{m}^{-1}$. But $a \notin R$ and this shows that $R \subsetneq \mathfrak{m}^{-1}$.

Note that $\mathfrak{m}\mathfrak{m}^{-1}$ is an ideal of R containing $\mathfrak{m}$. If $\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{m}$ then $a\mathfrak{m} \subseteq \mathfrak{m}$ and so a is integral over R (by the determinantal trick) and so $a \in R$ since R is normal. This is false, so $\mathfrak{m}\mathfrak{m}^{-1} = R$. This implies that $\mathfrak{m}$ is an invertible ideal of R and hence it is principal because it is prime. Since R is Noetherian and $\mathfrak{m}$ is principal, we have that R is DVR.

□

Theorem 0.2. *Let R be a Noetherian normal domain. Then all the associated primes P of principal ideals in R have height one and R_P is DVR. Moreover, $R = \cap_{\mathrm{ht}P=1} R_P$.*

In fact, in a Noetherian domain, if all the associated primes P of principal ideals in R have height one, then $R = \cap_{\mathrm{ht}P=1} R_P$.

Proof. Let $I = Rx$ be a principal ideal of R and P an associated prime of I. There exists $y \in R$ such that $P = (Rx :_R y)$. R_P is normal Noetherian domain as well. Let $a = y/x$ be an element of $Q(R)$. Now, $a \notin R_P$ and $aPR_P \subset R_P$ which implies that either $aPR_P \subseteq PR_P$, and so a is integral over R_P and hence in R_P (false), or $aPR_P = R_P$ which proves that PR_P is an invertible (prime) ideal of R_P. As before, this implies that PR_P is principal and so R_P is a DVR. In particular P has height one.

Let $a = y/x \in Q(R)$ such that $y/x \in R_P$ for all P prime ideals of height 1.

Consider $I = Rx = Q_1 \cap \cdots \cap Q_n$ a primary decomposition of I. Let $P_i = Rad(Q_i)$, and note that we proved that P_i have all height one since they are associated primes of I.

But then, by hypothesis, $y \in xR_{P_i} \cap R = Q_i$, since all P_i are minimal over x by height reasons.

Therefore $y \in Q_1 \cap \cdots \cap Q_n = I = Rx$ and hence $a = y/x \in R$. □

The following is an important characterization of normal rings.

Corollary 0.3. *A Noetherian domain R is normal if and only if*

(1) *for all prime ideals P of R of height 1, R_P is DVR.*
(2) *all associated prime ideals of principal nonzero ideals have height 1.*

Proof. One direction was already proven. We can see that we have seen that (2) implies that $R = \cap_{\mathrm{ht}P=1} R_P$. But R_P is a normal ring with $Q(R_P) = Q(R)$, and so R is normal as well.

□

The following result will introduce the concept of Dedekind rings.

Theorem 0.4. *Let R be a domain. The following assertions are equivalent:*

(1) *Every nonzero ideal of R is invertible.*
(2) *R is normal Noetherian domain of dimension 1, or a field.*
(3) *Every nonzero ideal of R is a product of finitely many prime ideals of R.*
Moreover, the representation in (3) unique.

Proof. (1) implies (2). Since an invertible ideal is finitely generated we get that R is Noetherian. Assume that R is not a field. Now, let P be a nonzero prime ideal. Since P is invertible we get that $\mathrm{ht}(P) = 1$ and R_P is DVR. This proves that R is one dimensional. The fact that every localization is a normal proves that R is normal as well.

(2) implies (1). R is Noetherian so every ideal is finitely generated. Let I be a nonzero fractional ideal of R. Let P be a maximal ideal of R containing I. Since $\mathrm{ht}(P) = 1$ we get that R_P is DVR, and so IR_P is cyclic. therefore I is invertible.

(1) implies that (3). First note that R is Noetherian. Assume that we proved the statement for all ideals J strictly containing I. We can assume $I \neq R$, and take $I \subseteq \mathfrak{m}$ in a maximal ideal. Therefore, $I \subsetneq I\mathfrak{m}^{-1} \subseteq R$.

The first inclusion is strict since otherwise $I\mathfrak{m} = I$ and Nakayama lemma implies that there exists $r \in I$ such that $(1 + r)\mathfrak{m} = 0$. This is impossible since R is domain.

But then $I \subseteq I\mathfrak{m}^{-1} = P_1 \cdots P_k$ gives $I = P_1 \cdots P_k\mathfrak{m}$.

We will not prove (3) implies (1), and the uniqueness here.

□

Definition 0.5. *A domain satisfying the conditions in the above theorem is called a* Dedekind ring *or* Dedekind domain.

For an R-module, let $M^\vee = \mathrm{Hom}_R(M, R)$.

Theorem 0.6. *Let R be a domain and M a finitely generated R-module.*

Then M is locally free of rank 1 if and only if the natural map $M \otimes M^\vee \simeq R$ is an isomorphism.

Proof. If M is locally free of rank 1, let P be a maximal ideal of R. It is enough to check that when we localize at P, the map $M_P \otimes (M^\vee)_P \simeq R_P$ is an isomophism. Since $(M^\vee)_P \simeq (M_P)^\vee$ and since $M_P \simeq R_P$ this is clear now.

Conversely, localize the isomorphism $M \otimes M^\vee \simeq R$ at P. We want to show that $M_P \simeq R_P$, so it is enough to assume that R is local with maximal ideal $\mathfrak{m}$. Tensor with $R/\mathfrak{m}$, and note that we are in the vector space case now, so we conclude that $M/\mathfrak{m}M$ is 1-dimensional, and so M is cyclic, by NAK. So, $M = R/I$ and similarly, $M^\vee = R/J$, and so the original isomorphism becomes $R/(I + J) \simeq R$, so $I + J = 0$, which gives $I = 0$, and the $M = R$.

□

Proposition 0.7. *Let R be a domain and M a finitely generated R-module that is locally free of rank* 1*. Then M is isomorphic to a fractional ideal.*

Proof. Since M is locally free of rank one and finitely generated, then it is projective. So, M is flat and then by tensoring $R \to K$ with M, we get $M \to M \otimes_R K = (R \setminus \{0\}^{-1} M \simeq K$ is an injection. This finishes the proof.

□

Proposition 0.8. *Let I, J be two invertible fractional ideals. Then the natural map $I \otimes_R J \to IJ$ is an isomorphism and moreover $I^{-1} \cdot J \to \mathrm{Hom}_R(I, J)$ by sending $a \in I^{-1}J$ to the map $\phi_a(x) = ax$, for all $x \in I$. In particular, $I^{-1} \simeq I^\vee$.*

Proof. For the first pat, note that I, J are locally free of rank one so the first isomoprhism can be checked locally, at every P prime ideal of R. But in that case, the isomorphism is trivial.

For the second part, note that there exists $u \in R$, nonzero, such that $uJ \subset R$, and so $J \simeq uJ$. Similarly, $I^{-1}J \simeq I^{-1}uJ$, so we can assume that J is a fractional ideal contained in R.

Note that $I^{-1}J = (J :_K I)$. Indeed clearly, $I^{-1}J \subseteq (J :_K I)$. If $xI \subset J$ then $xI \cdot I^{-1} \subseteq I^{-1} \cdot J$ and so $x \in I^{-1}J$, since $R = II^{-1}$.

Clearly, the map $a \to \phi_a$ is R-linear and $\phi_a = 0$ implies $a = 0$, so it is also injective.

For surjectivity, let $\phi \in \mathrm{Hom}_R(I, J)$. Since $J \subset R$, we have $\phi \in \mathrm{Hom}_R(I, R)$, and hence there exists $k \in K$ such that $\phi(t) = kt$, for all $t \in I$. Since $\mathrm{Im}(\phi) \subseteq J$ we see that $kt \in J$ for all $t \in I$, which proves that $k \in (J :_K I)$ and $\phi = \phi_k$.

□

One can consider the set of all fractional invertible ideals in a domain R. The multiplication of fractional ideals induces a multiplication such that this set becomes an Abelian group G, denoted by $C(R)$. Consider the subgroup H of nonzero principal fractional ideals of R. The subgroup G/H is called the **Picard group** of R and it is denoted by $Pic(R)$. It represents an important notion not only in commmutative algebra, but also

in number theory and algebraic geometry. When R is Dedekind, this object is called the **ideal class group** of R and it is denoted by $Cl(R)$.

Theorem 0.9. *Let R be a Noetherian domain. Then the Picard group of R is isomorphic to the Abelian group of isomorphism classes of finitely generated R-modules which are locally free of rank one, with the group operation given by $\otimes_R$.*

Corollary 0.10. *Let R Noetherian domain. The group $C(R)$ is generated by invertible ideals of R.*

Proof. Every invertible fractional ideal I admits $u \in R$ such that $uI \subseteq R$. But then $I = (uI) \cdot (u)^{-1}$, a product of invertible ideals in R.

□

Theorem 0.11. *Let R be a Dedekind domain. Then $C(R)$ is a free Abelian group generated by the maximal ideal of R.*

Proof. This follows at since since every fractional ideal in a Dedekind domain is a unique product of nonzero prime ideals. These prime ideals are exactly the maximal ideals in D.

□

Proposition 0.12. *Let R be a Dedekind ring. Then $Cl(R) = 0$ if and only if R is PID.*

Proof. Let I be a nonzero ideal in R. Then I is fractional, and so it is invertible. But $Cl(R) = 0$ hence $I = Rx$ for some $x \in K$, x nonzero.

But $I \subset R$ and so $x \in R$. Hence I is a principal ideal of R.

□

Theorem 0.13. *Let R be a Dedekind ring. Then R is PID if and only if R is UFD.*

Proof. Assume that R is a Dedekind domain and UFD. Then every nonzero prime ideal is of height one so it is principal (due to the UFD property). But every ideal is product of primes, so every ideal is principal. □

Definition 0.14. *Let I be an ideal of R. We say that I is of pure codimension* 1 *if all its associated primes have height* 1.

Theorem 0.15. *Let R Noetherian domain such that R_P is UFD, for all maximal ideals P in R. Then an ideal I of R is locally free of rank one if and only if I has pure codimension* 1.

Moreover, $C(R)$ is generated as a free Abelian group by primes of codimension 1.

Proof. This is Theorem 11.8 in Eisenbud.

□

Let R be a Noetherian normal domain with $K = Q(R)$. For every $P \in \mathrm{Spec}(R)$ of height 1, we have that R_P is DVR, and so we have an additive valuation $v_P : R_P \to \mathbb{Z}$.

For $f \in K$, nonzero, we can therefore define $v_P(f)$, for all height one primes P.

Denote $Div(R)$ the free Abelian group generated by prime ideals of height one. An element of this group is called a divisor on R, and it is of the form $n_1[P_1] + \cdots + n_k[P_k]$, where $n_1, \ldots, n_k$ are integers and $P_1, \ldots, P_k$ are height one primes.

Lemma 0.16. *For $f \in K$, nonzero, we have that $v_P(f) = 0$ for all but finitely many height one primes P.*

Proof. Let $f = a/b$ with a, b nonzero. Note that $v_P(f) = 0$ is equivalent to f a unit in R_P which means that a is not in P. But the set of prime ideals of height one containing a is finite because it is of same cardinality to the set of minimal primes in R/aR, a finite set.

□

Now define a principal divisor by $div(f) = \sum_{\mathrm{ht}(P)=1} v_P(f)[P]$, which is well defined by the above result. Denote by $Prin(R)$ the subgroup generated by all principal divisors on R.

By definition, $DvC(R) = Div(R)/Prin(R)$ is called the divisor class group of R.

Theorem 0.17. *Let R be a Noetherian domain. There is group homomorphism $\phi : C(R) \to Div(R)$ such that*

$$\phi(I) = \sum_{\mathrm{ht}(P)=1} \lambda(R_P/I_P) \cdot [P],$$

for any ideal invertible I of R. This map induces a map

$$Pic(R) \to DvC(R).$$

Both maps are injective if R is Noetherian normal domain.

Proof. See Theorem 11.10 and Proposition 11.11 in Eisenbud. □

In fact, if R is regular $Pic(R)$ is isomorphic to $DvC(R)$. Moreover, a Noetherian normal domain has $DvC(R) = 0$ if and only if R is UFD.

Proposition 0.18. *Let R be a Noetherian normal domain. Let P be a prime of height one. Then $[P] = div(y)$ in $Div(R)$ if and only if $P = (y)$.*

Proof. $[P] = div(y)$ implies that $v_P(y) = 1$ and so $y \in PR_P$ and $(y) = PR_P$. For any other prime Q of height 1, we have $v_Q(y) = 0$ and so $y \in \cap_{Q,\mathrm{height}(Q)=1} R_Q = R$, because R is normal. Therefore, $y \in R \cap PR_P = P$.

Let x be an element of P. Then $v_P(x) \geq 1$ and $v_Q(x) \geq 0$, for all prime ideals Q of height 1. So $v_Q(x/y) = v_Q(x) - v_Q(y) \geq 0$ for all prime Q of height 1. So $x/y \in \cap_Q R_Q = R$. And this gives $x \in (y)$. Hence $P = (y)$.

□

Corollary 0.19. *Let R be a Noetherian domain. Then R is UFD if and only if R is normal and $DvC(R) = 0$.*

Example 0.20.

(1) Let D a square free integer. The integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{D}) = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \omega$, where $\omega = \sqrt{D}$ if $D \equiv 2, 3$ modulo 4 and $\omega = \frac{1+\sqrt{D}}{2}$, if $D \equiv 1$ modulo 4. This ring is Dedekind. (Show it).

(2) Show that $[(y, z)]$ is an element of order two in $DvC(R)$, where $R = \frac{\mathbb{C}[X,Y,Z]}{(XY-Z^2)}$. and x, y, z denote the classes of X, Y, Z in R.

Let $P = (y, z)$. This is a prime ideal of R of height 1. Consider $div(y)$. If Q is a height one prime containing y then it must contain $z^2 = xy$ and so $z \in Q$.

So, $(y,z) \subseteq Q$ and since both have height one we must have equality. This shows that the only prime of height 1 containing y is P.

But in R_P y is in the square of the maximal ideal so $v_P(y) = 2$. Hence $div(y) = 2[P]$ and so in $DvC(R)$ we have $2[P] = 0$.

According to Proposition refprinc, if $[P] = 0$ in $DvC(R)$, then P is principal. But the maximal ideal of R has three minimal generators x, y, z. If P is principal, then it would imply that the maximal ideal of R is generated by two elements, impossible.

Theorem 0.21 (Nagata)**.** *Let R be a Noetherian normal domain. Let Q be a prime ideal of height 1 and $g \in Q$ such that Q is the only prime ideal of height 1 containing g.*

Then there exists a exact sequence of Abelian groups :

$$\mathbb{Z} \to DvC(R) \to DvC(R_g) \to 0$$

where the first map sends $1 \to [Q]$.

Proof. The right most non-trivial map is obtained as follows: at the level of divisors, send $[P]$ to itself for any prime of height 1 different than Q. And send $[Q]$ to zero. The hypothesis of the theorem implies that this map induces a map at the level of the diviors class groups. It is clear from the definition that its kernel is generated by $[Q]$, which proves the last assertion.

□

Example 0.22. Let $R = \frac{\mathbb{C}[X,Y,Z]}{(XY-Z^2)}$. We will prove that $DvC(R) = \mathbb{Z}_2$. Let x, y, z denote the classes of X, Y, Z in R.

Then Nagata's Theorem applies with $g = y$ and $Q = (y, z)$. Since $R_y = \mathbb{C}[y, y^{-1}, z]$ is UFD, then $DvC(R_y) = 0$. And so $\mathbb{Z} \to DvC(R) \to 0$ shows that $DvC(R) = \mathbb{Z}_2$ since $2 \cdot [(y, z)] = 0$.

Remark 0.23. (1) Let R be a Noetherian normal domain. Then for any $r \in R$, nonzero, the primary decomposition of the ideal it generates has the form $(r) = P_1^{(n_1)} \cap \cdots \cap P_k^{(n_k)}$, for some $P_1, \ldots, P_k$ height one prime ideals of R and $n_1, \ldots, n_k$ positive integers. This is so because principal ideals have no embedded primes. In

R_P all P-primary ideals have the form $P^m R_P$, for some m, and $P^{(m)} = P^m R_P \cap R$. With the notations above, $div(r) = \sum_i n_i[P_i]$.

More generally, for similar reasons, for an ideal I of pure height 1, the primary decomposition of I has the form $I = Q_1^{(n_1)} \cap \cdots \cap Q_k^{(n_k)}$, for some $Q_1, \ldots, Q_k$ height one prime ideals of R and $n_1, \ldots, n_k$ positive integers. Then one can associate the divisor $\sum_i n_i[Q_i]$ to I, denoted here by $div(I)$.

So the divisor class group of R measures roughly how many height one ideals in R are not principal.

One can prove that if I, J are two ideals of pure height one, then $div(I) = div(J)$ in $DvC(R)$ if and only if I, J are isomorphic R-modules if and only if there exist $r, s \in R$ such that $rI = sJ$.

(2) It is common to see the divisor class group of R denoted by $Cl(R)$ instead of $DvC(R)$.