LECTURE 16

1. Properties of UFDs and affine domains

Theorem 1.1. *A Noetherian domain R is an UDF if and only if every height one prime ideal of R is principal.*

Proof. Suppose that R is UFD. Let P a height one prime ideal of R and choose $0 \neq x \in P$. We can write $x = f_1 \cdots f_n$ where f_i are all prime elements, for $i = 1, \dots, n$. Then $x \in P$ implies that, for some i, $(f_i) \subseteq P$. But (f_i) is a prime ideal of height one, so $P = (f_i)$.

Conversely, we need to show that every irreducible element is prime. Let f be an irreducible element and consider a minimal prime P over (f). Then by Krull's PIT we have that $\mathrm{ht}(P) = 1$, and so there exists $x \in P$ such that $P = (x)$. But then, $f = yx$ for some $y \in R$. But f is irreducible and so y is a unit. Hence $P = (f)$ and so f is a prime element.

□

Lemma 1.2. *Let $A \subseteq R$ be an integral extension of domains with A UFD. Let P be a prime ideal in R of height one. The $P \cap A$ is principal.*

Proof. Since A is UFD, then A is normal, so we can apply the Going-Down Theorem. Hence $1 = \mathrm{ht}(P) = \mathrm{ht}(P \cap A)$.

But A is UFD so $P \cap A$ must be principal since it is a height one prime in A. □

Proposition 1.3. *Let k be a field and R be a finitely generated k-algebra. Assume that R is domain (such rings are called affine domains). The* $\dim(R)$ *is finite and any saturated chain of prime ideals has length equal to* $\dim(R)$*.*

Proof. By Noether normalization R is module finite over a polynomial subring of the form $A = k[x_1, \dots, x_n]$, for some n. Since $A \subset R$ is integral we get $\dim(R) = \dim(A) = n$.

So $n = \dim(R)$. We will do induction on n. The case $n = 0$ is obvious.

Let $P_0 \subset P_1 \subset \cdots \subset P_m$ be a saturated chain of prime ideals in R.

Mod out by P_1 and let $B = R/P_1$. Let us show that B has dimension $n-1$.

We have $A \subset R$ is module finite extension so $A/(P \cap A) \subset B$ is module-finite as well. But $P_1 \cap A = (f)$ for some f prime element in A, because A is UFD and P_1 is a height one prime ideal.

Therefore B is module finite over $A/(f)$. But we can first change variables in f so that f is monic in x_n. Then it is clear that $A/(f)$ is module finite over $k[x_1, \dots, x_{n-1}]$ generated by $1, x, \dots, x^k$ where k is the degree of f.

By the transitivity of the module-finite property we get that B is module finite over a polynomial ring over field in $n-1$ indeterminates. So $\dim(B) = n-1$.

By induction we are now done. $\square$

Proposition 1.4. *Let R be an affine domain over a field k (i.e an k-affine domain). Then* $\mathrm{trdeg_k(R)} = \mathrm{dim(R)}$.

Proof. By Noether normalization there exists $A = k[x_1, \dots, x_n] \subseteq R$ module finite over A.

Then $k(x_1, \dots, x_n) \subseteq (A \setminus 0)^{-1}R$ is an integral extension over a field, so $(A \setminus 0)^{-1}R$ is a field itself.

But then $Q(R)$ is a field as well (as a ring of fractions of a field), and so it must equal $(A \setminus 0)^{-1}R$. So, it is algebraic over $k(x_1, \dots, x_n)$ which says that $\mathrm{trdeg_k(R) = n = dim(R)}$.

$\square$

2. Valuation rings and invertible ideals

Definition 2.1. *A domain R is called a* valuation ring *if for every $x \in Q(R)$, $x \in R$ or $x^{-1} \in R$. This is equivalent to the condition that for any two elements in R one divides the other. Sometimes we say that R is a valuation ring of $K = Q(R)$.*

It is rather easy to see that any two ideals I, J is R one has that $I \subseteq J$ or $J \subseteq I$. Therefore a valuation ring R is local. We will denote the maximal ideal of R by $\mathfrak{m}$.

Theorem 2.2. *Let A be a subring of K and let $\mathfrak{p} \in \operatorname{Spec}(A)$. Then there exists a valuation ring R of K such that $A \subset R$ and $\mathfrak{m} \cap A = \mathfrak{p}$.*

Proof. We can replace A by $A_{\mathfrak{p}}$ and so we can assume that A is local and $\mathfrak{p}$ is its maximal ideal. Consider the family Γ of all subrings $A \subset B$ of K such that $1 \notin \mathfrak{p}B$. Then Γ satisfies the Zorn lemma conditions. Let R be a maximal element of Γ. Clearly if we localize at a maximal ideal of R containing $\mathfrak{p}R$ (which exists since $\mathfrak{p}R \neq R$) then we get a larger example so it follows that R is local with maximal ideal say $\mathfrak{m}$. Also, it is clear that $\mathfrak{m} \cap A = \mathfrak{p}$.

It remains to show that R is a valuation ring of K.

Let $x \notin inK \setminus R$. $R \subset R[x]$ so $1 \in \mathfrak{p}R[x]$, hence we have a relation of the form

$$a_0 + a_1 x + \cdots + a_n x^n = 1,$$

where $a_i \in \mathfrak{p}R \subset \mathfrak{m}$, for all $i = 1, \ldots, n$.

But $1 - a_0$ is invertible in R, so the relation can be modified to a relation of the form

$$1 = b_1 x + \cdots + b_n x^n,$$

with $b_i \in \mathfrak{m}$, $i = 1, \ldots, n$. Take a minimal n for which such a relation exists.

Apply the same reasoning for x^{-1} in case x^{-1}. Hence we can a minimal m such that there exists a relation of the type

$$1 = c_1 x^{-1} + \cdots + c_m (x^{-1})^m,$$

with $c_i \mathfrak{m}$, for all i.

If $n \geq m$, by multiplying the first relation by $b_n x^n$, and subtracting from the first we get contradict the minimlatiy of n. Similar reasoning goes if $m > n$.

□

Proposition 2.3. *A valuation ring is integrally closed.*

Proof. Let R be a valuation ring and $x \in K = Q(R)$.

Then there exists an integral dependence relation:

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0,$$

where $a_i \in R$. Assume that $x \notin R$. Then $x^{-1} \in R$ and more precisely $x^{-1} \in \mathfrak{m}$, otherwise x itself is in R. Since $x \neq 0$ we can divide by it.

Then $1 = (a_{n-1}x^{-1} + \cdots + a_1 x^{n-1} + a_0 x^{-n}) \subseteq \mathfrak{m}$, since x^{-1} is in $\mathfrak{m}$. Contradiction.

□

Theorem 2.4. *Let A be a subring of a field K. Then the integral closure of A in K is the intersection of all valuation rings of K containing A.*

Proof. Let $\overline{A}_K$ be the integral closure of A in K. The above Proposition implies that if B is a valuation ring then $\overline{A}_K \subset B$.

Conversely, let $a \in K \setminus \overline{A}_K$. It suffices to show that there exists a valuation ring B of K which does not contain x but contains A. Let $1/x = y \in K$ and note that $yA[y] \neq A[y]$ otherwise x is integral over A.

Let $\mathfrak{m}$ be a maximal ideal of $A[y]$ containing $yA[y]$. Then there exists a valuation ring of K containing A such that $B \cap \mathfrak{m} = \mathfrak{m}_B$. But then $y \in \mathfrak{m}_B$. This implies that $1/y \notin B$, and so $x \notin B$. □

Definition 2.5. *A totally order Abelian group is a group $(G, +)$ that admits a total relation on G, say $\geq$, such that $x \geq y, u \geq t$ implies $x + u \geq y + t$.*

Let R be a valuation ring and consider the set $G = \{xR : x \in K, x \neq 0\}$. One can prove that G is an Abelian group with the operation $xR + yR := xyR$. In fact, G is a totally ordered Abelian group with $xR \leq yR$ if and only if $yR \subseteq xR$. We will refer to G as the value group associated to R.

Definition 2.6. *Let K a field and G be a totally ordered Abelian group. An additive valuation on K with value group G is a function $v : K \to G \cup \{\infty\}$ such that*

(1) $v(x + y) \geq \min\{v(x), v(y)\}$,
(2) $v(xy) = v(x) + v(y)$,
(3) $v(x) = \infty$ *if and only if* $x = 0$.

Proposition 2.7. *Let R be a valuation domain. Let G be the value group associated to R and define $v : K \to G \cup \{\infty\}$ by $v(x) = xR$, for $x \neq 0$ and $v(0) = \infty$. Prove that v is an additive valuation on K with value group G.*

Proof. The proof is a simple verification. □

Now consider a valuation v on a field K, $v : K \to G \cup \{\infty\}$. Let $R_v = \{x \in K : v(x) \geq 0\}$. Ane can check that R_v is a subring of K and a domain. The group G will be called the value group of R.

Proposition 2.8. *Using the notations introduced in the paragraph above, R_v is valuation ring of K with maximal ideal $m_v = \{x \in K : v(x) > 0\}$.*

Definition 2.9. *Let P be an R-module. We say that P is a* projective module *if for any onto R-linear map $f : M \to N$ between R-module and any R-linear map $g : P \to N$ there exists $h : P \to M$ such that $g = fh$.*

Example 2.10. Let F be a free module. Then F is projective.

Indeed denote by $\{e_i\}_i \in I$ a canonical basis for F. We denote $g(e_i) = n_i \in N$. Lift n_i back to M, i. e. choose $m_i \in M$ such that $f(m_i) = n_i$ which is possible that f is onto. Construct h such that $h(e_i) = m_i$, and then one can check that $g = fh$ (it is enough to verify the equality on the basis elements).

Theorem 2.11. *Let P be an R-module. Then P is projective if and only if P is direct summand of a free R-module, i.e. there exists an R-module Q such that $P \oplus Q$ is free.*

Proof. Assume that P is projective. Let $\{x_i\}_{i \in I}$ be a generating set for P. Map a free module $R^{(I)}$ onto P, $f : R^{(I)} \to P$, by letting $f(e_i) = x_i$. Consider $g = id_P : P \to P$. By the definition of a projective module there exists an R-linear map $h : P \to F$ such that $fh = id_P$. This implies that P is a direct summand of $R^{(I)}$.

The converse is left as an exercise. □

Let R be a domain and let $K = Q(R)$ be its fraction field.

Definition 2.12. *An R-submodule I of K is called a* fractional ideal *if there exists $u \in R$ such that $uI \subseteq R$. For a fractional ideal I we can define $I^{-1} = \{x \in K : xI \subseteq R\}$. If $I^{-1}I = R$ we say that I is an* invertible ideal *of R.*

Note that since $uI \simeq I$ any fractional ideal I is finitely generated, whenever R is Noetherian. Also, any invertible ideal I is finitely generated: indeed $1 = \sum_{i=1}^{n} b_i a_i$ with $b_i \in I^{-1}, a_i \in I$. Therefore $x = \sum_{i=1}^{n}(b_i x)a_i$, and by the definition of I^{-1} we see that $b_i x \in R$. Hence $I =< a_1, \ldots, a_n >$.

Also, a principal (i.e. cyclic) fractional ideal I is invertible. Indeed, if $I = Rx$, then $x^{-1} \in I^{-1}$ and so $1 = xx^{-1}$ which shows that $II^{-1} = R$.

Lemma 2.13. *Let I a finitely generated fractional ideal in R and P a prime ideal. Then $(I_P)^{-1} = I_P^{-1}$.*

Proof. Let $x/s \in I_P^{-1}$. Then $(x/s)I_P \in R_P$ because $xI \in R$. This proves one inclusion.

Now let $I = Ra_1 + \ldots + Ra_n$. Say $x \in (I_P)^{-1}$ and so $xI_P \in R_P$ which gives that for all i there exists $c_i \notin P$ such that $c_i x a_i \in R$. Let $c = c_1 \cdots c_n$. Then $(cx)a_i \in R$ for all i. So, $(cx)I \in R$ which proves that $cx \in I^{-1}$ or $x \in (I^{-1})_P$.

$\square$

Theorem 2.14. *Let R be a Noetherian domain and I a fractional ideal. The following asserstions are equivalent:*

(1) *I is invertible;*
(2) *I is R-projective;*
(3) *I is finitely generated and for any maximal ideal P of R, I_P is a cyclic R_P-module.*

Proof. (1) implies (2): Since I can be generated by finitely many elements, say n, using the same notations as the ones introduced above note that there exists a map $f : I \to R^n$, defined by $f(x) = (b_i x)_i$. We have a natural onto homomorphism $g : R^n \to I$ defined by $g(e_i) = a_i$. Clearly $(gf)(x) = g((b_i x)_i) = \sum_{i=1}^{n}(a_i b_i x) = 1 \cdot x = x = id_I(x)$ so I is a direct summand in R^n, hence projective.

(2) implies (1):

First note that any R-linear map $h : I \to R$ is of the form $h(a) = ka$, where $k \in K$. We can assume that I is an ideal of R. Then for any $a, b \in I$ we can see that $bf(a) = f(ab) = af(b)$ and so $f(a)/a$ is constant if $a \neq 0$. Denote this by k and note that $f(a) = ka$.

Let $g : F = R^{(I)} \to I$ a surjective homomorphism such that $g(e_i) = a_i$. This map splits hence there exists $f : I \to F$ such that $gf = id_I$. But then $f = (f_i)$ with $f_i : I \to R$ and hence $f_i(x) = k_i x$ for all $x \in I$. For every x finitely many $f_i(x)$ are nonzero, therefore finitely many k_i are nonzero. We remark that $b_i x = f_i(x) \subset R$, so $b_i \in I^{-1}$.

Then for all $x \in I$, $x = \sum a_i k_i x$ and so $1 = \sum a_i k_i$ which prove that $II^{-1} = R$.

(1) implies (3):

Using the notations introduced above, the equality $1 = \sum_{i=1}^{n} a_i b_i$ implies that there exists i such that $a_i b_i$ is a unit in R_P. This proves that $IR_P = a_i R_P$.

(3) implies (1):

By the lemma proved earlier, we see that $(I_P)^{-1} = I_P^{-1}$. Since I_P is cyclic, we know that $I_P(I_P)^{-1} = R_P$.

Assume that $II^{-1} \neq R$ and choose a maximal ideal P such that $II^{-1} \subseteq P$. and so $(II^{-1})_P \neq R_P$. But $(II^{-1})_P = I_P(I^{-1})_P = I_P I_P^{-1} = R_P$. Contradiction. $\square$