

# MATH 603 Notes

David Zhu

April 22, 2024

## 1 More on Commutative Rings

Let  $a, b \in R$ . Then  $a|b \iff \exists a' \in R, b = aa'$ ; A semi ring on  $(R, \leq)$  defined by  $a \leq b \iff a|b$ . Note that  $\leq$  is usually not a partial order: let  $b \in R^\times$ , then  $a \leq ab \leq a$ , but  $a \neq ab$ .

**Proposition 1.1.**  $a \sim b$  iff  $a \leq b$  and  $b \leq a$  iff  $(a) = (b)$  is an equivalence relation.

For  $R$  a domain, the induced relation gives a well-defined definition of greatest common divisor.

**Definition 1.1.** The **gcd** of  $a, b$ , denoted by  $gcd(a, b)$ , if exists, is any  $d \in R$  such that  $d|a, b$  and for any other  $d'$  satisfying the condition,  $d'|d$ .

**Definition 1.2.** The **lcm** of  $a, b$ , denoted by  $lcm(a, b)$ , if exists, is any  $d \in R$  such that  $a, b|d$  and for any other  $d'$  satisfying the condition,  $d|d'$ .

**Proposition 1.2.** If  $gcd(a, b)$  exists, then  $gcd(a, b) = \sup\{d : d \leq a, b\}$ . If  $lcm(a, b)$  exists, then  $lcm(a, b) = \inf\{d : a, b \leq d\}$ .

Note that maximal/minimal elements always exists by Zorn's lemma. However, the unique supremum/infimum may not exist. We have our following example:

**Example 1.1.** Take  $R = [\sqrt{-3}]$ . Let  $a = 4 = (1 + \sqrt{-3})(1 - \sqrt{-3})$  and  $b = 2(1 + \sqrt{-3})$ . Then,  $(1 + \sqrt{-3})$  and 2 are both maximal divisors, but they are not comparable since the only divisors of 2 are  $\{\pm 1, \pm 2\}$  by norm reasons, and none divides  $1 + \sqrt{-3}$ .

**Proposition 1.3.** Let  $a, b \in R$  be given. Then the following hold:  $gcd(a, b) = d$  exists iff  $(d)$  is the unique maximal principal ideal such that  $(a) + (b) \subseteq (d)$ . Dually,  $lcm(a, b) = c$  exists iff  $(c) = (a) \cap (b)$ . If both holds, then  $a \cdot b = lcm(a, b) \cdot gcd(a, b)$

*Proof.* Easy exercise. Note that the inclusion can be proper, for example, take  $R = k[x, y]$  and ideals  $(x), (y)$ . Then  $(1)$  is the gcd, but the containment is proper.  $\square$

Recall that  $Id(R)$  is partially ordered by inclusion.

**Definition 1.3.**  $(Id(R), +, \cap, \cdot, \leq)$  is the lattice of ideals of  $R$ .

Note that  $+$ ,  $\cap$  are simply the sums and intersection, but  $\cdot$  is the ideal generated by the products, i.e the set of finite sums of products.

**Theorem 1.1.** Let  $Id^\infty(R)$  be the set of non-finitely generated ideals for  $R$ ; the following are equivalent:

1.  $Id^\infty(R)$  is non-empty;
2. There exists an infinite non-stationary chain of ideals  $(\sigma_i)$ , where  $\sigma_i \in Id(R)$ ;

*Proof.* For  $1 \implies 2$ , let  $I$  be a non-finitely generated ideal of  $R$  and pick  $x_1 \in I$ . Let  $\sigma_1 = (x_1)$ . Because the ideal is non-finitely generated, we can pick  $x_2 \in I$  such that  $x_2 \notin \sigma_1$ . Let  $\sigma_2 = (x_1, x_2)$ . Continue inductively gives us an infinite non-stationary chain of ideals.

For  $2 \implies 1$ , take the union of all the ideals in the infinite non-stationary chain. It is an ideal and it cannot be finitely generated.  $\square$

**Theorem 1.2.** (Cohen's lemma): Let  $Id^\infty(R) \neq \emptyset$ . Then, it has a maximal element and any such maximal element is prime.

Before proving Cohen's lemma, we need the following technical lemma:

**Lemma 1.3.** Let  $I$  be an ideal. Define  $(I : a) := \{b \in R : ab \in I\}$ . If  $I + (x)$  and  $(I : x)$  are both finitely generated, then  $I$  is finitely generated.

*Proof of Lemma 1.3.* By assumption, there is finite set  $\{\alpha_i := a_i + f_i x : a_i \in I, f_i \in R, i = 1, \dots, k\}$  that generate  $I + (x)$ , and a finite set  $\{b_j : j = 1, \dots, l\}$  that generate  $(I : x)$ . We claim that the set  $\{a_i, b_j x : i \in I, j \in J\}$  generate the entire  $I$ : since  $I \subseteq I + (x)$ , we can write any element  $\pi \in I$  as a finite linear combination  $\pi = \sum_{i=1}^k g_i \alpha_i = \sum_{i=1}^k g_i (a_i + f_i x)$ , where  $g_i \in R$ . We note that  $\pi - \sum_{i=1}^k g_i a_i = \sum_{i=1}^k g_i f_i x$  is in  $I$ ; it follows that  $\sum_{i=1}^k g_i f_i \in (I : x)$ , so  $\sum_{i=1}^k g_i f_i x$  is generated by the set  $\{b_j x\}$ , and we are done.  $\square$

With the lemma in hand, now we can prove Theorem 1.2

*Proof of Theorem 1.2.* Zorn's lemma implies  $Id^\infty(R)$  has maximal elements. Let  $I$  one such maximal element, and suppose it is not prime. Then, there exists  $xy \in I$  and WLOG suppose  $x \notin I$ . By maximality,  $I + (x)$  must be finitely generated. By definition, we have  $y \in (I : x)$ . Lemma 1.3 implies  $(I : x)$  is not finitely generated, and in particular,  $I \subseteq (I : x)$ . Applying maximality again, we have  $I = (I : x)$ , which forces  $y \in I$ , a contradiction.  $\square$

## 2 Euclidean Rings

**Definition 2.1.** A Principal Ideal Ring is any ring  $R$  in which every ideal is principally generated. If  $R$  is a domain, then  $R$  is called a PID.

**Definition 2.2.** A **Factorial Ring** is any ring  $R$  in which all units can be written as a finite product of irreducible elements, unique up to a unit. If  $R$  is domain, then it is called a **UFD**.

Note that if the ring  $R$  it is not a domain,  $x|y$  and  $y|x$  does not imply  $x = uy$  for some unit  $u$ . Let us prove that this holds for a domain: suppose  $x = ys$  and  $y = xt$ , and  $x, y \neq 0$  then  $x = xts$ , which implies  $x(1 - ts) = 0$ . This forces  $1 - ts = 0$ , and  $t, s$  are then units. We can concoct counterexamples when  $R$  is not a domain accordingly: let  $R = k[x]/(x^3 - x)$  and take  $a = x, b = x^2$ . Clearly,  $a|b$  and  $b = x^2 \cdot x = x^3$ , so  $b|a$ . However,  $x$  is not a unit.

**Definition 2.3.** A **Noetherian Ring** is any ring  $R$  such that any ideal is finitely generated.

**Definition 2.4.** Let  $R$  be a domain. A **Euclidean norm** on  $R$  is any map  $\phi : R \rightarrow \mathbb{N}$  satisfying  $\phi(x) = 0$  iff  $x = 0$  and for every  $a, b \in R$  with  $b \neq 0$ , then there exists  $q, r \in R$  such that  $a = bq + r$  with  $\phi(r) < \phi(b)$ . A **Euclidean Domain** is any domain equipped with a Euclidean norm.

Example of Euclidean domains include  $\mathbb{Z}, \mathbb{Z}[i]$ . A non-trivial example  $R = F[t]$ , with  $\phi(p(t)) = 2^{\deg(p(t))}$ . A non-example is  $\mathbb{Z}[\sqrt{6}]$  for it is not a PID.

**Proposition 2.1.** Euclidean Domains are PIDs.

*Proof.* By the well-ordering principal, for every ideal  $I$  in a Euclidean domain, there exists an element other than 0 of the smallest norm. It is easy exercise that such element generate the entire ideal.  $\square$

**Proposition 2.2.** (The Euclidean Algorithm): Given  $a, b \in R, b \neq 0$ . Set  $r_0 = a, r_1 = b$ , and continue inductively  $r_{i-1} = r_i \cdot q_i + r_{i+1}$ . Then,  $r_i = 0$  for  $i > \phi(b)$  and if  $r_{i_0} \geq 1$  maximal with  $r_{i_0} \neq 0$ , then  $r_{i_0} = \gcd(a, b)$ .

*Proof.* Note that the remainder is strictly decreasing, so  $r_i$  must become 0 after  $\phi(b)$  steps. Note that once  $r_{i+1} = 0$ , we have  $r_i|r_n$  for all  $n \leq i$ . Conversely, it is clear that any divisor of  $a, b$  divides all  $r_n$  for  $n \leq i$ .  $\square$

### 3 Principal Ideal Domains

**Theorem 3.1.** (Charaterization) For A domain  $R$ , the following are equivalent:

1.  $R$  is a PID.
2. every  $p \in \text{Spec}(R)$  is principal.

*Proof.* One direction is trivial; for the other direction, assume that every prime is principal. Then, Cohen's Lemma implies  $\text{Id}^\infty(R) \neq \emptyset$ ; In particular, every ideal is finitely generated, so the ring is Noetherian. We may apply Zorn's lemma on the set of non-principally generated ideal (since every chain stablizes and has a maximal element), and let  $P$  be a maximal non-principally generated ideal. Suppose it is not prime, and let  $xy \in P$  with  $x \notin P$ . Then,  $P \subset (P : x)$  and  $P \subset P + (x)$  properly. By maximality, we have  $(P : x) = (c)$ , and  $(I : c) = (d)$ . By definition, we have  $cd \in I$ ; moreover, suppose  $x \in I$ , then  $x = cr = cdt$  for some  $r, t \in R$ . Thus,  $I = (cd)$  is principal, a contradiction.  $\square$

**Proposition 3.1.** PIDs are UFDs.

*Proof.* Let  $a \in R$  such that  $a$  is non-zero and not a unit. Then, there exists  $p \in \text{Spec}(R)$  such that  $(a) \subseteq p$ . Hence  $R$  being a PID implies  $\exists \pi \in R$  such that  $p = (\pi)$ . Hence,  $\pi$  must be prime and  $\pi|a$ . Set  $a_1 = a$ ,  $\pi_1 = \pi$ , and let  $a_2$  be the element such that  $\pi_1 a_2 = a_1$ . If  $a_2$  is not a unit, find  $(a_2) \subset (\pi_2)$ , where  $\pi_2$  is prime. Let  $a_3$  be the element such that  $\pi_2 a_3 = a_2$ . Continue inductively until  $a_n$  is a unit. The process must terminate, for otherwise we get an infinite chain of distinct principal ideals  $(a_i)$  that does not stabilize (stabilizing is equivalent to  $(a_n) = (a_{n+1})$  for some  $n$ , which implies they differ by a unit).  $\square$

**Corollary 3.1.1.** Let  $R$  be a PID; let  $P \subset R$  be a set of representatives for the prime elements up to association. For every  $a \in R$ ,  $\exists \epsilon \in R^\times$  and  $e_\pi \in \mathbb{N}$  such that almost all  $e_\pi = 0$ . Then, every  $a \in R$  can be written as  $a = \epsilon \prod_{\pi \in P} \pi^{e_\pi}$ . We proceed to recover  $\gcd$  and  $\text{lcm}$ , up to associates.

Note that the above corollary generalizes to the quotient field by replacing  $\mathbb{N}$  with  $\mathbb{Z}$ .

## 4 Unique Factorization Domains

**Definition 4.1.** The following are equivalent for a domain  $R$ :

1.  $R$  is a UFD.
2. Every minimal prime ideal (prime of height 1) is principal and every non-zero, non-invertible elements in contained in finitely many primes.

*Proof.*  $1 \implies 2$ : For every non-zero prime  $P$ , pick  $x \in P$  has factor. One of the prime factors must be in  $P$ , and it follows by minimality that  $P$  must be generated by such prime factor. For the second part, the finite factorization of the element gives precisely the finite primes that it is contained in.  $2 \implies 1$ : given  $x \in R$ , the finitely many primes containing  $x$  are principally generated by prime elements, which gives a factorization.  $\square$

Remark: we recover the  $\gcd$  and  $\text{lcm}$  definition using the same factorization as Corollary 3.1.1.

**Theorem 4.1.** (Gauss Lemma) Let  $R$  be a UFD; then  $R[t]$  is a UFD.

To prove the theorem, we need the following lemma on contents:

**Definition 4.2.** Let  $f(t) = a_0 + \dots + a_n t^n$  be given. Then, the content of  $f$ , denoted  $C(f)$ , is the GCD of all coefficients. In particular,  $C(f)|a_i$  for all  $i$ , and  $f_0 := f/(C(f))$  has content 1.

**Lemma 4.2.** Let  $R$  be a UFD, then the following hold: (1).  $C(f) : R[t] \rightarrow R$  given by  $f \mapsto C(f)$  is multiplicative; in particular, if  $C(f) = C(g) = 1$ , then  $C(fg) = 1$ .

*Proof of lemma 4.2.* given  $f(t) = a_0 + \dots + a_n t^n$  and  $g(t) = b_0 + \dots + b_m t^m$ . If one of  $f, g$  is constant, then it is easy exercise; suppose neither is constant, then set  $f = f_0 \cdot C(f)$  and  $g = g_0 \cdot C(g)$ . Clearly we have  $C(f) \cdot C(g) | C(fg)$ . Hence it suffices to prove that  $C(f_0 g_0) = 1$ . Equivalently, let  $\pi \in R$  be a prime element, we want to show there exists a coefficient  $c_k \in f_0 g_0$  such that  $\pi$  does not divide  $c_k$ . Suppose

$\pi|_{c_k} = \sum_{i+j=k} a_i b_j$  for all  $k$ . Because  $C(f_0) = C(g_0) = 1$ , then there exists minimal  $a_i, b_j$  such that  $\pi$  does not divide  $a_{i_0}, b_{j_0}$ . Then,  $\pi$  does not divide  $C_{i_0+j_0}$ . □

**Proposition 4.1.** Let  $K := \text{Quot}(R)$ , and  $f \in K[t]$ . Then, let  $d$  be the least common multiple of the denominators of the coefficients of  $f$ . Then,  $f = df/d$ , and  $df \in R[t]$ . Define  $C_K(f) = C(df)/d$ . It is standard to check the analog for lemma 4.2 holds for  $C_K$  as well.

**Proposition 4.2.** Let  $R$  be a UFD. For any irreducible  $f \in R[t]$ , either  $f$  is a constant and thus prime in  $R$ , or  $f$  is primitive, i.e  $C(f) = 1$ .

*Proof.* If  $f$  is a constant, the first part of the proposition is obvious; now suppose  $f$  has degree  $> 0$ ; then  $f$  can be factored into its primitive part and content; if  $C(f) \neq 1$ , we either have a non-trivial factorization of  $f$  or  $f$  will be a constant multiplied by a unit, a contradiction. □

**Theorem 4.3.** Let  $R$  be a UFD. For  $f(t) \in R[t]$ , let  $K := \text{Quot}(R)$ . Then, the following are equivalent:

1.  $f(t)$  is prime
2.  $f(t)$  is irreducible
3. Either  $f$  is an irreducible constant in  $R$  or  $f$  is irreducible in  $K[t]$  and  $C_K(f) = 1$ .

*Proof.*  $1 \implies 2$  holds in every domain: suppose  $a$  is prime and  $a = bc$ . Then by primeness, we have  $a|b$  or  $a|c$ . WLOG, suppose  $a|b$ , such that  $ax = b$  and  $a = axc$ , so  $cx - 1 = 0$ , which implies  $c$  is a unit.

$2 \implies 1$  in UFDs: suppose  $f$  is an irreducible and  $f|gh$ , then we have some  $l$  such that  $fl = gh$ . Because  $g, h, l$  can be uniquely written as a product of irreducibles up to permutation and units, we see that the irreducible  $f$  must appear on the RHS once, i.e  $f|g$  or  $f|h$ .

For  $2 \implies 3$ : If  $f$  is a constant, then it become a unit in the field of fractions; suppose  $\deg(f) > 0$ , so irreducibility implies  $C(f) = 1$ . Suppose by contradiction that  $f$  is reducible over  $K[t]$ , and let  $f = gh$  for  $g, h \in K[t]$  be a factorization in  $K[t]$ . Note that given  $g, h \in K[t]$ , there is some  $x_g, x_h \in K$  such that  $x_g g, x_h h \in R[t]$  and  $C(x_h h) = C(x_g g) = 1$ . Then,  $x_g x_h f = (x_g g)(x_h h) \in R[t]$ . By Proposition 4.2, we have  $C(x_g x_h f) = x_g x_h C(f) = 1$ , which implies  $x_g x_h = 1$  (up to a unit in  $R$ ). However, this implies  $f = (x_g g)(x_h h)$ , a contradiction.

So we are left to prove  $3 \implies 2$ . Suppose  $f$  is not a constant and  $f$  primitive and irreducible. Suppose  $f = gh \in R[x]$ . WLOG  $g$  is a unit in  $K[x]$ , so  $g$  is a nonzero element of  $R$ . Now  $g$  divides all the coefficients of  $f$ , so  $g$  is a unit in  $R$ . □

**Proposition 4.3.**  $R[t_i]_{i \in I}$  is UFD if  $R$  is UFD.

*Proof.* By induction it suffices to show that  $R[t]$  is a UFD. The idea is that  $K[t]$  is PID so it is a UFD. A factorization in  $K[t]$  will correspond to a factorization in  $R[t]$  by the equivalence of 2 and 3 in Theorem 4.3. □

## 5 Noetherian Rings

**Definition 5.1.** A commutative ring  $R$  is called a **Noetherian** ring if every chain of ideals in  $R$  is stationary.

**Proposition 5.1.** The following are equivalent:

1. Every chain of ideals is stationary.
2. All ideals are finitely generated.
3.  $\text{Spec}(R) \subseteq \text{Id}^f(R)$ .

Terminology: the condition 1 is called the ACC (Ascending Chain Condition).

*Proof.* By Cohen's lemma, we deduce  $2 \iff 3$ ;  $1 \iff 2$  is an easy exercise.  $\square$

For non-commutative rings, it is possible that a ring is left Noetherian but not right Noetherian.

**Example 5.1.**  $R = \left\{ \begin{bmatrix} p & q \\ 0 & m \end{bmatrix} : p, q \in \mathbb{Q}; m \in \mathbb{Z} \right\}$  is left Noetherian but not right Noetherian.

**Proposition 5.2.** (Basic Properties) Let  $R$  be a Noetherian ring. The the following hold:

1. If  $\mathfrak{a}$  is an ideal of  $R$ , then  $R/\mathfrak{a}$  is Noetherian if  $R$  is Noetherian.
2. If  $\Sigma \subset R$  is a multiplicative system, then  $R_\Sigma$  is Noetherian.
3. The radical of an ideals  $\mathfrak{a}$ ,  $\text{rad}(\mathfrak{a})$ , has a power contained in  $\mathfrak{a}$ .
4. Let  $\text{Spec}_{\min}(\mathfrak{a}) := \{p \in \text{Spec}(R) : \mathfrak{a} \subseteq p, p \text{ minimal}\}$  is finite.

*Proof.* To 1. Ideals in  $R/\mathfrak{a}$  corresponds bijectively to ideals in  $R$  that contains  $\mathfrak{a}$ . Finite generation of ideals in  $R$  clearly implies the finite generation of ideals in the quotient.

To 2.  $\text{Spec}(R_\Sigma)$  corresponds bijectively to primes in  $\text{Spec}(R)$  with empty intersection with  $\Sigma$ . We also have  $p$  finite generated implies  $p^e$  f.g.

To 3. Suppose  $\text{rad}(\mathfrak{a}) = (r_1, \dots, r_n)$  f.g. For every  $i$ , we have  $r_i^{n_i} \in \mathfrak{a}$  for some  $n_i$ . Take  $n = \sum n_i$  and  $\text{nil}(\mathfrak{a})^n \subset \mathfrak{a}$ .

To 4. The first method to prove this is by contradiction: let  $A = \{\mathfrak{a} : \text{Spec}_{\min}(\mathfrak{a}) \text{ is infinite}\}$ . Then  $A$  has maximal elements. Let  $\mathfrak{a}_0$  be maximal. Note that  $\mathfrak{a}_0$  cannot be prime for it is over itself. Suppose it is not prime, then there exists  $xy \in \mathfrak{a}$  with both  $x$  and  $y$  not in  $\mathfrak{a}$ ; for every prime ideal  $P$  containing  $\mathfrak{a}$ ,  $P$  contains either  $x$  or  $y$ . By pigeonhole, there must be infinite such primes containing either  $\mathfrak{a} + (x)$  or  $\mathfrak{a} + (y)$ , which contradicts maximality.

The second method is using the fact that  $\text{Spec}(R)$  is a Noetherian topological space, which has finitely many irreducible components.  $\square$

The third method is through primary decomposition. An ideal  $I$  is irreducible if  $I = a_1 \cap a_2$  then,  $I = a_1$  or  $I = a_2$ . For principal ideals, this is equivalent to the generator being irreducible.

**Proposition 5.3.** If  $R$  is Noetherian, then every ideal  $I \in R$  is in the finite intersection of irreducible ideals in  $R$ .

*Proof.* By contradiction, let  $X$  be the set of ideals that does not satisfy the proposition. Then,  $X$  is non-empty, and by Noetherian assumption, there is a maximal element  $\mathfrak{a}_0$ . Then,  $\mathfrak{a}_0$  is not irreducible, for it would be the intersection of itself. Therefore, there exists  $I_0, I_1$  such that  $\mathfrak{a}_0 = I_0 \cap I_1$ , where  $\mathfrak{a}_0$  is properly contained in both. By maximality,  $I_0, I_1$  are both finite intersection of irreducibles, and we can decompose  $\mathfrak{a}_0$  based on such, a contradiction.  $\square$

**Definition 5.2.** Let  $R$  be a commutative ring. Then an ideal  $I \subset R$  is primary if for all  $x, y \in R$  we have: if  $xy \in I$ ,  $x \notin I$ , then there exists  $n \in \mathbb{N}$  such that  $y^n \in I$ .

In general, a power of prime ideal is not primary. If  $I = \mathfrak{m}^n$  for some maximal ideal  $\mathfrak{m}$ , then  $I$  is in fact primary.

**Proposition 5.4.** Let  $R$  be Noetherian, and  $\mathfrak{a} \in Id(R)$  be an irreducible ideal. Then,  $\mathfrak{a}$  is primary, and  $nil(\mathfrak{a})$  is prime.

*Proof.* Exercise  $\square$

These two facts imply  $Spec_{min}$  must be finite. In general, quotient of  $UFD$  and  $PID$  are not  $UFD$  or  $PID$ . but this holds for Noetherian rings.

**Theorem 5.1.** Let  $R$  be a Noetherian ring. Then the following hold:

1. (Hilbert Basis Theorem):  $R[t_1, \dots, t_n]$  is Noetherian.
2. Every finitely generated  $R$ -algebra  $S$  is Noetherian.
3. The power series ring  $R[[x]]$

*Proof.* Note that  $1 \implies 2$  since every finitely generated algebra is a quotient of polynomial rings over finitely many variables. To prove 1, by induction it suffices to show for  $i = 1$ . We now present a proof that applies for both 1 and 3. Let  $I \in R[t]$  be an ideal. Claim:  $I$  is f.g. Inductively, we may choose elements  $f_i \in I$  with  $deg(f_i)$  being minimal in  $I \setminus (f_1, \dots, f_{i-1})$ . If the process terminates, then we are done; otherwise, let  $a_i$  be the leading coefficient of  $f_i$ , and the chain of ideals  $(I_i := (a_1, \dots, a_i))$  must stabilize by Noetherian assumption on  $R$ . Suppose it stabilizes at step  $N$ , and moreover suppose by contradiction that  $f_1, \dots, f_N$  does not generate  $\mathfrak{a}$ . Then, consider the element  $f_{N+1}$ , which by our argument is not contained in  $(f_1, \dots, f_N)$  and of minimal degree. The leading coefficient of  $f_{N+1}$  is expressed as  $a_{N+1} = \sum_{i=1}^N \mu_i a_i$ . Then, we cook up

$$g = \sum_{i=1}^N \mu_i f_i x^{deg(f_{N+1}) - deg(f_i)}$$

where  $g \in (f_1, \dots, f_N)$  by construction, and  $f_{N+1} - g \notin (f_1, \dots, f_N)$ . However,  $f_{N+1} - g$  has degree strictly less than  $f_N$  since we cancelled the leading term, which is impossible.  $\square$

## 6 Valuation Rings

**Proposition 6.1.** Let  $R$  be a domain. Then the following are equivalent:

1. The ideals in  $R$  are totally ordered by inclusion.
2. The principal ideals in  $R$  are totally ordered by inclusion, i.e.  $id(R)$  is a chain
3. For every  $x \in \text{Quot}(R)$ , if  $x \notin R$  then  $x^{-1} \in R$ .

*Proof.*  $1 \implies 2$  is trivial; for  $2 \implies 3$ , suppose  $\frac{a}{b} \notin R$ ; then since the principal ideals are totally ordered, the elements are totally ordered by divisibility. Hence,  $b \nmid a$  implies  $a \mid b$ , so  $\frac{b}{a} \in R$ . For  $3 \implies 1$ , suppose we are given ideals  $I, J$ . If there exists  $j \in J$  such that  $j \notin I$ , then  $\frac{i}{j} \in R$  for all  $i \in I$ , for otherwise there exists  $i'$  such that  $\frac{i'}{j} \in R$ , which implies  $j \in I$ . Thus,  $I \subseteq J$ .  $\square$

**Definition 6.1.** A ring  $R$  satisfy one of the conditions above is called a (Krull) **Valuation Ring**.

**Example 6.1.**  $\mathbb{Z}_{(p)} = \{\frac{q}{l} \in \mathbb{Q} : \gcd(l, p) = 1\}$  is a valuation ring with maximal ideal  $(p)$ . The valuation on  $v_p$  is defined by  $v(\frac{q}{l}) = r$  where  $r$  is the maximal natural number such that  $p^r \mid q$ . The natural extension of such valuation on the entire  $\mathbb{Q}$  is  $v(\frac{p}{q}) = v(p) - v(q)$ .

**Proposition 6.2.** (Properties) Let  $R$  be a valuation ring, and  $K$  be its quotient field. The the following hold:

1.  $R$  is local, and  $m = \{x \in R : x^{-1} \notin R\}$ . The maximal ideal is called **valuation ideal** of  $R$ .
2.  $\Gamma_R := K^\times / R^\times$  is totally ordered by  $xR^\times \leq yR^\times$  iff  $yR \subseteq xR$  iff  $x \mid y$  in  $R^\times$ . The group is called the **value group** of  $R$ .
3. The natural map  $v_R : K \rightarrow \Gamma_R \cup \{\infty\}$ ,  $v(0) = \infty$  satisfies  $v(xy) = v(x) + v(y)$  and  $v(x + y) \geq \min(v(x), v(y))$ . Such map is called the (canonical) **valuation** of  $R$ .

*Proof.* To 1, note that by Proposition 6.1.1, the ideals are linearly ordered, so there exists a unique maximal ideal, and the ring is local. In a local ring, the maximal ideal is precisely the non-units.

To 2, the statement is obvious from 6.1.2 that elements in  $R$  are totally ordered by divisibility.

To 3, it is clear that if  $x \mid y$ , then  $x \mid x + y$ . Therefore,  $v(x + y) \geq \min\{v(x), v(y)\}$ .  $\square$

Note  $R$  is the set  $\{x \in K : v_R(x) \geq 0\}$ ;  $\mathfrak{m}$  is the set  $\{x \in K : v_R(x) > 0\}$ ;

**Definition 6.2.** Let  $R$  be a domain, and  $K$  be a field,  $(\Gamma, +, \leq)$  be a totally ordered abelian group. Let  $v : K \rightarrow \Gamma \cup \{\infty\}$  be a map satisfying

1.  $v(x) = \infty$  iff  $x = 0$
2.  $v(xy) = v(x) + v(y)$
3.  $v(x + y) \geq \min(v(x), v(y))$

Then, the map  $v$  is called a **valuation** of  $K$ .

**Proposition 6.3.**  $R_v = \{x \in K : v(x) \geq 0\}$  is a valuation ring. The map  $\tau : \Gamma_{R_v} \rightarrow \Gamma$ , given by  $xR_v^\times \mapsto v(x)$  is an order preserving embedding. Moreover,  $v = \tau \circ v_{R_v} : K \rightarrow \Gamma \cup \{\infty\}$ .



*Proof.* It is easy to check  $R_v = \{x \in K : v(x) \geq 0\}$  is a ring from the definition of a valuation above. To see that it is valuation ring, note that  $v(\frac{x}{y}) = v(x) - v(y) = -v(\frac{y}{x})$ . Therefore one of them is  $\geq 0$  and thus in  $R_v$ . The order on  $\Gamma_{R_v}$  is given by  $xR_v^\times \leq yR_v^\times$  iff  $x|y$  in  $R_v^\times$  iff  $v(\frac{y}{x}) \geq 0$  iff  $v(x) \leq v(y)$ . The final composition is easy to check by definition.  $\square$

Given a valuation ring,  $R \subset K$ , every embedding of totally ordered groups  $\Gamma_R \rightarrow \Gamma$  gives rise to a valuation.

**Definition 6.3.** The following are equivalent definitions for equivalence of valuations on  $K$ :

1. Two valuations  $v, w$  on  $K$  are equivalent if  $R_v = R_w$ .
2. Two valuations  $v, w$  on  $K$  are equivalent if  $\mathfrak{m}_v = \mathfrak{m}_w$ .
3. Given  $v : K \rightarrow \Gamma_v \cup \{\infty\}$  and  $w : K \rightarrow \Gamma_w \cup \{\infty\}$ , with embeddings  $\tau_v : \Gamma_{R_v} \rightarrow \Gamma_v$ ,  $\tau_w : \Gamma_{R_w} \rightarrow \Gamma_w$ . Then,  $v, w$  are equivalent if there exists an order preserving isomorphism  $\tau_{vw} : \tau_v(\Gamma_{R_v}) \rightarrow \tau_w(\Gamma_{R_w})$  that fits into the following commutative diagram

$$\begin{array}{ccccc} \Gamma_{R_v} & \longrightarrow & \tau_v(\Gamma_{R_v}) & \longrightarrow & \Gamma_v \\ & & \downarrow \tau_{vw} & & \\ \Gamma_{R_w} & \longrightarrow & \tau_w(\Gamma_{R_w}) & \longrightarrow & \Gamma_w \end{array}$$

To see that the above definitions are indeed equivalent, note that  $1 \implies 2$  is trivial; for  $2 \implies 1$ , suppose there exists  $a \in R_v - \mathfrak{m}_v$  such that  $a \notin R_w - \mathfrak{m}_w$ . Then, by properties of a valuation ring,  $a^{-1} \in R_w$  and in particular, it is not in the maximal ideal, so it is a unit, and  $a \in R_w$ . For  $1 \implies 3$ : if  $R_v = R_w$ , then  $\Gamma_{R_v} = \Gamma_{R_w}$  by definition. For  $k \in \tau_v(\Gamma_{R_v})$ , pick a representative  $\tau_v^{-1}(k) \in \Gamma_{R_v} = \Gamma_{R_w}$ , and define  $\tau_{vw}(k) = \tau_w(\tau_v^{-1}(k))$ . It is standard to verify the map is an order-preserving isomorphism. For the converse, the map is also easy to construct given the isomorphism  $\tau_{vw}$ .

**Definition 6.4.** A valuation ring  $R$  is called **discrete**, if  $v_R(K) \cong \mathbb{Z}$  as ordered abelian groups. An element  $\pi$  such that  $v_R(\pi)$  generates  $\mathbb{Z}$  is called a **uniformizing parameter**.

**Example 6.2.**  $\mathbb{Z}_{(p)} \subset \mathbb{Q}$  is a discrete valuation ring. The uniformization parameter is  $p\epsilon$  with  $\epsilon$  a unit.

A valuation ring  $R$  is called rank 1 if  $v_r(K)$  satisfies the Archimedean axiom, i.e for  $\forall \gamma_1, \gamma_2 \in \Gamma_R, \gamma_1 > 0$ ,  $\exists n \in \mathbb{N}$  such that  $\gamma_2 \leq n \cdot \gamma_1$ . A totally ordered group  $\Gamma$  is Archimedean if there is an ordered preserving embedding into the reals. In relation to absolute values,

**Definition 6.5.** An absolute value of a field  $K$  is any map  $|\cdot| : K \rightarrow \mathbb{R}_{\geq 0}^+$  iff it satisfies the norm axioms. An absolute value is called **non-Archimedean** or **ultra-metric** if  $|x + y| \leq \max\{|x|, |y|\}$ .

**Example 6.3.** Let  $|\cdot| : K \rightarrow \mathbb{R}$  be a non-Archimedean absolute value. Then  $v(-) := -\log(|\cdot|) : K \rightarrow \mathbb{R} \cup \{\infty\}$  is rank 1 valuation. Conversely, let  $v : K \rightarrow \mathbb{R} \cup \{\infty\}$  be a rank one valuation, then  $|\cdot|_v := e^{-v(-)} : K \rightarrow \mathbb{R}_{\geq 0}$  is a non-Archimedean absolute value.

**Theorem 6.1.** The following facts about possible valuations

1. If  $K|F_p$  algebraic, then no non-trivial valuations exists on  $K$ .
2. If  $v$  is a valuation of  $F(t)$  such  $v$  is trivial on  $F$ , then  $R_v = F[t]_{p(t)}$ , where  $p(t)$  irreducible or  $R_v = F[\frac{1}{t}]_{(\frac{1}{t})}$ .
3. If  $v$  is a non-trivial valuation on  $\mathbb{Q}$ , then  $R_v = \mathbb{Z}_{(p)}$  for some  $p$  prime.

*Proof.* For 1, let  $K|F_p$  be an algebraic extension. Then, any element  $a \in K$  is a root to the polynomial of the form  $x^{p^k-1} - 1$ . A valuation on  $K$  satisfies  $0 = v(1) = v(a^{p^k-1}) = (p^k - 1)v(a) = v(a)$ . Thus, the valuation must be trivial.

For 2,3, refer to HW7 problem 6. □

**Theorem 6.2.** (Ostrowski's Theorem) Every non-trivial absolute value on  $\mathbb{Q}$  is equivalent to either the usual real absolute value or a  $p$ -adic absolute value.

In general, the space of all valuations on  $K$ , denoted  $Val(K)$ , is called the Zariski-Riemann space. Moreover,  $Val(K)$  carries a topology called a patch topology, or constrcutible topology, which makes the space compact and totally disconnected. The space is usually very complicated.

**Theorem 6.3.** (Chevalley's Theorem for extension of Valuations) Let  $A$  be a domain,  $p \in Spec(a)$  a prime ideal, Then, there exists a valuation ring  $R$  of  $K = Quot(A)$  such that  $\mathfrak{m}_R \cap A = p$ .

*Proof.* Replace  $A$  with  $A_p$  if needed, so that we may assume  $A$  is local with maximal ideal  $p$ . Let  $H = \{B \subset K : B \text{ local, } \mathfrak{m}_B \cap A = p\}$ . Then, it is easy to check that the union of a chain of ascending local rings is again a local ring, with maximal ideal containing  $p$ . Applying Zorn's lemma gives us the maximal local ring  $R$  containing  $A$  such that  $\mathfrak{m}_R \cap A = p$ . It remains to show that  $R$  is local.

Suppose  $x \in K$  but  $x \notin R$ . Suppose neither  $x, \frac{1}{x}$  is in  $R$ ; if either  $x, \frac{1}{x}$  is integral over  $R$ , then  $R[x]$  has a maximal ideal lying over  $p$ . After localization, we get a local ring lying over  $A$  that strictly contains  $R$ , which contradicts maximality. In particular,  $\frac{1}{x}$  is not integral over  $R$ , and we claim that  $\mathfrak{p}^e$  in  $R[\frac{1}{x}]$  is not the entire ring: suppose other wise, then  $1 = a_0 + \frac{a_1}{x} + \dots + \frac{a_n}{x^n}$ , where  $a_i \in p$ . Multiplying  $x^n$  to both sides yields  $(1 - a_0)x^n + a_1x^{n-1} + \dots + a_n = 0$ , and since  $1 - a_0$  is a unit, this shows  $x$  is integral over  $R$ , a contradiction. Thus,  $R[\frac{1}{x}]$  localized at  $p^e$  gives us a local ring with maximal ideal  $\mathfrak{m}'$  lying over  $p$ . ( $p \subseteq A \cap \mathfrak{m}'$ , then apply maximality ). This contradicts maximality of  $R$ , therefore one of  $x, \frac{1}{x}$  is in  $R$ . □

## 7 Artin Rings

**Definition 7.1.** A commutative ring  $R$  is called Artin, if every descending chain of ideals  $(I_n)$  is stationary.

**Proposition 7.1.** Let  $R$  be Artinian. Then the following hold:

1. If  $\Sigma$  is a multiplicative system, then  $\Sigma^{-1}R$  is also Artinian.
2. If  $I \subset R$  is an ideal. Then,  $R/I$  is Artinian.
3. An integral Artinian domain is a field.
4.  $Spec(R) = Max(R)$  is finite.

*Proof.* To 1, 2, ideals under localization and quotients have nice correspondence with those in  $R$  that respects inclusion.

To 3, given any  $a \neq 0 \in R$ , where  $R$  is an Artinian domain, the chain  $(a) \subseteq (a^2) \subseteq (a^3) \dots$  must stabilize, so  $(a^{n+1}) = (a^n)$  for some  $n$ . But this implies  $a^n = a^{n+1}r$ , which implies  $a^n(1 - ar) = 0$ . By  $R$  being a domain, we get  $a$  is invertible.

To 4, let  $p \in \text{Spec}(R)$ . Then,  $R/p$  is an Artinian domain. Then,  $R/p$  must be a field. Thus, all primes are maximal.

If  $\mathfrak{m}_1, \mathfrak{m}_2, \dots$  is infinite, then we claim  $\mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \dots \supset \mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3 \dots$  does not stabilize: suppose otherwise  $\mathfrak{m}_1\mathfrak{m}_2 \dots \mathfrak{m}_k = \mathfrak{m}_1 \dots \mathfrak{m}_{k+1} \subseteq \mathfrak{m}_{k+1}$  for some  $k$ . By primeness, this implies  $\mathfrak{m}_j \subseteq \mathfrak{m}_{k+1}$  for some  $1 \leq j \leq k$ , which contradicts maximality.  $\square$

**Lemma 7.1.** If  $R$  is Artin or Noetherian of Krull dimension 0, then  $J(R) = N(R)$  is nilpotent.

*Proof.* In Artinian rings or any ring of Krull dimension 0, all prime ideals are maximal, and we get the equality  $J(R) = N(R)$ .

In the case of  $R$  is Artin, by DCC,  $(N^n(R))_{n \in \mathbb{N}}$  stabilizes at an ideal  $I$  where  $I \subseteq N(R)$ . Suppose  $I \neq 0$ . Then, let  $H$  be the set of all ideals of  $R$  whose product with  $I$  is not 0. The set is non-empty since  $I$  is in  $H$ ; by artinian assumption, the set has a minimal element, call it  $\mathfrak{a}$ . By construction, there exists  $x \in \mathfrak{a}$  such that  $(x)I \neq 0$ , so we must have  $(x) = \mathfrak{a}$  by minimality. However,  $((x)I)I = (x)I$ , so  $(x)I = (x)$ . In particular, this implies  $xi = x$  and consequently  $xi^n = x$  for some  $i \in N(R)$  and  $n \in \mathbb{N}$ . However,  $i$  is nilpotent, which contradicts the assumption that  $x \neq 0$ .

In the case where  $R$  is Noetherian, we simply note that  $N(R) = \text{rad}((0))$ , and  $\text{nil}((0))^k \subseteq (0)$  for  $k$  large enough by proposition 5.2.3,  $\square$

If  $R$  is Artin or Noetherian of dimension 0, then every prime is both maximal and minimal, which means  $\text{Max}(R)$  is finite. We now present a proof of structure theorem for Artin rings, with an argument that also applies for Noetherian rings of dimension 0 without knowing a priori that they are in fact equivalent.

**Theorem 7.2.** (Structure Theorem) If  $R$  is Artin or Noetherian of dimension 0 with  $\text{Max}(R) = \{m_1, \dots, m_r\}$  is finite. Moreover,  $R \cong R/(m_1)^n \times \dots \times R/m_r^n$ . Hence,  $R$  is a product of local Artinian rings.

*Proof.* We know the  $J(R)^n = (\cap_{i=1}^k \mathfrak{m}_i)^n = 0$  for some  $n$  by Lemma 7.1. The goal is to use the Chinese Remainder Theorem and show that  $R \cong R/(0) = R/J(R)$  has the desired form. First, we note that  $\mathfrak{m}_i + \mathfrak{m}_j = 1$  by maximality, so  $(\mathfrak{m}_i)$  are pairwise coprime. Furthermore, this implies that  $\mathfrak{m}_i^n + \mathfrak{m}_j^n = 1$  for all  $i, j$ : if not, then there exists minimal prime  $p$  over  $\mathfrak{m}_i^n + \mathfrak{m}_j^n$ , which implies  $\mathfrak{m}_i^n \subseteq p$  and  $\mathfrak{m}_j^n \subseteq p$ , which in turn implies  $\mathfrak{m}_i \subseteq p$  and  $\mathfrak{m}_j \subseteq p$ , which is impossible. Thus,  $(\mathfrak{m}_i^n)$  are also pairwise coprime. It follows that  $0 = (J(R))^n = \prod \mathfrak{m}_i^n$ , since intersection of ideals is product of ideals when the ideals are coprime. It is then a straight application of Chinese Remainder Theorem that  $R \cong R/(m_1)^n \times \dots \times R/m_r^n$ .

Lastly, note that each ring of the form  $R/(\mathfrak{m}^k)$  is local: any suppose  $\mathfrak{m}^k \subset p$  for  $p$  prime, then for every  $m \in \mathfrak{m}$ , we have  $m^k \in p$ , so by primeness we have  $m \in p$ , and  $\mathfrak{m} \subseteq p$ . Thus, the only prime ideal is the image of  $\mathfrak{m}$ .  $\square$

**Theorem 7.3.** (Relations of Artin Rings and Noether Rings) Let  $R$  be a commutative ring. The following are equivalent:

1.  $R$  is an Artin ring
2.  $R$  is Noether and Krull dimension of  $R$  is 0.

*Proof.* Step one is reduce to the case where  $R$  is local by structure theorem, since product of Noetherian rings is Noetherian and product of Artin rings is Artin.

Now assume  $(R, \mathfrak{m})$  is a local Artin ring. For  $k > 0$ , we have the exact sequence of  $R$ -modules

$$0 \longrightarrow \mathfrak{m}^k / \mathfrak{m}^{k+1} \xrightarrow{i} R / \mathfrak{m}^{k+1} \xrightarrow{p} R / \mathfrak{m}^k \longrightarrow 0$$

where  $i$  is the inclusion map and  $p$  is the canonical projection. By proposition 9.2, which we will prove latter,  $R / \mathfrak{m}^{k+1}$  is Noetherian provided both  $R / \mathfrak{m}^k$  and  $\mathfrak{m}^k / \mathfrak{m}^{k+1}$  are Noetherian. Moreover,  $R$  being Artinian implies  $\mathfrak{m}^k = 0$  for  $k$  large enough, and we have  $R / \mathfrak{m}^k \cong R$  for  $k$  large enough. Our goal is to inductively show  $R / \mathfrak{m}^k$  Noetherian for all  $k$ : when  $k = 1$ ,  $R / \mathfrak{m}$  is a field and thus Noetherian; now suppose  $R / \mathfrak{m}^n$  is Noetherian.

Note  $\kappa := R / \mathfrak{m}$  is a field, and  $\kappa$  acts on  $\mathfrak{m}^n / \mathfrak{m}^{n+1}$  in the following way:  $\bar{r} \cdot \bar{m} := \overline{rm}$ . So,  $\mathfrak{m}^n / \mathfrak{m}^{n+1}$  has a canonical  $\kappa$ -vector space structure.

In particular, there is an inclusion preserving bijection

$$\{\kappa\text{-vector subspaces of } \mathfrak{m}^n / \mathfrak{m}^{n+1}\} \iff \{R\text{-ideals } \mathfrak{n} : \mathfrak{m}^{n+1} \subseteq \mathfrak{n} \subseteq \mathfrak{m}^n\} = \epsilon$$

Note  $R$  Artinian implies  $R / \mathfrak{m}^{n+1}$  is Artinian. Thus, the set  $\epsilon$  is finite, and  $\mathfrak{m}^n / \mathfrak{m}^{n+1}$  is a finite dimensional vector space. This condition forces  $\epsilon$  to satisfy both ACC and DCC, and by ideal correspondence,  $\mathfrak{m}^k / \mathfrak{m}^{k+1}$  as an  $R$ -module satisfies ACC and is thus Noetherian.

For the converse, let  $(R, \mathfrak{m})$  be a Noetherian local ring of dimension 0. Note we also have  $\mathfrak{m}^k = 0$  for  $k$  large enough, since  $\mathfrak{m} = N(R)$ , which is nilpotent by proposition 7.1.

We proceed inductively as before: if  $k = 0, 1$  then  $R / \mathfrak{m}^k$  is clearly Artin. Now suppose it holds for  $k = n$  such that  $R / \mathfrak{m}^n$  is Artin. By using the same argument as before,  $R / \mathfrak{m}^{n+1}$  is Noetherian and satisfies ACC, so  $\mathfrak{m}^n / \mathfrak{m}^{n+1}$  is again finite dimensional, which forces  $\mathfrak{m}^n / \mathfrak{m}^{n+1}$  satisfying DCC as well.  $\square$

## 8 Krull's Theorem on Noetherian Rings

**Definition 8.1.** Let  $R$  be a commutative ring;  $\mathfrak{a} \subset R$  a proper ideal. Consider  $\mathfrak{a}^n$  and the projection  $p_n : R / \mathfrak{a}^{n+1} \rightarrow R / \mathfrak{a}^n$ . Then,  $(R / \mathfrak{a}^n, p_n)_{n \in \mathbb{N}}$  is a projective system. The limit  $\hat{R} := \varprojlim R / \mathfrak{a}^n$ , together with  $i : R \rightarrow \hat{R}$  is called  **$\mathfrak{a}$ -adic completion** of  $R$ .

**Proposition 8.1.** The kernel of the inclusion  $\pi : R \rightarrow \hat{R}$  is the intersection of all  $\mathfrak{a}^n$ .

*Proof.* We note  $a \in \ker(\pi)$  iff  $\pi(a) = 0$  iff  $p_n(a) = 0$  for all  $n$  iff  $a \in \bigcap_{i=0}^{\infty} \mathfrak{a}^i$ .  $\square$

The reason we refer  $i$  as the inclusion map is because when  $R$  is Noetherian and local/integral, the kernel of  $i$  is trivial by the following theorem by Krull.

**Theorem 8.1.** (The Intersection Theorem) Let  $R$  be a Noetherian ring that is local or integral. Let  $\mathfrak{a} \subset R$  be a proper ideal. Then,  $\bigcap_{n=0}^{\infty} \mathfrak{a}^n = 0$ . In particular, the inclusion map in the  $\mathfrak{a}$ -adic completion is injection.

*Proof.* Suppose  $R$  is Noetherian and local with maximal ideal  $\mathfrak{m}$ . By Noetherian assumption, the ideal  $\mathfrak{a}_0 := \bigcap \mathfrak{a}^k$  is finitely generated. Moreover,  $\mathfrak{m}_0 := \bigcap \mathfrak{m}^k$  is f.g with  $\mathfrak{a}_0 \subseteq \mathfrak{m}_0$ . We then have  $\mathfrak{m} \cdot \mathfrak{m}_0 = \mathfrak{m}_0$ , and apply Nakayama's lemma, we get  $\mathfrak{m}_0 = (0)$ .

Now suppose  $R$  is Noetherian and integral, and choose  $\mathfrak{m}$  be a maximal ideal over  $\mathfrak{a}$ . The integral assumption implies  $\phi : R \rightarrow R_{\mathfrak{m}}$  is injective, and we reduce to the local case.  $\square$

**Example 8.1.** The intersection theorem does not hold for generic Noetherian Rings. For example, in  $\mathbb{Z}/6$ , which is not a domain nor local, and the ideal  $I = (2)$  is idempotent. Thus,  $\bigcap_{i=0}^{\infty} I = I$ .

**Definition 8.2.** Given a ring  $R$  and  $I$  an ideal, we equip  $R$  with  $I$ -adic topology given by the following basis  $\{x + I^n : x \in R, n \in \mathbb{N}\}$ . Moreover, a sequence of points  $(x_n)$  is called Cauchy if for every  $k > 0$ , there exists  $N$  such that for  $m, n > N$ , we have  $x_n - x_m \in I^k$ .

It is standard to verify that this is well-defined basis. Heuristically, the larger  $n$  the smaller the open neighborhood is. In particular, the intersection theorem says if  $R$  is Noetherian and integral/local, then the  $I$ -adic topology is Hausdorff. (an element eventually lives outside of  $I^n$  for  $n$  large enough). Then, the  $I$ -adic completion  $\widehat{R}_I$  is the topological completion of  $R$ .

It is easy to extend the whole package of definitions up to this point to  $R$ -modules. Given an  $R$ -modules  $M$  equipped with a choice of  $I$ -adic topology and a submodule  $N$ , it is natural to ask whether the subspace topology and  $I$ -adic topology on  $N$  agrees. The Artin-Rees lemma gives us a positive answer in the case when the ring is Noetherian and  $M$  is finitely generated.

**Theorem 8.2.** (Artin-Rees Lemma) Let  $R$  be a Noetherian ring and  $I$  an ideal. Let  $M$  be a finitely generated  $R$ -module and  $N \subset M$  a submodule. Then, there exists an integer  $k \geq 1$  such that for  $n \geq k$ , we have

$$I^n M \cap N = I^{n-k} (I^k M \cap N)$$

Before proving Theorem 8.2, we first set up some necessary tools.

**Definition 8.3.** Let  $R$  be a ring and  $I \subset R$  an ideal. Then, the blow-up algebra of  $R$  is the graded  $R$ -algebra

$$B_I R := \bigoplus_{i=0}^{\infty} I^i$$

Note that when  $R$  is Noetherian,  $I$  is finitely generated as an  $R$ -module, and the generators generate  $B_I R$  as an  $R$ -algebra, which implies  $B_I R$  is a Noetherian ring as well.

**Definition 8.4.** Let  $R$  be a ring and  $I \subset R$  an ideal, and let  $M$  be an  $R$ -module. A filtration  $M = M_0 \supset M_1 \supset \dots$  is called an  $I$ -filtration if  $IM_n \subset M_{n+1}$  for all  $n$ . The filtration is called  $I$ -stable if  $IM_n = M_{n+1}$  for  $n$ -large enough. Given an  $I$ -filtration  $J$  of  $M$ , define the blow-up module as  $B_J M := \bigoplus_{i=1}^{\infty} M_i$ .

Note that  $B_J M$  has a natural  $B_I R$ -module structure. We now introduce a proposition that relates stability and finite generation of blow-up modules.

**Proposition 8.2.** Let  $R$  be a ring,  $I \subset R$  an ideal, and let  $M$  a finitely generated  $R$ -module with  $I$ -filtration  $J : M = M_0 \supset M_1 \supset \dots$ , where each  $M_i$  is finitely generated. Then, the filtration  $J$  is  $I$ -stable iff the  $B_I R$ -module  $B_J M$  is finitely generated.

*Proof.* Easy Exercise. □

We are now ready to prove Artin-Rees:

*Proof of Theorem 8.2.* Note  $B_J M \cap N$  has a natural  $B_I R$ -module structure, which makes it a submodule of  $B_J M$ . In particular, if  $J$  is an  $I$ -stable filtration of  $M$ , then  $B_J M$  is finitely generated over a Noetherian ring  $B_I R$ , so the submodule  $B_J M \cap N$  is a finitely generated  $B_I R$ -module, which implies the desired equality. □

**Theorem 8.3.** If  $R$  is Noetherian, then all  $\mathfrak{a}$ -adic completions of  $R$  is Noetherian.

*Proof.* Let  $(f_1, \dots, f_n)$  be a set of generators for a given  $\mathfrak{a}$ . There is a natural surjection from the power series ring  $R[[x_1, \dots, x_n]] \rightarrow \widehat{R}_{\mathfrak{a}}$  given by the map  $x_i \mapsto f_i$ . Then,  $\widehat{R}_{\mathfrak{a}}$  is a quotient of a Noetherian ring and is thus Noetherian. □

**Definition 8.5.** Let  $R$  be a ring. For  $r \in R$ , define  $\text{Spec}_{\min}(r) := \{p \in \text{Spec}(R) : (r) \subset p \text{ minimal}\}$ . For a set of elements  $\{r_1, \dots, r_n\}$ , define similarly  $\text{Spec}_{\min}(r) = \{p \in \text{Spec}(R) : (r_1, \dots, r_n) \subset p \text{ minimal}\}$

**Definition 8.6.** For  $p \in \text{Spec}(R)$ , the height of  $p$  is the krull dimension of  $R_p$ . The coheight is the krull dimension of  $R/p$ .

**Proposition 8.3.**  $\text{height}(p) + \text{coheight}(p) \leq \text{Krull dimension of } R$ .

*Proof.* Trivial. □

**Definition 8.7.** For  $q \in \text{Spec}(R)$ , the symbolic  $n$ -th power of  $q$  is defined as  $q^{(n)} := q^n R_q \cap R$ . In other words,  $q^{(n)} = \{r \in R : sr \in q^n \text{ for some } s \in R \setminus q\}$

**Lemma 8.4.**  $q^{(n)} R_q = (q R_q)^n$ .

*Proof.* Suppose  $x \in (q R_q)^n$ , then  $x = x_1 \dots x_n$  where  $x_i = \frac{r_i}{s_i}$ , where  $r_i \in q$  and  $s_i \in R \setminus q$ . It is clear that  $(\prod s_i)x \in q^n$ , so  $x = \frac{\prod x_i}{\prod s_i} \in q^{(n)} R_q$ ; on the other hand, if  $y \in q^{(n)} R_q$ , then  $y = \frac{m}{n}$  where  $m \in q^{(n)}$  and  $n \in R \setminus q$ . By definition, there exists  $s \in R \setminus q$  such that  $sm = q_1 \dots q_n \in q^n$ , where  $q_i \in q$ . Then,  $y = \frac{m}{n} = \frac{q_1 \dots q_n}{sn} = \prod \frac{q_i}{sn} \in (q R_q)^n$ . □

**Lemma 8.5.** For  $q \in \text{Spec}(R)$ , the  $n$ th symbolic power  $q^{(n)}$  is primary. If  $ax \in q^{(n)}$ , and  $x \notin q$ , then  $a \in q^{(n)}$ .

*Proof.* Note that  $q^{(n)}$  is the contraction of the ideal  $q^n R_q$ , which is a power of maximal ideal and thus primary. Thus,  $q^{(n)}$  is primary as well. By definition, if  $ax \in q^{(n)}$ , then  $a(sx) \in q^n$  with  $s, x \notin q$ , which implies  $a \in q^{(n)}$ .  $\square$

**Theorem 8.6.** (Krull's Principal Ideal Theorem/ Hauptidealsatz) Let  $R$  be a Noetherian ring. Then, for all non-units  $r \in R$ , one has  $\text{height}(q) \leq 1$  for all  $q \in \text{Spec}_{\min}(r)$ , with equality when  $r$  is not a zero-divisor.

*Proof.* Suppose there exists a chain  $q_0 \subset q$  of prime ideals, and we want to show that  $\text{height}(q_0) = 0$ , so that  $\text{height}(q) \leq 1$ . We may localize at  $q$  so that we may assume  $R$  is local with maximal ideal  $q$ . By the assumption that  $p$  is minimal over  $r$ , the ring  $R/(x)$  is Noetherian and of dimension 0, hence Artinian. Thus, the chain

$$(r) + q_0^{(n)}$$

stabilizes. Say we have  $(r) + q_0^{(k)} = (r) + q_0^{(k+1)}$ . It follows that  $q_0^{(k)} \subset (r) + q_0^{(k+1)}$ , so for any  $f \in q_0^{(k)}$  we may write  $f = ar + g$  with  $g \in q_0^{(k+1)}$ . It is immediate that  $ar \in q_0^{(k)}$ , but  $r \notin q_0$  by minimality, so  $a \in q_0^{(k)}$ .

From this we have  $q_0^{(k)} = (x)q_0^{(k)} + q_0^{(k+1)}$ . Taking things modulo  $q_0^{(k+1)}$ , we have  $x \in J(R)$ , and an application of Nakayama's lemma says  $q_0^{(k)} = q_0^{(k+1)}$ . We further localize to  $R_{q_0}$ , and Lemma 8.4 and another application of Nakayama's lemma gives us  $(q_0 R_{q_0})^k = 0$ . In other words, the maximal ideal  $q_0 R_{q_0}$  is nilpotent in the local ring  $R_{q_0}$ . It follows that  $q_0 R_{q_0} \subseteq N(R_{q_0})$ , which forces  $q_0 R_{q_0}$  to be the unique prime ideal. We have  $R_{q_0}$  is of dimension 0, as desired.

For the second part of the statement, if  $\text{height}(q) = 0$ , then  $q$  is nilpotent in  $R_q$ , and let  $n$  be minimal such that  $r^n = 0 \in R_q$ , which implies  $sr^n = 0 \in R$  for some  $s \neq 0$ . By minimality,  $sr^{n-1} \neq 0$ , so  $r$  must be a zero divisor.  $\square$

**Definition 8.8.** A sequence of elements  $r_1, \dots, r_n$  is called a **regular** sequence if  $(x_1, \dots, x_d)$  is a proper ideal for all  $d \leq n$ , and  $r_i$  is not a zerodivisor in  $R/(r_1, \dots, r_{i-1})$  for all  $i \leq n$ .

We have a generalization of the PIT for a system of elements:

**Theorem 8.7.** (Krull's Dimension Theorem) Let  $R$  be a Noether ring, and  $r = (r_1, \dots, r_m)$  a system. Then  $\text{Spec}_{\min}(r)$  contains prime ideals of height  $\leq m$ , with equality when  $r$  is regular.

*Proof.* We proceed by induction:  $n = 1$  is PIT; now assume the dimension theorem holds for  $n = m$ . Given  $r = (r_1, \dots, r_{m+1})$ , and  $p \in \text{Spec}_{\min}(r)$ , let  $q \subset p$  be a maximal prime ideal contained in  $p$ . Our goal is to show that  $\text{ht}(q) = m$ , which immediately implies that  $\text{ht}(p) = m + 1$ . By localizing at  $p$ , we may assume that  $R$  is local with maximal ideal  $p$ .

Since  $q$  is properly contained in  $p$ , we have WLOG that  $r_{m+1} \notin q$  by minimality. Consider  $\mathfrak{a} = q + (r_{m+1})$ ,  $q \subset \mathfrak{a} \subseteq p$ . Then,  $\text{nil}(\mathfrak{a}) = p$  since  $p$  is the only prime ideal containing  $\mathfrak{a}$ . By definition, we have  $r_i \in p$  for all  $i = 1, \dots, m + 1$ , and there exists  $a_i \in R$  and  $s_i \in q$  such that  $r_i^{n_i} = s_i + a_i r_{m+1}$ . Thus, we have  $r_i^{n_i} \in (s_1, \dots, s_m, r_{m+1})$ , and a prime containing  $(s_1, \dots, s_m, r_{m+1})$  will contain all  $r_i$  as well. It follows that  $p$

is minimal over  $(s_1, \dots, s_m, r_{m+1})$ . Let  $s = (s_1, \dots, s_m)$ . The image of  $p$  under the quotient map  $R \rightarrow R/s$  is minimal over  $r_{m+1}$ . Therefore by PIT,  $\bar{p}$  has height at most 1, which forces the image of  $q$  having height 0, which means  $q$  is minimal over  $(s_1, \dots, s_m)$ . By induction hypothesis, we are done.

Note that in our proof,  $\bar{p}$  has height 1 when  $r_{m+1}$  is not a zero-divisor under the quotient by PIT, which is equivalent to saying the system is regular.

□

**Corollary 8.7.1.** Let  $R$  be Noether. Then, the following hold:

1. Every descending sequence of prime ideals is stationary.
2. if  $ht(p) = m$ , then there exists a regular system of length  $m$  with  $p$  a minimal prime over it.

*Proof.* To 1: every prime ideal in a Noetherian ring is finitely generated. In particular, given  $p$  we can find a system of generators  $(r_1, \dots, r_m)$  for  $p$  such that  $p$  is minimal over the system by definition. Then,  $ht(p) \leq m$  by dimension theorem.

To 2: we proceed by induction: it is trivial if  $m = 1$  by taking the system  $r = (0)$ . Inductively suppose  $m = k + 1$ . Let  $p_1 \subset \dots \subset p_k \subset p_{k+1} = p$  be a chain of length  $k + 1$ . Then,  $p_k$  is minimal over a regular system  $(x_1, \dots, x_k)$ . First, quotient out the bottom prime so the ring is assumed to be integral. By Noetherian assumption, there is only a finite set of primes  $\{q_i\}$  minimal over  $(x_1, \dots, x_k)$ . Then by prime avoidance,  $p$  cannot be contained in the union of  $\{q_i\}$ , otherwise contradicting minimality. Therefore, we may choose an element  $x_{k+1} \notin (x_1, \dots, x_k)$  such that  $p$  is minimal over  $(x_1, \dots, x_{k+1})$ , and it is regular.

□

## 9 Modules over special classes of rings

### 9.1 Modules over PIDs

The motivating fact for the following lemma is this: given a non-zero functional on a finite dimensional real vector space  $\phi : V \rightarrow \mathbb{R}$ , the range is one dimensional, say generated by  $v \in V$ . Then, we may decompose  $V$  as  $V = \text{span}(v) \oplus \ker(\phi)$ .

**Lemma 9.1.** Let  $R$  be a PID and  $M$  a free  $R$ -module. Given a submodule  $N \subset M$ , there exists  $y, y_1 \in N$  and  $v \in \text{Hom}_R(M, R)$  such that the following hold:

1.  $M = Ry_1 \oplus \ker(v)$ ;
2.  $N = Ry \oplus (N \cap \ker(v))$

*Proof.* The proof is trivial if  $N = 0$ , so assume  $N$  is not trivial. First, note that for any  $\phi \in \text{Hom}_R(M, R)$ , the image  $\phi(N)$  is an ideal of  $R$  and thus principally generated by some element  $a_\phi \in R$ . Let

$$\Sigma = \{a_\phi : \phi \in \text{Hom}_R(M, R)\}$$

Then,  $\Sigma$  is not empty because  $0 \in \Sigma$ . Since PID are noetherian,  $\Sigma$  has a maximal element. Let  $v$  be the homomorphism such that  $v(N) = (a_v)$  is maximal, and  $y \in N$  be the element such that  $v(y) = a_1$ . To see that  $a_1$  is not trivial, it suffices to demonstrate one homomorphism where  $N$  is not contained in the kernel. Let  $(x_1, \dots, x_n)$  be a basis for  $M = \bigoplus_{i=1}^n Rx_i$ . Since  $N \neq 0$ , there must be the projection map onto the  $i$ th summand restricts to a homomorphism where  $N$  is not contained in the kernel.

The next step is to demonstrate  $a_1$  divides all  $\phi(y)$  for  $\phi \in \text{Hom}_R(M, R)$ . Note that ideal generated by  $a_1$  and  $\phi(y)$  is principal, and let  $b$  be its generator. Then, we may write  $b = r_1 a_1 + r_2 \phi(y)$  for some  $r_1, r_2 \in R$ .



Consider the homomorphism  $r_1v + r_2\phi \in \text{Hom}_R(M, R)$ , which sends  $y$  to  $r_1v(y) + r_2\phi(y) = b$ . Therefore by maximality, we must have  $(a_1) = (b)$ , and it follows that  $a_1|\phi(y)$ .

In particular, we have  $a_1|\pi_i(y)$ , where  $\pi_i$  is the projection onto the  $Rx_i$  summand. In other words,  $y = \sum_{i=1}^n (a_1b_i)x_i$  for  $b_i \in R$ . By factoring out the  $a_1$  term from the coefficients, we get  $y_1 := \sum_{i=1}^n (b_i)x_i$  where  $v(y_1) = 1$ . The claim is that  $M = Ry_1 \oplus \ker(v)$  and  $N = Ry \oplus (N \cap \ker(v))$ . For the first equality, we note that every  $x \in M$  can be written as  $x = v(x)y_1 + (x - v(x)y_1)$ , where  $(x - v(x)y_1) \in \ker(v)$  by a direct verification. For the second equality, for every  $x' \in N$ , we have  $x' = v(x')y_1 + (x' - v(x')y_1)$ . Note that  $a_1|v(x')$ , so  $v(x')y_1 \in Ry$ ; by similarly reasoning, we have  $(x' - v(x')y_1) \in N$  and  $v(x' - v(x')y_1) = 0$ . Both sums are easily seen to be direct.  $\square$

**Theorem 9.2.** Every submodule of a finitely generated free module over PID is free.

We use induction on rank. Suppose  $N \subset M$  is of rank 0, then it must be torsion and any non-zero submodule of a free module is torsion free. Thus,  $N = 0$  and it is free. Suppose the statement holds for submodules of rank  $m$ . For submodule  $N$  of rank  $m+1$ , we decompose  $N = Ry \oplus N \cap \ker(v)$ , where  $N \cap \ker(v)$  must be of rank  $m$ . It follows from the induction hypothesis that  $N$  is a direct sum of free modules and thus free.

Note that we may alter the proof slightly by choosing a well-ordered basis for  $M$  if it is not finitely generated and use transfinite induction to prove the result in general.

**Theorem 9.3.** (Invariant Factors Theorem) Let  $R$  be a principal ideal domain and  $M$  a free  $R$ -module,  $N \subset M$  a submodule. Then, there exists  $R$ -basis  $A = (\alpha_1, \dots, \alpha_m)$  of  $M$  and  $\delta_1|\delta_2|\dots|\delta_n$  in  $R$  such that  $\delta_1\alpha_1, \dots, \delta_n\alpha_n$  is an  $R$ -basis for  $N$ , unique up to association.

*Proof.* We induct on rank of  $M$ : if rank of  $M = 0$ , then there is nothing to prove. Suppose the statement holds for  $\text{rk}(M) = n$ . Since  $M = Ry_1 \oplus \ker(v)$ , we know there is a basis  $y_2, \dots, y_n$  of  $\ker(v)$  and  $\delta_2|\dots|\delta_n$  such that  $\delta_2\alpha_2, \dots, \delta_n\alpha_n$  is an  $R$ -basis for  $N \cap \ker(v)$ . We are left to show that  $\delta_1 := a_1$  divides all  $\delta_i$ , and in particular it suffices to prove  $\delta_1|\delta_2$ . The proof follows from the similar vein as in Lemma 9.1, based on the maximality of  $\delta_1$ .  $\square$

**Theorem 9.4.** (Structure Theorem) Let  $R$  be a PID, and  $M$  a finite  $R$ -module. Then, there exists non-units  $\delta_1|\dots|\delta_n$  unique up to association such that  $M \cong \oplus R/(\delta_i) \oplus R^f$

*Proof.* Let  $(x_1, \dots, x_n)$  be a system of generators for  $M$ . Let  $f : R^n \rightarrow M$  be the morphism given by  $e_i \mapsto x_i$ . Then, the kernel is a submodule of  $R^n$ , so by invariant factors theorem we get a basis  $(e'_1, \dots, e'_n)$  for  $R^n$  and a basis  $\delta_1e'_1, \dots, \delta_me'_m$  for  $\ker(f)$ . By isomorphism theorem, we have

$$M \cong R^n / \ker(f) = Re'_1 \oplus \dots \oplus Re'_n / R\delta_1e'_1 \oplus \dots \oplus R\delta_me'_m \cong \oplus R/(\delta_i) \oplus R^{n-m}$$

For uniqueness, given  $M \cong \oplus R/(\delta_i) \oplus R^f$  and the projection  $p : R^n \rightarrow M$ . We get  $N = \ker(p)$  has basis required in the invariant factors theorem, which is unique.  $\square$

**Corollary 9.4.1.** The following hold for finitely generated modules over PID:

1.  $M$  is torsion free iff  $M$  is free.
2. The torsion submodule of  $M$  is finitely generated.

**Example 9.1.** For a finitely generated abelian group  $A$ ,  $A \cong \mathbb{Z}/(d_1) \oplus \dots \oplus \mathbb{Z}/(d^r) \oplus \mathbb{Z}^f$

**Example 9.2.** (Smith Normal Form) Given an  $n \times m$  matrix  $A$  with entries in PID, there exists a decomposition  $A = LDR$ , where  $L, R$  are invertible matrices representing row and column operations, and  $D$  is a diagonal matrix of the form

$$\begin{bmatrix} \delta_1 & & & \\ & \delta_2 & & \\ & & \dots & \\ & & & \delta_n \end{bmatrix}$$

where  $\delta_1 | \dots | \delta_n$ . The diagonal matrix is called the Smith Normal Form of  $A$ . In the context of Invariant factor theorem, the decomposition says that under the basis change to  $y_1, \dots, y_m$  given by  $R$ , the vectors  $\delta_1 y_1, \dots, \delta_n y_m$  spans the range, under the base change  $L$ .

The algorithm of reducing a matrix  $A$  to the smith normal form is as follows: starting with the first column, we may use elementary row operations to reduce the 1,1 entry to the  $d = \gcd(a_{1,1}, a_{2,1})$ :  $R$  being a PID implies there exists  $r_1, r_2 \in R$  such that  $r_1 a_{1,1} + r_2 a_{2,1} = d$  (note that having a Euclidean Algorithm will make this actually algorithmically computable instead of theoretically exists). The row operation corresponds to the matrix

$$\begin{bmatrix} r_1 & r_2 \\ -a_{1,1}/d & a_{2,1}/d \end{bmatrix}$$

which has determinant 1 and thus invertible. Now we can subtract and get rid of all entries in the first column other than  $a_{1,1} = d$ . Do the same for the first row, which possibly adds new entries back to the first column, but the number of prime factors of  $a_{1,1}$  reduces, therefore the algorithm must terminate.

Now we have obtained a diagonal matrix. To put it into the desired form, suppose  $\delta_1 \nmid \delta_2$ . Then, we may add  $\delta_2$  back to the first column, and perform the same operations to turn  $\delta_1$  into  $\gcd(\delta_1, \delta_2)$ . By the same reasoning, the process terminates.

**Example 9.3.** (Rational Canonical Form) Let  $k$  be a field and  $V$  a finite dimensional vector space over  $k$ . Fix some  $\varphi \in \text{End}(V)$ . Then,  $V$  becomes a  $k[t]$ -module by

$$p(t) \cdot v = p(\varphi)(v)$$

By Cayley-Hamilton,  $V$  is a finite-torsion  $F[t]$  module. Hence,  $V \cong F[t]/(\delta_1) \oplus \dots \oplus F[t]/(\delta_n)$ , with  $\delta_1 | \dots | \delta_n$ . Let  $\delta_i = t^{n_i} + a_{n_i-1}t^{n_i-1} \dots + a_0$ . Then  $R_i := R/(\delta_i)$  has basis  $(1, t, \dots, t^{n_i-1})$ . The action of  $t$  on the basis vectors is  $t \cdot x^k = x^{k+1}$  for  $k < n_i$  and  $t \cdot x^{n_i} = -(a_{n_i-1}t^{n_i-1} \dots + a_0)$ . Thus, each  $R_i$  has the matrix form

$$\begin{bmatrix} & & & & -a_0 \\ & & & & -a_1 \\ & & & & -a_2 \\ & & & & -a_3 \\ 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & \dots & \\ & & & & 1 & -a_{n_i-1} \end{bmatrix}$$

and  $V = R_1 \oplus \dots \oplus R_n$ .

**Proposition 9.1.** Given a  $n \times n$  matrix  $A$ , the invariant factors  $\delta_1, \dots, \delta_n \in k[t]$  can be determined by reducing the matrix  $A - tI$  to the smith normal form.

*Proof.* It is easy to prove the lemma that each block  $R_i - tI$  has a smith normal form

$$\begin{bmatrix} \delta_i & & & \\ & 1 & & \\ & & 1 & \\ & & & \dots \\ & & & & 1 \end{bmatrix}$$

The proposition follows from the fact that two matrices  $A, B$  are similar iff their characteristic matrices are equivalent (i.e you can get from the other through elementary matrix operations). In particular, the minimal polynomial of  $\phi$  is  $\delta_n$ , and the characteristic polynomial is the product  $\prod_{i=1}^n \delta_i$ .  $\square$

**Example 9.4.** We find the invariant factors of the matrix

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix}$$

It is easy to calculate the characteristic polynomial to be  $t(t-1)^3$ , and the minimal polynomial is  $t(t-1)^2$ . We see that this forces the invariant factors to be  $t-1$  and  $t(t-1)^2$ . The may sanity check by reducing the characteristic matrix to the smith normal form

$$A - tI \Rightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & t-1 & 0 \\ 0 & 0 & 0 & t(t-1)^2 \end{bmatrix}$$

This means the rational canonical form of  $A$  is

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 2 \end{bmatrix}$$

## 9.2 Noetherian/Artinian Modules

Let  $R$  be a (not necessarily commutative) ring, and  $M$  be a (left/right/bi) module. We say that  $M$  satisfies ACC/DCC iff that set of submodules satisfies ACC/BCC with respect to inclusion.

**Example 9.5.** If  $R$  is a Noetherian/artinian ring. Then it is a Noetherian/Artinian module over itself.

**Proposition 9.2.** (Characterization) Let  $M$  be an  $R$ -module. Then the following hold:

1.  $M$  satisfies ACC/DCC if every subset of submodules has maximal/minimal elements with respect to inclusions.
2.  $M$  satisfies ACC iff every submodule is finitely generated.

*Proof.* To 1: Suppose  $X$  is a subset of submodules. If the subset has no maximal/minimal elements, then there exists a non-stablizing ascending/descending chain of submodules, so  $M$  cannot satisfy ACC/DCC. Conversely, if there is a infinite ascending/descending chain of submodules of  $M$ , then collection of the submodules in the chain is a subset with no maximal/minimal elements.

To 2: If  $N \subseteq M$  is not finitely generated, we may inductively choose elements in  $x_i \in M \setminus M_{i-1}$ , where  $M_{i-1} := (x_1, \dots, x_{i-1})$  is the module generated by the elements in the parenthesis. Then,  $(M_i)_{i \in \mathbb{N}}$  is a non-stablizing ascending chain. Conversely, if  $(M_i)_{i \in \mathbb{N}}$  is a non-stablizing ascending chain of submodules, then  $\bigcup_{i=0}^{\infty} M_i$  is a submodule that is not finitely generated.  $\square$

**Proposition 9.3.** (Properties) The following hold:

1. If  $M$  satisfies ACC/DCC, then every submodule of  $M$  and quotient module of  $M$  satisfies ACC/DCC.
2. The category of  $R$ -modules satisfying ACC/DCC has finite products and coproducts.
3. Localization preserves ACC/DCC.

*Proof.* To 1: Trivial. To 2: Consider the projection  $p : M \rightarrow M/IM$ . The inverse image  $p^{-1}$  takes a submodule to a submodule, and it is (proper) inclusion preseving. Thus, every ascending/descending chain in  $M/IM$ ,  $M/IM$  lifts to an ascending/descending chain in  $M$ . To 3: In **R-Mod**, finite product and coproducts agree, and it suffices to consider the direct product  $M \times N$ . If  $M \times N$  has ascending/descending chain of submodules, then the projection map onto  $M$  and  $N$  takes the chain to ascending/descending chains as well. If both chains stablize after some finite degree  $n$ , then it is clear that the original chain stablize after degree  $n$  as well. To 4: consider the inclusion  $i : M \rightarrow \Sigma^{-1}M$ . The inverse image  $i^{-1}$  takes a submodule to a submodule, and it is (proper) inclusion preseving (a submodule in  $\Sigma^{-1}M$  is equal to the localization of its contraction). Thus, every ascending/descending chain in  $\Sigma^{-1}M$  lifts to an ascending/descending chain in  $M$ .  $\square$

**Proposition 9.4.** For  $R$ -module  $M$ , the following hold:

1. Given a short exact sequence

$$0 \longrightarrow M_0 \longrightarrow M_1 \xrightarrow{p} M_2 \longrightarrow 0$$

We have  $M_1$  satisfies ACC/DCC iff  $M_0$  and  $M_2$  satisfies ACC/DCC.

2. Let

$$0 \longrightarrow M_0 \longrightarrow M_1 \longrightarrow \dots \longrightarrow M_n \longrightarrow 0$$

Then,  $(M_{2k})$  satisfies ACC/DCC iff  $(M_{2k+1})$  does so.

*Proof.* To 1: assume  $M_1$  satisfies ACC/DCC: then  $M_0$  is canonically a submodule of  $M_1$  and  $M_2$  is a quotient  $M_1$ , so they satisfy ACC/DCC by Proposition 9.2.1; now suppose  $M_1$  does not satisfy ACC/DCC, which means there is a non-stablizing ascending/descending chain  $C = (C_n)$  of submodules. Now  $C \cap M_1$  is naturally a chain of submodules of  $M_0$ , and  $p(C)$  is an ascending/descending chain of submodules of  $M_2$ . Suppose by contradiction that both chain stabilizes, which means there exists  $N$  such that  $C_N + M_0 = C_{N+1} + M_0$  and

$C_N \cap M_0 = C_{N+1} \cap M_0$ . However, the first equality implies  $C_{N+1} - C_N \subset M_0$  for ascending ( $C_N - C_{N-1}$  for descending), and combined with the second equality we have  $C_N = C_{N-1}$ , a contraction.

To 2, we may break the long exact sequence to short exact sequences by adding in the kernel and cokernel terms. The result is then a simple corollary of part 1. □

Recall the discussion on composition series of  $R$ -modules. If a composition series exist, then all such have the same length and the same simple factors up to permutation.  $0 \subseteq M_1 \subseteq M_2 \subseteq \dots \subseteq M_n = M$  such that  $M_i/M_{i-1}$  is simple.

**Proposition 9.5.** Let  $M$  be a (left) modules. Then,  $M$  has a (left) composition series iff  $M$  satisfies ACC and DCC.

*Proof.* Let  $0 \subseteq M_1 \subseteq M_2 \subseteq \dots \subseteq M_n = M$  be a composition series, and make induction on  $n$ . For  $n = 1$ , the module is simple and it automatically satisfies ACC and DCC. For inductive step, suppose  $0 \subseteq M_1 \subseteq M_2 \subseteq \dots \subseteq M_n$  is a composition series, so  $M_n$  satisfies ACC and DCC. Then, there exists the exact sequence

$$0 \longrightarrow M_n \xrightarrow{f} M_{n+1} \xrightarrow{g} M_{n+1}/M_n \longrightarrow 0$$

and by proposition 9.2,  $M_{n+1}$  satisfies ACC and DCC since  $M_{n+1}/M_n$  is simple.

Suppose  $M$  satisfies ACC and DCC. In particular,  $M$  has minimal submodules  $M_1$  by DCC, which must be simple. Proceed inductively, and consider the set  $M' = \{N | M_1 \subset N\}$ , which also has minimal elements, say  $M_2$ . Then,  $M_2/M_1$  must be simple. By ACC, the sequence must terminate and we get a finite composition series. □

## 10 Integral extensions

### 10.1 Basic Facts

**Definition 10.1.** A commutative ring extension is any injective ring homomorphism  $R \hookrightarrow S$ . We denote such an extension by  $S|R$ . An element  $x \in S$  is called integral or algebraic if it is a root of a monic polynomial in  $R[t]$ .

**Example 10.1.** The canonical embedding  $\mathbb{Z} \hookrightarrow \mathbb{Q}$  is a ring extension. The only integral elements are elements in  $\mathbb{Z}$ . In general, if  $R$  is a UFD, then  $x \in S$  integral over  $R$  iff  $x \in R$ . For example,  $\mathbb{Z}[t] \hookrightarrow \mathbb{Q}[t]$ .

**Proposition 10.1.** Let  $S|R$  be a ring extension. Then, the following are equivalent:

1.  $x \in S$  is integral over  $R$ .
2.  $R[x]$  is a finite  $R$ -module
3. There exists a subring  $T$  such that  $R \subseteq T \subseteq S$  where  $x \in T$ , and  $T$  is a finite  $R$ -module.

*Proof.* For  $1 \implies 2$ , suppose  $x$  satisfies the minimal monic polynomial  $p(t) = t^n + a_{n-1}t^{n-1} + \dots + a_0$ . Then,  $R[x] \cong R[t]/(p(t))$ , which is a finite  $R$  module generated by  $1, t, \dots, t^{n-1}$ .  $2 \implies 3$  is trivial.

For  $3 \implies 1$ , suppose  $T$  as an  $R$  module is finitely generated by  $(v_1, \dots, v_n)$ . Then,  $x$  acts on  $T$  by left multiplication, and suppose  $xv_i = \sum_{j=1}^n a_{i,j}v_j$ . Let  $A = (a_{i,j})$  and  $v$  be the column vector  $(v_1, \dots, v_n)^T$ . Then, the equation says  $(A - xI)v = 0$ , which implies  $\det(A - xI) = 0$  (for  $R$  a domain, we may enlarge to the quotient field and the statement is purely linear algebra; for general  $R$ , this can be proven using Cramer's rule). Thus,  $x$  satisfies the characteristic polynomial of  $A$ , which makes it integral.  $\square$

The proof of proposition 10.1.3 generalizes to the famous Cayley-Hamilton Theorem

**Theorem 10.1.** (Cayley-Hamilton) Let  $R$  be a ring,  $I \subset R$  an ideal,  $M$  a finitely generated  $R$ -module that is generated by  $n$  elements. Fix  $\varphi \in \text{End}_R(M)$ . If

$$\varphi(M) \subset IM$$

then there exists a monic polynomial  $p(x) = x^n + p_1x^{n-1} + \dots + p_n$  with  $p_i \in I^i$  such that  $p(\varphi) = 0$ .

**Proposition 10.2.** Let  $S|R$  be a ring extension.

1. If  $x_1, \dots, x_n \in S$  are integral over  $R$ . Then,  $R[x_1, \dots, x_n]$  is a finite  $R$ -module.
2.  $\tilde{R} := \{x \in S : x \text{ integral over } R\}$  is a subring containing  $R$ .
3. If  $I \in \text{Id}(R)$ , and  $\tilde{I} = \{x \in S : x \text{ integral over } I\}$  is an ideal of  $\tilde{R}$  containing  $I$ . In particular, it is  $N(I\tilde{R})$ .

*Proof.* To 1: direct corollary of Proposition 10.1.2.

To 2. Note that if  $a, b$  are integral over  $R$ , then  $a + b$  and  $ab$  are contained in the ring  $R[a, b]$ , which by 1 is finite over  $R$ . By Proposition 10.1.3, we are done.

To 3: For the  $\tilde{I} \subseteq N(I\tilde{R})$  direction, let  $x \in \tilde{R}$  be integral over  $I$ , which means there is  $x^n + a_{n-1}x^{n-1} + \dots = 0$ . We may rewrite the equation as  $x^n = (-a_{n-1}x^{n-1} + \dots) \in I\tilde{R}$ , hence  $x \in N(I\tilde{R})$ . For the other direction, let  $y \in N(I\tilde{R})$ , which implies  $y^k = \sum_{i=1}^n b_i x_i$ , where  $b_i \in I$  and  $x_i \in \tilde{R}$ . Then,  $M = R[x_1, \dots, x_n]$  is finite module over  $R$ , and  $y^k M \subset IM$ . Left multiplication by  $y^k$  again is again an endomorphism of  $IM$ , and we finish by Cayley-Hamilton.  $\square$

**Definition 10.2.** Let  $S|R$  be a ring extension. The ring  $\tilde{R} = \{x \in S : x \text{ algebraic over } R\}$  is called integral closure of  $R$ .  $S|R$  is called integral if  $\tilde{R} = S$ .  $R$  is called integrally closed in  $S$  if  $\tilde{R} = R$ .

**Definition 10.3.** Let  $R$  be a domain and  $K$  its quotient field.  $R$  is called integrally closed if  $R$  is integrally closed in  $K$ .

**Proposition 10.3.** UFDs are integrally closed.

*Proof.* Suppose  $R$  is a UFD. Let  $f(t) = a_0 + \dots x^n$  be a monic polynomial in  $R[x]$ . Suppose  $\frac{p}{q} \in \text{Quot}(R)$  is a root to  $f(t)$  with  $\gcd(p, q) = 1$ . Then,  $q^n f(\frac{p}{q}) = p^n + a_{n-1}p^{n-1}q + \dots + a_0q^n = 0$ . In particular, we see  $q$  clearly divides every term of degree  $< n$ , so it must divide  $p^n$  as well. By  $\gcd$  assumption,  $q$  must be a unit, and  $\frac{p}{q} \in R$ . We conclude  $R$  is integrally closed.  $\square$

**Proposition 10.4.** Valuation rings are integrally closed.

*Proof.* Let  $R$  be a valuation ring, and  $f(t) = a_0 + \dots + t^n$  be a monic polynomial in  $R[t]$ . If  $b$  is a root to  $f(t)$ , we know one of  $b$  and  $b^{-1}$  is in  $R$ ; if  $b \in R$  we are done; if  $b^{-1} \in R$ , by  $f(b) = 0$  we get  $b + a_{n-1} + a_{n-2}b^{-1} \dots + a_0b^{-n+1} = 0$ , so  $b \in R$  as well. We conclude  $R$  is integrally closed.  $\square$

**Theorem 10.2.** Let  $R$  be a domain. Then,  $R$  is integrally closed iff  $R = \cap R_v$  where  $R_v$  is a valuation ring over  $R$  in the quotient field.

*Proof.* The intersection of integrally closed subrings of a common quotient field is clearly integrally closed in the quotient field: an element integral over the intersection is integral over every ring in the intersection, thus contained in every ring in the intersection.

Suppose  $R$  is integrally closed in the quotient field  $K$ . Clearly,  $R \subseteq \cap R_v$  where  $R_v$  are valuation rings lying over  $R$  since they are integrally closed. Conversely, if  $x \in K$  is an element not integral over  $R$ , then  $x^{-1} \notin R$  by the same argument as above. Let  $\mathfrak{m} \subset R$  be a maximal ideal containing  $x^{-1}$ . By Chevalley's extension theorem, there is a valuation ring  $(V, \mathfrak{m}_V)$  over  $R$  with  $\mathfrak{m}_V \cap R = \mathfrak{m}$ . In particular,  $V$  is a valuation ring containing  $x^{-1}$  but not  $x$ . Thus,  $R = \cap R_v$

$\square$

**Proposition 10.5.** The following hold:

1. (Transitivity) Let  $S_2|S_1|R$  be ring extensions. Then,  $S_2|R$  is integral iff  $S_2|S_1$  is integral and  $S_1|R$  is integral as well.
2. (Functoriality) Suppose  $S|R$  is integral,  $b$  a proper ideal of  $S$ , and let  $a := b \cap R$ . Then  $S/b|R/a$  is integral.
3. Let  $S|R$  be integral, and  $\Sigma$  be a multiplicative system of  $R$ . Then,  $S_\Sigma|R_\Sigma$  is integral.

*Proof.* To 1: if  $S_2|R$  is integral, then clearly both  $S_2|S_1$  and  $S_1|R$  are integral. Conversely, suppose  $S_2|S_1$  and  $S_1|R$  are integral. Given  $x \in S_2$ , we have  $x$  satisfying  $x^n + s_{n-1}x^{n-1} + \dots + s_0 = 0$ . Consider the subring  $R' := R[s_0, \dots, s_{n-1}]$ , which is a finite module over  $R$ . Then,  $R[x]$  is finite over  $R'$ , therefore finite over  $R$  as well.

To 2: Suppose we have  $x \in S$ , then  $x^n + p_{n-1}x^{n-1} + \dots + p_0 = 0$  for  $p_i \in R$ . Reduce the equation mod  $b$  gives us a monic polynomial over  $R/a$ .

To 3: Let  $\frac{s}{b} \in S_\Sigma$ . By integral assumption,  $s^n + p_{n-1}s^{n-1} + \dots + p_0 = 0$ . Replace  $p_i$  with  $p_i/b^i$  gives us a monic polynomial with coefficients in  $R_\Sigma$  and  $\frac{s}{b}$  a root.  $\square$

## 10.2 Going-Up Theorem

**Proposition 10.6.** Let  $S|R$  be a integral extension. If  $S$  is a domain, then  $S$  is a field iff  $R$  is a field. In particular, if  $\mathfrak{m}$  is maximal in  $S$  iff  $\mathfrak{m} \cap R$  is maximal.

*Proof.* First, assume  $R$  is a field. Take  $x \neq 0 \in S$ , and there exists  $a_0, \dots, a_{n-1} \in R$  such that  $a_0 + \dots + a_{n-1}x^{n-1} + x^n = 0$ . By the domain assumption, we may assume  $a_0 \neq 0$ , for otherwise we may factor out  $x^k$  as necessary. Then  $x(x^{n-1} + \dots + a_1) = -a_0$  is invertible, so  $x \in S^\times$ . Conversely, suppose  $x \in R$ . Then,

$x^{-1} \in S$  is integral over  $R$ , satisfying  $x^{-n} + p_{n-1}x^{-n+1} + \dots + p_0 = 0$ . Multiplying both sides with  $x^{n-1}$  shows  $x^{-1}$  is in  $R$  as well.

Finally, if  $\mathfrak{m} \in \text{Max}(S)$  and  $\mathfrak{n} = \mathfrak{m} \cap R$ . Then,  $S/\mathfrak{m}$  is integral over  $R/\mathfrak{n}$  by Proposition 10.5.2. Therefore,  $R/\mathfrak{n}$  is a field and thus  $\mathfrak{n}$  is maximal.  $\square$

**Proposition 10.7.** Let  $S|R$  be an integral extension. Suppose we have  $q_1, q_2 \in \text{Spec}(S)$  with  $q_1 \subseteq q_2$  such that  $q_1 \cap R = q_2 \cap R$ . Then,  $q_1 = q_2$ .

*Proof.* We may localize both ring at  $q_1 \cap R$ . Then,  $q_1, q_2$  are still primes in  $S$ , while  $q_1 \cap R$  is maximal in  $R$ . By Proposition 10.6, we have  $q_1, q_2$  both maximal, so we have  $q_1 = q_2$ .  $\square$

**Theorem 10.3.** Let  $S|R$  be a integral ring extension. Then, the following hold:

1. **(Lying-over)** For every  $p \in \text{Spec}(R)$ , there exists  $q \in \text{Spec}(S)$  such that  $q \cap R = p$ .
2. **(Going-up)** Let  $p_1 \subseteq p_2 \subseteq \dots \subseteq p_n$  be a chain in  $\text{Spec}(R)$ ,  $p_1 \subseteq p_2 \subseteq \dots \subseteq p_m$  a chain in  $\text{Spec}(S)$ , such that  $m < n$  and  $q_j \cap R = p_j$  for all  $j \leq m$ . Then, the chain in  $\text{Spec}(S)$  can be extended to length  $n$ . In particular, Krull dimension of  $R$  equals the Krull dimension of  $S$ .

*Proof.* To prove the lying over property: let  $p \in \text{Spec}(R)$  be given. Consider  $R_p \subset S_p$ . Then,  $S_p$  over  $R_p$  is integral. In particular,  $R_p$  is local and  $p$  is maximal. Using Proposition 10.6, taking any maximal ideal in  $S_q$  finishes.

To prove going-up, it suffices to show  $n = 2$  and  $m = 1$ : suppose we have  $p_1 \subset p_2$  with  $q_1$  such that  $q_1 \cap R = p_1$ . Then, consider  $R' := R/p_1$  and  $S' := S/q_1$ . By lying over, there is a prime in  $S'$  lying over  $\overline{p_2}$ . Lift back to  $S$  finishes.  $\square$

**Corollary 10.3.1.** Given a integral extension  $i : R \rightarrow S$ , the induced map  $i^* : \text{Spec}(S) \rightarrow \text{Spec}(R)$  is surjective.

## 11 Noether Normalization Theorem

Let  $k$  be a field;  $R|k$  be a algebra of finite type. We first prove two lemma regarding change of variables. The first one applies when normalizing  $k$ -algebras when  $k$  is infinite.

**Lemma 11.1.** Suppose  $k$  is an infinite field. Given  $q \in k[x_1, \dots, x_n]$ , there is a choice of  $a_1, \dots, a_n \in k$  such that the change of variables  $x_i \mapsto x_i + a_i x_n$  for  $i < n$  and  $x_n \mapsto a_n x_n$  take  $q$  to the form

$$q = cx_n^d + (\text{terms in which } x_n \text{ has exponent less than } d)$$

*Proof.* It suffices to consider the homogeneous part of highest total degree  $d$ , denoted by  $q_d$ , since the linear change of variables does not change the total degree. The coefficients of  $x_n^d$  is precisely  $q_d(a_1, \dots, a_n)$ . Thus, the lemma reduces to whether a homogeneous polynomial  $q_d$  does not vanish everywhere on  $k^n$ . When  $k$  is infinite, this is standard to prove by induction on number of variables, and the fact that a polynomial over  $R[x]$  has only finitely many roots.



Note that since  $k$  is a field and the polynomial is homogeneous, we can divide out an appropriate constant so that  $c = q_d(a_1, \dots, a_n) = 1$ .  $\square$

**Example 11.1.** This argument fails when  $k$  is finite. For example, the polynomial  $x^3 + 2x = x(x-1)(x-2)$  vanishes everywhere on  $F_3$ .

Now we prove a more generalized change of variables that applies without the assumption of the infinitude of  $k$ .

**Lemma 11.2.** Suppose  $D$  is a integral domain. Given  $q \in D[x_1, \dots, x_n]$ , there is a choice of  $m_1, \dots, m_n \in k$  such that the change of variables  $x_i \mapsto x_i + x_n^{m_i}$  for  $i < n$  and  $x_n \mapsto x_n^{m_n}$  take  $q$  to the form

$$q = cx_n^m + (\text{terms in which } x_n \text{ has exponent less than } d)$$

*Proof.* Let  $N$  be a natural number larger than the highest exponent of  $x_i$  anywhere in  $q$ , and take  $m_i = N^i$ . Then, let  $cX$  be a term in  $q$ , where the exponents of  $X$  is given by the multindices  $\alpha := (\alpha_0, \dots, \alpha_n)$ . Then, the term having the highest exponent of  $x_n$  is the monomial  $x_n^{T_\alpha}$ , where  $T_\alpha = \sum_{i=0}^n \alpha_i N^i$ . Note that given a different set of multindices  $\alpha'$ , we have  $T_\alpha \neq T_{\alpha'}$  by uniqueness of  $N$ -ary representation. Therefore, we obtain a monomial  $cx_n^m$ , with  $m$  being the unique largest exponent after the change of variables.

Again, if  $D$  is a field, we may take  $c = 1$  by dividing out an appropriate constant.  $\square$

**Theorem 11.3.** (Noether Normalization Theorem) Let  $R = k[x_1, \dots, x_n]$  be a  $k$ -algebra of finite type. Then, there exists  $t_1, \dots, t_d \in R$ ,  $d \leq n$  such that  $\{t_i\}$  algebraically independent over  $R$  and  $R$  is integral over  $R_0 := k[t_1, \dots, t_d]$ , a polynomial ring over  $d$  variables.

*Proof.* We induct on  $n$ . If  $n = 1$ , and  $x_1$  is algebraic over  $k$ , then  $k[x]$  is a vector space and thus we take  $R_0 = k$  as well; if  $x_1$  is not algebraic over  $k$ , then take  $t$  be a transcendental variable and  $k[x] = k[t]$ . Now suppose the theorem holds for  $n = m$ . For  $n = m + 1$ , if all elements  $x_1, \dots, x_m$  again are algebraically independent, we may just take  $t_i = x_i$ . Otherwise, there exists a non-zero polynomial  $p$  such that  $p(x_1, \dots, x_n) = 0$ . Using Lemma 11.2, we may let  $x'_i = x_i - x_n^{m_i}$  for  $i < n$ , and  $x_n$  is integral over  $R_0 := k[x'_1, \dots, x'_{n-1}]$ . Then,  $x_n^{m_i}$  are integral over  $R_0$ , and the sum of integral elements  $x_i + x_n^{m_i} = x'_i$  are integral as well. Therefore,  $R|R_0$  is integral. By transitivity of integrality and the inductive hypothesis, we are done.  $\square$

**Definition 11.1.** The new set of variables  $t_1, \dots, t_n$  is called a **Noether Basis** of  $R$  over  $k$ .

*Proof.* We proceed by induction: if  $n = 1$ , then the ring is a field or a PID and every non-zero prime ideal is maximal. Thus, every chain is of length 0 or 1, respectively.  $\square$

**Definition 11.2.** Let  $R$  be a commutative ring, and  $f \in R$ . Then,  $V(f) := \{\mathfrak{m} \in \text{Max}(R), f \in \mathfrak{m}\}$ . This is called the **zero set** of  $f$  in  $R$ . More generally, given  $I \in \text{Id}(R)$ , we denote  $V(I) := \{\mathfrak{m} \in \text{Max}(R), I \subset \mathfrak{m}\}$

**Example 11.2.** Let  $R = k[x_1, \dots, x_n]$ . Then, every maximal ideal of  $R$  is of the form  $(x_1 - a_1, \dots, x_n - a_n)$  for  $a_i \in k$ .

**Theorem 11.4.** (Hilbert Nullstellensatz) Let  $R = k[x_1, \dots, x_n]$  be a  $k$ -algebra of finite type.

1. If  $R$  is a field, then  $R$  is a finite extension of  $k$ . In particular,  $p \in \text{Spec}(R)$  is maximal iff  $R/p$  is algebraic over  $k$ .
2. Given  $\mathfrak{a} \in \text{Id}(R)$ , then  $N(\mathfrak{a}) = J(\mathfrak{a})$ .
3. Let  $g, f_1, \dots, f_m \in R$  be given. Then, the zeros of  $f_1, \dots, f_m$  are contained in the zeroes of  $g$  iff there exists  $N > 0$ ,  $\lambda_i \in R$  such that  $g^N = f_1 \lambda_1 + \dots + f_m \lambda_m$ .

*Proof.* To 1: By contradiction, suppose  $R|k$  is not algebraic. Then, by Noether Normalization, there exists  $T = (t_1, \dots, t_d)$  such that  $R|R_0 := k[t_1, \dots, t_d]$  a finite extension. which leads to a contradiction.

To 2, Let  $f \in J(\mathfrak{a})$ , and suppose by contradiction that  $f \notin N(\mathfrak{a})$ . Then,  $\Sigma = \{1, f^1, f^2, \dots\}$  is a multiplicative system, and  $R_\Sigma = R[\frac{1}{f}]$  is an  $R$ -algebra of finite type. let  $\mathfrak{m}_\Sigma$  be a maximal ideal. Let  $\mathfrak{m} = (\mathfrak{m}_\Sigma)^c$  is maximal in  $R$ . Then,  $f \notin \mathfrak{m}$ .

To 2: set  $\mathfrak{a} = (f_1, \dots, f_m)$ . Then,  $V(\mathfrak{a}) \subset V(g)$ . Show  $g \in N(\mathfrak{a})$ . □

Geometric interpretation of Hilbert Nullstellensatz: let  $K|k$  an algebraically closed field extension.

**Definition 11.3.** An algebraic set over  $k$  with values in  $K = \bar{k}$  is any set defined as follows: for  $n \geq 1$ ,  $f_1, \dots, f_n \in k[x_1, \dots, x_n]$  such that  $\Sigma = \{a = (a_1, \dots, a_n) \in K^n : f_i(a) = 0\}$  V=Verschwinden, to vanish.  $I(\Sigma) = \{g \in R : g(\Sigma) = 0\}$ .

## 12 Integral Extensions over Integral Domains

**Proposition 12.1.** Let  $S|R$  be an integral extension where  $R$  is integral domain. Let  $K$  be the quotient field of  $R$ ,  $L$  be the quotient field of  $S$ . Then the following hold:

1.  $L|K$  is an algebraic field extension and there exists a basis in  $S$ .
2. If  $x \in L$  algebraic over  $R$  iff  $Mipo_K(x) \in R[t]$
3. If  $L|K$  is finite with basis  $\beta_1, \dots, \beta_n$ . Then the integral closure of  $S$  in  $L$  is contained in  $\sum_{i=1}^k R\beta_i^*$ .

*Proof.* To 1:  $L|K$  algebraic is exercise. Let  $\beta'_i$  be a  $K$  basis of  $L|K$ . Rewrite things as a basis in  $S$ . To 2: Let  $x \in S$  be integral over  $R$ . Hence, we have  $f(t) = x^n + \dots + a_0 = 0$  with  $a_i \in R$ . WLOG, we have  $a_0 \neq 0$ . Let  $\tilde{S} = \{\tilde{x} \in \bar{L} : \tilde{x} \text{ st } f(t) \in R[t]\}$ . Hence, all  $\tilde{x}$  are algebraic independent over  $R$ ; and  $f(t)$  splits over  $\tilde{S}$ . Hence,  $Mipo(x)|f(t)$ . Then,  $f(t) = \prod(t - \tilde{x}_i) = t^n + (\sum_{i=1}^k x_i)t^{n-1} + \dots \prod \tilde{x}_i$ . Show that all coefficients are in  $\tilde{S} \cap K = R$ . □

**Theorem 12.1.** (Going Down) Let  $S|R$  be a integral ring extension of domains, with  $R$  integrally closed, then it satisfies the going down property.

*Proof.* By induction, reduce to the case where  $R$  is local. □

**Corollary 12.1.1.** Let  $R := k[x_1, \dots, x_n]$  be a finitely generated  $k$ -algebra.

Then,  $R$  is strongly catenary, i.e every maximal sequence of prime ideals has length  $n = d$ .

## 13 Introduction to Hilbert Decomposition Theory

Let  $R$  be an integrally closed domain.  $K$  the quotient field.  $L|K$  the algebraic separable extension.  $S$  the integral closure of  $R$  in  $L$ . The question is describe the behaviour of  $\text{Spec}(R)$  under the integral ring extension  $S|R$ . Especially when  $L|K$  is Galois. In some sense, this extends the usual Galois theory for field extension to ring extensions.

**Proposition 13.1.** Let  $G$  be a profinite group, acting continuously on a discrete ring  $S$ . Then, the orbit for every  $x \in S$  is finite under  $G$ .

**Proposition 13.2.** Let  $G_i = g/N_i$ . Then,  $S_i = S^{G_i} := \{x \in S : G_i x = x\}$ .

1. Then,  $\cup S_i = S$
2. Let  $R = S^G$ . Then,  $S_i|R$  is integral. Moreover,  $G_i \subset \text{Aut}_R(S_i)$ , with  $S_i^{G_i} = R$ .

**Proposition 13.3.** Let  $R = S^G$ . Then,  $S_i|R$  and  $S|R$  are integral ring extensions. Hence,  $S_j|S_i$  for  $N_j \subset N_i$  is integral extension.

**Proposition 13.4.** Let  $p \in \text{Spec}(R)$ , and denote  $X_p^i = \{q \in \text{Spec}(S_i) : q_i \cap R = p\}$  and  $X_p = \{q \in \text{Spec}(S) : q \cap R = p\}$ . Then,  $G$  acts Transitively on  $X_p$ , and  $G_i$  acts transitively on  $X_p^i$ .

Fact: Let  $L|K$  be Galois; let  $G$  be the galois group. Then,  $\sigma \in G$  implies  $\sigma(S) = S$ .

The ring extensions  $S_j|R$  satisfies  $\text{Spec} S_i \rightarrow \text{Spec}(R)$  given by  $q_i \mapsto q_i \cap R$  is surjective. Then,  $\text{Spec}(R) = G_i \text{Spec}(S_i)$  is the  $G_i$  orbits of  $\text{Spec}(S_i)$ . Finally,  $\text{Spec}(S)$  is the projective limit of  $\text{Spec}(S_i)$  as  $G$ -spaces.

**Definition 13.1.** Given  $q \in \text{Spec}(X_p)$ , the **q-decomposition group**  $D_{q|p} = \text{st}_G(q) = \{\sigma \in G : \sigma q = q\}$ .

**Proposition 13.5.** Let  $\Sigma \subset R$  be a multiplicative system. Then,  $G$  acts on  $S_\Sigma$   $\sigma(\frac{q}{r}) = \frac{\sigma(q)}{r}$ . And,  $S_\Sigma^G = R_\Sigma$  Moreover,  $p \cap \Sigma = \emptyset$ . Then,  $X_{p_\Sigma} = \{q_\Sigma : q \in X_p\}$ . And  $D_{q_\Sigma|p_\Sigma} = D_{q|p}$ .

**Proposition 13.6.** Let  $H \subset G$  be an open subgroup. Define  $q^H = q \cap S^H$ .

1.  $q^H \cap R = p$  and  $D_{q|q^H} = D_{q|p} \cap H$ .
2. If  $H$  is normal, let  $\bar{G} : G/H$ . Then,  $\bar{G}$  acts on  $S^H$  by  $\bar{\sigma}(h) = \sigma(h)$ . Then,  $(S^H)^{\bar{G}} = R$ , and  $D_{q^H|p} = \overline{D_{q|p}} := D_{q|p}/H$ .

**Corollary 13.0.1.** Let  $G, S|R$  be as usual. Then,

1. The going-down for  $S|R$  holds. Given  $p_1 \subset \dots \subset p_n$  a chain in  $\text{Spec}(R)$ , and  $q_m \subset \dots \subset q_n$  with  $m \leq n$ , then there exists  $q_1 \subset \dots \subset q_m$  in  $\text{Spec}(S)$  that prolongs the sequence.

*Proof.* By induction, it suffice to consider  $n = 2$  and  $m = 1$ . Hence  $p_1 \subset p_2$  and  $q_2 \cap R = p_2$ . Recall there exists  $q'_1 \in \text{Spec}(S)$  such that  $q'_1 \cap R = p_1$ . By going-up, there exists  $q'_2 \in \text{Spec}(S)$  such that  $q'_2 \cap R = p_2$ . Since  $G$  acts transitively on  $X_{p_1}$  and  $X_{p_2}$  such that  $\exists \sigma \in G$  such that  $\sigma' q_2 = q'_2$ . Take  $\sigma^{-1}$  finishes.  $\square$

**Theorem 13.1.** The restriction map  $\text{Spec}(S) \rightarrow \text{Spec}(R)$  by  $q \mapsto q \cap R$  defines a bijection between the maximal chain of prime ideals in the two rings.

Let  $H \subset G$  be a closed subgroup.  $S^H$  be the fixed ring.  $\text{Spec}(S^H) \rightarrow \text{Spec}(R)$  be the restriction map. Then, the previous theorem also holds.

**Example 13.1.** Main example of the theory is: Let  $R$  be an integrally closed domain.  $K$  be the quotient field of  $R$  and  $L|K$  galois extensions. Take  $S$  be the integral closure of  $R$  in  $L$ . Recall  $G$  acts on  $S$  via  $L$  (check  $\sigma s \in S$ ). Then,  $S|R$  is quasi-galois extension with  $G = \text{Aut}_R(S)$ . Hence, the Hilbert Decomposition Theory works for  $S|R$ , the going down.

**Example 13.2.** Let  $R = \mathbb{Z}$ ,  $K = \mathbb{Q}$  and  $L = \mathbb{Q}[\sqrt{d}]$ . Then,  $S = \sqrt{\phantom{x}}$  iff  $d \not\equiv 1 \pmod{4}$ . Otherwise  $S = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ . Then  $G = \mathbb{Z}/2$ . Let  $\mathfrak{P} \in X_p \in \text{Spec}(S)$ . Then the decomposition group is either 1 or the entire  $G$ . Look at  $x^2 - d \pmod{p}$ . If reducible, then  $p$  cannot be prime.

**Example 13.3.**  $R = k[t]$  and  $K = k(t)$ ,  $L = k(\sqrt{f})$ .

## 14 Dedekind domains

**Definition 14.1.** A domain  $R$  is called a **Dedekind** domain if every proper ideal can be written as a product of prime ideals.

**Example 14.1.** All PIDs are Dedekind Domains. The integral closure of a dedekind doamin under the galois extension is still a Dedekind domain.

**Definition 14.2.** Let  $R$  be a commutative ring and  $K$  be its total ring of fractions. If  $R$  is a domain, then  $K$  is a field. A fractional ideal of  $R$  is any  $R$ -submodule  $M \subset K$  such that there exists non-zero divisor  $r$  such that  $rM \subset R$ .

**Definition 14.3.** Given  $M \subset K$  a fractional ideal, it is called **invertible** if there exists  $N \subset K$  fractional ideal such that  $MN = R$ .

**Proposition 14.1.** Let  $I'_R$  be the set of fractional ideals of  $R$ . Then, the set is closed under addition and multiplication.

**Proposition 14.2.** Every invertibe ideal  $M$  is finitely generated.

**Definition 14.4.**  $I_R \subset S'_R$  is the set of invertible fractional ideals.

**Proposition 14.3.** The following hold:

1.  $I_R$  is the group of invertible elements in  $I'_R$ .
2.  $M \subset I_R$  implies  $M$  finitely generated as  $R$ -module, and there exists  $s \in \Sigma_R^0 \cap M$ , meaning there must be non-zero divisors of  $M$ .
3. Let  $N' := (R : M)$ , then  $N'M \subset R$  and  $N'M = R$  iff  $M \in I_R$

*Proof.* Exercise. To 2: let  $N \in I_R$  such that  $NM = R$ ; then there exists  $n_i \in N$ ,  $m_i \in M$  such that  $\sum_{i=1}^k n_i m_i = 1 \in R$ .  $\square$

**Proposition 14.4.** Being invertible is a local property.

*Proof.* Exercise. The hint is  $N_p := (R_p : M_p)$  for all prime  $p$ .  $\square$

**Theorem 14.1.** (Characterization of Dedekind Domains) The following are equivalent:

1.  $R$  is a Dedekind domain,
2.  $I'_R = I_R$ . In other words, all non-zero fractional ideals are invertible.
3. All non-zero prime ideals of  $R$  are invertible.
4. For all  $m \in \text{Max}(R)$ , we have  $R$  Noetherian, and  $R_m$  is a DVR.
5.  $R$  is Noetherian, integrally closed, and Krull dimension is 1.

*Proof.* Let  $M \in I'_R$ ,  $M \neq 0$ , and  $r \in R$  such that  $rM \in \text{Id}(R)$ . Then,  $M \in I_R$  iff  $rM \subset R$  is invertible.

For  $a \in \text{Id}(R)$ , choose  $r \neq 0$ ,  $r \in a$ . Then,  $a \subset (r)$  both have a prime decomposition, with exponents comparable.

For  $iii \implies iv$ , if  $M \in I_R$ , then  $M$  is finitely generated. Hence, all  $p \in \text{Spec}(R)$  are finitely generated and we get Noetherian. The claim now is  $\dim(R_m) = 1$ . Let  $p \in \text{Spec}(R_m)$ , and  $p \neq m$ . Look at  $a = pm^{-1}$ . Then,  $p = ma$ . Thus, we have  $a \subset p$ . On the other hand  $p \subset qm^{-1}$ , we have  $p = a$ . By Nakayama, we have  $p = pm$  in a noetherian local ring and  $p$  must be 0. Check that the maximal ideal is principal, so that the ring is a DVR.

For  $iv \equiv v$ : see lemma below.

For  $iv \implies i$ : let  $a \in \text{Id}(R)$  be a proper ideal. For every  $m \in \text{Max}(R)$ , there exists  $N_m > 0$  such that  $a_m = m_m^{N_m}$ . Since the ring is noetherian and of Krull dimension 1, the set  $\{N_m : N_m > 0\} = \text{Spec}_{\min}(a)$  is finite.  $\square$

**Lemma 14.2.** Let  $R$  be a local domain. Then the following are equivalent:

1.  $R$  is integrally closed and of Krull dimension 1.
2.  $R$  is Noetherian and the maximal ideal is principal
3.  $R$  is a PID
4.  $R$  is DVR.

*Proof.* For  $r \neq 0$ , there exists minimal  $N$  such that  $m^N \subset (r)$ . Conclude that there exists  $a \in m^{N-1}$  such that  $\frac{a}{r}$  is not in  $R$ . But,  $\frac{r}{a}m \subseteq R$ . But  $m$  is finitely generated, we get  $\frac{r}{a}$  is integral over  $R$ .  $\square$

**Theorem 14.3.** (Permanence Properties) Let  $R$  be a Dedekind domain. Then, the following hold:

1. If  $\Sigma \in R$  is a multiplicative system, and  $R_\Sigma$  not a field. Then,  $R_\Sigma$  is a dedekind domain.
2. Let  $K = \text{Quot}(R)$ , and  $L|K$  a separable extension,  $S$  be the inetrgal closure of  $R$  in  $L$ . Then,  $S$  is Dedekind domain.

*Proof.* To 1: Exercise. To 2: suppose  $L|K$  is separable, then  $S$  is a finite  $R$  module hence noetherian and has the same krull dimension 1. Therefore, the  $S$  is Dedekind. Suppose  $L|K$  is purely inseperable, then it following from a theorem by Krull-Akizuki.  $\square$

**Proposition 14.5.** Some remarks: Let  $R$  be Dedekind domain.

1. If  $\text{Spec}(R)$  is finite. Then,  $R$  is a PID.
2. If  $a \in \text{Id}(R)$  there exists  $x, y \in a$  such that  $a = (x, y)$ .

*Proof.* Exercise.  $\square$

**Definition 14.5.** The set of invertible ideals of  $R$  is called the Cartier divisors of  $R$ . If  $R$  is Dedekind, then the group is called the divisor group of  $R$ . The group  $H_R$  is the subgroup of divisor group of  $R$  that are principlally generated.

**Definition 14.6.** The Ideal class group is the quotient  $\text{Div}(R)/H_R$ .

**Example 14.2.**  $cl(\mathbb{Z}) = 1$ ;  $cl(k[t]) = 1$ ; If  $K|\mathbb{Q}$  a quadratic number field,  $O_K$  be the ring of integers. Then,  $cl(O_k)$  not always 1.