

MATH 603 Notes

David Zhu

March 29, 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 (σ_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, π 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 π_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 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 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 π 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 π does not divide a_{i_0}, b_{j_0} . Then, π 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_Σ 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 Σ . 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 a 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.

Proof. Note that $1 \implies 2$ since every finitely generated algebra is a quotient of polynomial rings over finitely many variable. To prove 1, by induction it suffices to show for $i = 1$. Let $\mathfrak{a} \in R[t]$ be an ideal. Claim: \mathfrak{a} is f.g. Inductively, we may choose elements $f_i \in I$ with $deg(f_{i+1})$ 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 ≥ 0 and thus in R_v . The order on Γ_{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 τ_{vw} .

Definition 6.4. A valuation ring R is called **discrete**, if $v_R(K) \cong \mathbb{Z}$ as ordered abelian groups. An element π 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 ϵ 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 Γ 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 Σ 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 $\mathfrak{m}_1 \subset \mathfrak{m}_1\mathfrak{m}_2 \subset \dots \subset \mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3 \dots$ 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.

$J(R) = N(R)$ is nilpotent.

Proof. In Artinian rings, all prime ideals are maximal, and we get the equality $J(R) = N(R)$. 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 $x \neq 0$. \square

Theorem 7.2. (Structure Theorem) Let $\text{Max}(R) = \{m_1, \dots, m_r\}$. Then, $R \cong R/(m_1)^n \times \dots \times R/m_r^n$. 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 $R \cong R/(m_1)^n \times \dots \times R/m_r^n$. \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 R local as follows: R Artin ring implies $R = \prod R_i$, where R_i are local Artin rings. In particular, the product is Noetherian iff each R_i is Noetherian. R is Noetherian and Krull dimension 0 implies $\text{Max}(R) = \text{Spec}(R)$, hence $\text{rad}(R) = \text{Jac}(R)$. Thus, R has only finitely many prime ideals. Hence, $\text{Max}(R)$ is finite and we reduce to the finite case.

Step two: now assume R is local. Assume (R, \mathfrak{m}) is a local Artin ring. To prove R is Noetherian, it suffices to show \mathfrak{m} is finitely generated. For $k > 0$, we have the exact spectral sequences

$$0 \longrightarrow \mathfrak{m}^k / \mathfrak{m}^{k+1} \xrightarrow{f} R / \mathfrak{m}^{k+1} \xrightarrow{g} R / \mathfrak{m}^k \longrightarrow 0$$

Note $\kappa := R/\mathfrak{m}$ is a field, R acts on $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ through the projection $R \rightarrow \kappa$. In particular, there is a bijection

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

Note R Artinian implies R/\mathfrak{m}^{k+1} is Artinian. Thus, the set ϵ is finite, and $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ is finite dimensional. Then induction on k : suppose R/\mathfrak{m}^k is Noetherian. Then, $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ is finite R -module.

For the reverse implication: Given (R, \mathfrak{m}) Noetherian and $\mathfrak{m}^k = 0$ for k sufficiently large. If $k = 0$ then the statement holds; suppose it holds for k ; consider the exact sequence above and R/\mathfrak{m}^k is Artin. Let (\mathfrak{a}_i) be a descending sequence of $\text{Id}(R/\mathfrak{m}^{k+1})$. Hence, there exists i_0 such that $\pi_k(\mathfrak{a}_i)\pi_k(\mathfrak{a}_{i_0})$ for all $i > i_0$. Then, look at

$$0 \longrightarrow \mathfrak{a}_i \cap \mathfrak{m}^k/\mathfrak{m}^{k+1} \xrightarrow{f} \mathfrak{a}_i/\mathfrak{m}^{k+1} \xrightarrow{g} \mathfrak{a}_i/\mathfrak{m}^k \longrightarrow 0$$

□

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, $(R/\mathfrak{a}^n, p_n)$ is a projective system. The limit $\widehat{R} := \varprojlim R/\mathfrak{a}^n$, together with $i : R \rightarrow \widehat{R}$ is called \mathfrak{a} -adic completion of R .

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

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, $\cap \mathfrak{a}^n = 0$. In particular, the inclusion map in the \mathfrak{a} -adic completion is injection.

Proof. Suppose R is local with maximal ideal \mathfrak{m} . Let $\mathfrak{a}_0 = \cap \mathfrak{a}^k$ is a finitely generated ideal. Let $\mathfrak{m}_0 = \cap \mathfrak{m}^k$ is f.g with $\mathfrak{a}_0 \subset \mathfrak{m}_0$. 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 \mathfrak{m} be a maximal ideal over \mathfrak{a} , and let $\phi : R \rightarrow R_{\mathfrak{m}}$ be the localization is injective. □

Much more is true.

Theorem 8.2. (Artin-Reese Lemma) Let R be a Noetherian ring. Given ideals $\mathfrak{a}, \mathfrak{b}, I$, there exists k such that for $k' > k$, we have $\mathfrak{a}^{k'}\mathfrak{b} \cap I = (\mathfrak{a}^{k'-k})$.

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

Definition 8.2. Let R be a ring. For $r \in R$, let $\text{Spec}_{\min}(r) = \{p \in \text{Spec}(R) : (r) \subset p \text{ minimal}\}$. Definition goes similarly for a set of elements.

Definition 8.3. For $p \in \text{Spec}(R)$, the height of p is the krull dimension of R_p . The coheight is the krull dimension is the krull dimension of R/p .

Proposition 8.2. $\text{height}(p) + \text{coheight}(p) \leq \text{Krull dimension of } p$.

Theorem 8.4. (Krull's Principal Ideal Theorem/ Hauptideasatz) Let R be a Noetherian ring. Then, for all non-units $r \in R$, one has $\text{height}(p) \leq 1$ for all $p \in \text{Spec}_{\min}(r)$, with equality when r is not a zero-divisor.

Proof. Suppose by contradiction that $\text{height}(p) > 1$. Equivalently, there exists a chain $q_0 \subset q$ prime ideals. Reduction step: can replace R by R/p_0 , and q/q_0 and p/q_0 . Can replace R, q, p by R_p, p_p, q_p . So WLOG, R is local, and p is maximal. Hence, $(r) \subset p$, and $\text{rad}(r) = p$. Conclude $\bar{R} := R/(r)$ is Artin. Hence, $q^{(n)}$ gives $(\bar{q}^{(n)})_n$ a descending sequence, so it must stabilize. \square

Lemma 8.5. For $q \in \text{Spec}(R)$, let $q^{(n)} := (q^n R_q)^c$. Then, $(q^{(n)})^e = q^n R_q = (q R_q)^n$. $q^{(n)}$ is called the symbolic n -th power of q .

Proof. exercise \square

Lemma 8.6. $q^{(n)}$ is primary if $ax \in q^{(n)}$, and $x \notin q$, then $a \in q^{(n)}$.

Proof. exercise \square

Definition 8.4. Let $r = (r_1, \dots, r_n)$ be given. It is called a regular sequence if r_i is not a zerodivisor in $R/(r_1, \dots, r_{i-1})$.

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. Induction: $n = 1$ is PIT; Given $r = (r_1, \dots, r_{m+1})$, and $p \in \text{Spec}_{\min}(r)$. Let $q \subset p$ be a maximal with this property. Claim: $\text{ht}(q) = m$. Hence $\text{ht}(p) = m + 1$. By contradiction, let $\text{ht}(q) > m$ and consider $q_0 \subset q_1 \subset \dots \subset q_m = q$. Reduction step 1: replace R, p, q by $\bar{R} := R/q_0, \bar{p} := p/q_0, \bar{q} := q/q_0$. WLOG, $R = \bar{R}$ is a Noetherian domain. Reduction step 2 Replace R, p, q with their localization at p . Then, R is local with $\text{max}(R) = p$.

Since q is properly contained in p , there exists $r_i \notin q$ by minimality. WLOG, $r = m + 1$. Consider $\mathfrak{a} = q + (r_{m+1})$, which implies $q \subset \mathfrak{a} \subseteq p$. Then, $\text{nil}(\mathfrak{a}) = p$ since p is the only prime ideal containing \mathfrak{a} . Conclude that $r_i \in p$ implies $r_i \in \text{nil}(\mathfrak{a})$, hence for every $i = 1, \dots, m$, there exists $a_i \in R$ and $s_i \in q$ such that $r_i^{n_i} = s_i + a_i r_{m+1}$. Conclude that $s = (s_1, \dots, s_m)$ and $\text{nil}(s) = q$. In particular, q is a minimal prime ideal containing elements s_1, \dots, s_m . Look at $R \rightarrow R/s$, and $\bar{p} = p/s$. Hence, $\text{ht}(\bar{p})$ is at most 1, and 1 \bar{r}_{m+1} is not a zero divisor. \square

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. exercise □

9 Modules over special classes of rings

9.1 Modules over PIDs

Lemma 9.1. Let $C = (\gamma_1, \dots, \gamma_n)$ be an R -basis of a free R -module P , and $\gamma'_1 = \sum_{i=1}^m r_i \gamma_i$ such that $\gcd(r_1, \dots, r_m) = 1$. Then there exists a basis $C' = (\gamma'_1, \dots, \gamma'_m)$

Proof. Induction: $n = 1$ trivial; let $x = \sum_{i=1}^{m+1} r_i \gamma_i = \sum_{i=1}^m r_i \gamma_i + r_{m+1} \gamma_{m+1}$. We can write $\sum_{i=1}^m r_i \gamma_i$ with respect to the new basis by induction step. since the gcd of the sequence is $\gcd(d, r_{m+1})$, which must be 1. □

Theorem 9.2. Let R be a PID. Then, the following hold:

1. If M is a free R module, every R -submodule of M is R -free.
2. A finite torsion free R -module is R -free

Proof. To 1: let $A = (\alpha_i)$ be a basis for M . Suppose I is well-ordered (otherwise use Zorn's lemma), we make transfinite induction: let i_0 be the minimal element of I , $M_{i_0} = \langle \alpha_{i_0} \rangle$ be the cyclic submodule. Let $M_{i'} = \langle \alpha_{i'} : i \leq i' \rangle$ and $N_{i'} = N \cap M_{i'}$. Note that $N_{i_0} = N \cap R_{\alpha_{i_0}}$, and the submodules of a PID is precisely the principal ideals, which are free.

To 2: let (x_1, \dots, x_m) be a system of generators and let $R^m \rightarrow M$ be the natural surjection. If the system is linearly independent, we are done. Let $\sum_{i=1}^k r_i x_i = 0$. Divide out the gcd, and if there is no torsion, we can apply the lemma. □

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 .

Proof. Let $D = \{d \in R : \exists y \in N, \text{basis}(\beta_1, \dots, \beta_m) \text{ of } M \text{ s.t. } d\beta_1 = y\} = \{d \in R : \exists y = \sum_{i=1}^k r'_i \alpha'_i \in N, \gcd(r_i) = 1\}$. □

Lemma 9.4. $d_1 = \inf D$ exists, where the ordering is by divisibility.

Proof. Obviously, D has minimal elements. Let d', d'' be minimal elements, and $d = \gcd(d', d'')$, and show $d \in D$. □