MATH 603 Notes

David Zhu

March 25, 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 usally 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 prinipal 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. ☐

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 $x_1 \in\in I$. 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 $\{\alpha_i := a_i + f_i x : a_i \in I, f_i \in R, i = 1, ..., k\}$ that generate $I + (x)$, and a finite set $\{b_j : j = 1, ..., l\}$ 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 i 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 $\phi : R \to \mathbb{N}$ 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. Eucldiean 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 $n \leq i$. Coversely, it is clear that any divisor of a, b divdes 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 $p \in Spec(R)$ is principal.

Proof. One direction is trivial; for the other direction, assume that every prime is principal. Then, Cohen's Lemma implies $Id^\infty(R) \neq \emptyset$; 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 $p \in Spec(R)$ 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 stablize(stablizing is equivalent to $(a_n) = (a_{n+1})$ for some n, which implies they differ by a unit). □

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.

□

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 $f(t) = a_0 + ... + a_n t^n$ be given. Then, the **<u>content</u>** 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). $C(f) : R[t] \to R$ 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 $f(t) = a_0 + ... + a_n t^n$ and $g(t) = b_0 + ... + b_m t^m$. 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 divede $C_{i_0+j_0}$.

□

Note that proof goes similarly for quotient fields.

Theorem 4.3. Let R be a UFD. For $f(t) \in R[t]$, the following are equivalent:
1. $f(t)$ is prime
2. $f(t)$ is irreducible
3. If f in the polynomial ring over the quotient field is irreducible or $C(f) = 1$ and f is irreducible.

Proof. $1 implies 3$ trivial. By contradiction, let $f = gh$ in $K[t]$ gh irreducible. Then, $C(f) = C(g)C(h)$. Let $f = x_f f_0$ and $g = x_g g_0$ such that $1 = C(f_0)C(g_0)$. Let $x_f x_g = \frac{a}{b}$ in simplest terms such that $gcd(a, b) = 1$ (we can do this in UFD). We then get $bf = ag_0h_0$. We get that f irreducible over $R[t]$. □

Proposition 4.1. $R[t_i]_{i \in I}$ is UFD if R is UFD.

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. $Spec(R) \subseteq Id^f(R)$.

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

Remark: if R is not commutative, then there exists left/right Noetherian, and it is possible that a ring 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 nilradical of an ideals $\mathfrak{a}$, $nil(\mathfrak{a})$, has a power contained in $\mathfrak{a}$.
4. Let $Spec_{min}(\mathfrak{a}) := \{p \in Spec(R) : \mathfrak{a} \subset p, \; p \text{minimal}\}$ is finite.

Proof. To 1. $Spec(R_\Sigma)$ corresponds bijectively to primes in $Spec(R)$ with empty intersection with Σ. We also have p finite generated implies p^e f.g.

To 2. $nil(\mathfrak{a}) = (r_1, ., , , r_n)$ f.g. For every i, we have $r_i^{n_i} \in \mathfrak{a}$ for some n_i. Take $n = \sum_{n_i}$ and $nil(\mathfrak{a})^n \subset \mathfrak{a}$.

To 3. The first method to prove this is by contradiction: let $A = \{\mathfrak{a} : Spec_{min}(\mathfrak{a}) \text{infinite}\}$. Then A has maximal elements. Let $\mathfrak{a}_o$ be maximal. Note that $\mathfrak{a}_o$ cannot be prime for it is over itself. Suppose it is not prime, then there exists $xy \in \mathfrak{a}$ WLOG $x \notin \mathfrak{a}$. Then, $\mathfrak{a} + (x)$ contradicts maximality.

The second method is using the fact that $Spec(R)$ 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 contradction, 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 $\mathfrak{a}_\mathfrak{o}$. Then, $\mathfrak{a}_\mathfrak{o}$ is not irreducible, for it would be the intersection of itself. Therefore, there exists I_0, I_1 such that $a_0 = I_0 \cap I_1$, where a_0 is properly contained in both. By maximality, I_0, I_1 are both finite intersection of irreducibles, and we can decompose a_0 based on such, a contradction. $\square$

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 ther 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): $R[t_1, ..., t_n]$ 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. For every $n \geq 0$, let $\{\mathfrak{a}_n\}$ be the set of leading coefficients of polynomials of degree n in $\mathfrak{a}$. We note that $(\mathfrak{a}_\mathfrak{n})$ is a chain of ideals in R. Thus, there exists an index m at which the chain stablizes. For $r \leq m$, let $\mathfrak{a}_\mathfrak{r} = (a_{r_1}, ..., a_{r_n})$. Do induction on m. Idea is to deduct something to drop the degree by 1.

$\square$

6 Valuation Rings

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

1. Every ideal in R is comparable, i.e $id(R)$ is a chain
2. For every $x \in \mathrm{Quot}(R)$, if $x \notin R$ then $x^{-1} \in R$.

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

Example 6.1. $\mathbb{Z}_{(p)}$ is a valuation ring.

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 $yR \subset xR$. The group is called the **value group** of R.
3. The natural map $v_R : K \to \Gamma_R \cup \{\infty\}$, $v(0) = \infty$ 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. Exercise. □

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

Let R be a domain, and K be a field, $(\Gamma, +, \leq)$ be a totally orderedd abelian group. Let $v : K \to \Gamma \cup \{\infty\}$ 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 $\tau : \Gamma_{R_v} \to \Gamma$, given by $xR_v^\times \mapsto v(x)$ is an order preserving embedding. Moreover, $v = \tau \circ v_{R_v} : K \to \Gamma \cup \{\infty\}$.

Proof. Exercise. □

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

Definition 6.2. 1. Two valuations v, w on K are equivalent if $R_v = R_w$. If $v : K \to \Gamma_v \cup \{\infty\}$ and $w : K \to \Gamma_w \cup \{\infty\}$, with embeddings $\tau_v : \Gamma_{R_v} \to \Gamma_v$ $\tau_w : \Gamma_{R_w} \to \Gamma_w$. There exists an order preserving commutative diagram

$$\begin{tikzcd} \Gamma_{R_v} \arrow[r] & \tau_v(\Gamma_{R_v}) \arrow[r] \arrow[d, "\tau_{vw}"] & \Gamma_v \\ \Gamma_{R_w} \arrow[r] & \tau_w(\Gamma_{R_w}) \arrow[r] & \Gamma_w \end{tikzcd}$$

2. Two valuations v, w on K are equivalent iff $\mathfrak{m}_v = \mathfrak{m}_w$

A valuation ring R is called **discrete**, if $v_R(K) \cong \mathbb{Z}$ as ordered abelian groups. If $\pi \in R$ has $v_R(\pi)$ minimal since $\mathbb{Z}$ has minimal elements, then π is called a uniformizing parameter.

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

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

Definition 6.3. An absolute value of a field K is any map $|-| : K \to \mathbb{R}^+_{\geq 0}$ iff it satisfies the norm axioms. An absolute value is called **non-Archimedian** or **ultra-metric** if $|x + y| \leq max\{|x|, |y|\}$.

Let $|-| : K \to R$ be a non-Archimedian absolute value. Then $v_{|-|} := -log \circ |-| : K \to \mathbb{R} \cup \{\infty\}$ is rank 1 valuation. Conversely, let $v : K \to R \cup \{\infty\}$ be a rank one valuation, then $|-|_v := e^{-v} : K \to \mathbb{R}_{\geq 0}$ is a non-Archimedian absolute value.

Theorem 6.1. The following facts about possible valuations

1. If $K|F_p$ algebraic, then no non-trivial valuations.
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 $R_v = F[\frac{1}{t}]_{(\frac{1}{t})}$. thus all valuations are discrete.
3. If v is a non-trivial valuation on $\mathbb{Q}$, then $R_v = \mathbb{Z}_{(p)}$ for some p prime. Morever, all non-archimedian absolute values of $\mathbb{Q}$ corresponds to the valuation above. (Ostrowskis Theorem).

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, that makes the space compact totally disconnected. The space is usually very complicated.

Theorem 6.2. (Chevalley's Theorem for Existence of Valuations) Let A be a domain, $p \in Spec(a)$ a prime ideal, $\kappa(p)Quot(A/p) \subset \Omega$, with Ω algebraically closed. Then, there exists a valuation ring R of $K = Quot(A)$ such that $\mathfrak{m}_R \cap A = p$, and $R/\mathfrak{m} \hookrightarrow \Omega$.

Proof. Set up for Zorn's lemma: $H = \{(B, q) : A \subset B, q \in Spec(B), q \cap A = p\}$ such that the embedding into the closure Ω commutes. Prove that H has maximal elements R. If R is not local, then $R_\mathfrak{m}$ is local and bigger than R. Thus, R is local. let $x \in K$, we want to show $x \notin R$ implies $x^{-1} \in R$. Claim, if $m[x] = R[x]$, then $m[x^{-1}] \subset R[x^{-1}]$. If so m then $R_x := R[x^{-1}]$ is greater than R, a contradictin. By contradiction, let $m[x] = R[x]$, $m[x^{-1}] = R[x^{-1}]$. Then, there exists coefficients in m such that polynomials are 1. $\square$

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. $Spec(R) = Max(R)$ is finite.

Proof. To 1. pull back of ideals respects inclusion. To 2. obvious. To 3, let $p \in Spec(R)$. Then, R/p is an integral Artinian ring. Then, R/p must be a field. Thus, all primes are maximal. If $\mathfrak{m}_1, ..., \mathfrak{m}_n$, then $\mathfrak{m}_1 \subset \mathfrak{m}_1\mathfrak{m}_2 \subset ... \subset \mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3....$ □

Theorem 7.1. Let R be an Artinian ring. Then the following hold:

1. J(R)=N(R) is nilpotent.
2. (Structure Theorem) Let $Max(R) = \{m_1, ..., m_r\}$. Then, $R \to R/(m_1)^n \times ... \times R/m_r^n$. Hence, R is a product of local Artinian rings.

Proof. Look at $J(R) \subset J^2(R) \subset ...$ becomes stationary. Thus, there exists n minimal such that $I = J^n(R)$ such that $I^k = I$ for all k. Let H be the set of ideals in R sich that □