Chapter 3

Commutative Rings and Modules

3.1 Chain Conditions

(VIII.1) In this section, R is always a ring with identity (not necessary commutative) unless otherwise specified.

Def. *A module A is said to satisfy the* **ascending chain condition (ACC) on submodules** *or to be* **Noetherian** *if for every ascending chain of submodules of A:*

$$A_1 \subset A_2 \subset A_3 \subset \cdots$$

there is an integer n such that $A_n = A_{n+1} = A_{n+2} = \cdots$.

Def. *A module B is said to satisfy the* **descending chain condition (DCC) on submodules** *or to be* **Artinian** *if for every descending chain of submodules of B:*

$$B_1 \supset B_2 \supset B_3 \supset \cdots$$

there is an integer n such that $B_n = B_{n+1} = B_{n+2} = \cdots$.

Ex. *As $\mathbf{Z}$-modules:*

1. *$\mathbf{Z}$ is Noetherian but not Artinian.*
2. *$\mathbf{Z}_m$ is both Noetherian and Artinian. In general, a finite abelian group is both Noetherian and Artinian.*
3. *$\mathbf{Q}$ is neither Noetherian nor Artinian.*
4. *Given a prime number p, the $\mathbf{Z}$-module*

$$\mathbf{Z}(p^\infty) := \{\overline{a/b} \in \mathbf{Q}/\mathbf{Z} \mid a, b \in \mathbf{Z} \quad \text{and} \quad b = p^i \quad \text{for some} \quad i \geq 0\}$$

is Artinian but not Noetherian.

Ex. *As a $\mathbf{Q}$-module, $\mathbf{Q}$ is both Noetherian and Artinian. In general, a finite dimensional vector space V over a division ring D is both Noetherian and Artinian D-module.*

Def. *A ring R is* **left Noetherian** *if R satisfies ACC as a left R-module. The ring R is* **Noetherian** *if it is both left and right Noetherian.*

Likewise for **left Artinian** and **Artinian** ring.

Ex. *A division ring D is both a Noetherian ring and an Artinian ring.*

Ex. *Every commutative principal ideal ring is Noetherian (e.g. PIDs).*

Def. *A module A is said to satisfy the* **maximum [resp. minimum] condition on submodules** *if every nonempty set of submodules of A contains a maximal [resp. minimal] element with respect to set theoretical inclusion.*

Thm 3.1. *A modules A satisfies ACC [resp. DCC] if and only if A satisfies the maximal [resp. minimal] condition on submodules.*

Thm 3.2. *Let $0 \to A \overset{f}{\hookrightarrow} B \overset{g}{\twoheadrightarrow} C \to 0$ be a short exact sequence of modules. Then B satisfies ACC [resp. DCC] if and only if both A and C satisfy it.*

Proof. 1. If B satisfies ACC, it is easy to show that A and C satisfy ACC.

2. If A and C satisfy ACC, we show that B satisfies ACC. Let $B_1 \subset B_2 \subset \cdots$ be a chain of submodules of B. Then $B_1 \cap \operatorname{Im} f \subset B_2 \cap \operatorname{Im} f \subset \cdots$ is a chain of submodules of $\operatorname{Im} f \simeq A$, and $g(B_1) \subset g(B_2) \subset \cdots$ is a chain of submodules of C. For sufficiently large n we have $B_n \cap \operatorname{Im} f = B_{n+1} \cap \operatorname{Im} f = \cdots$ and $g(B_n) = g(B_{n+1}) = \cdots$. Then

$$\frac{B_n + \operatorname{Im} f}{\operatorname{Im} f} = \frac{B_{n+1} + \operatorname{Im} f}{\operatorname{Im} f} = \cdots$$

and thus $B_n = B_{n+1} = \cdots$.

□

Cor 3.3. *If A is a submodule of B, then B satisfies ACC [resp. DCC] if and only if A and B/A satisfy it.*

Cor 3.4. *If $A_1, \cdots, A_n$ are modules, then $A_1 \oplus \cdots \oplus A_n$ satisfies ACC [resp. DCC] if and only if each A_i satisfies it.*

Thm 3.5. *If R is a left Noetherian [resp. Artinian] ring with identity, then every finitely generated unitary left R module A satisfies ACC [resp. DCC].*

Proof. Use Corollaries 3.3 and 3.4. □

Ex. *Every finitely generated module A over a PID R is Noetherian.*

Thm 3.6. *A module A satisfies ACC if and only if every submodule of A is finitely generated. In particular, a commutative ring R is Noetherian if and only if every ideal of R is finitely generated.*

Proof. $\Longrightarrow$: Let $B \leq A$. Let S be the set of all fin gen submods of B. Then S contains a maximum element, say $C = \langle c_1, c_2, \cdots, c_n \rangle$. For every $b \in B$, $\langle b, c_1, \cdots, c_n \rangle$ is in S and so $\langle b, c_1, \cdots, c_n \rangle \leq C$. Therefore, $b \in C$. This shows that $B = C$ is fin gen.

$\Longleftarrow$: Given a chain $A_1 \subset A_2 \subset \cdots$ of submods of A, $\bigcup_{i=1}^{\infty} A_i$ is a submod of A. So $\bigcup_{i=1}^{\infty} A_i = \langle a_1, \cdots, a_k \rangle$ for some a_j's. There is a sufficiently large n such that $a_j \in A_n$ for all j. Then $A_n = A_{n+1} = \cdots = \bigcup_{i=1}^{\infty} A_i$.

□

Def. *A* **normal series** *for a mod A is a chain*

$$A = A_0 \supset A_1 \supset A_2 \supset \cdots .$$

The **factors** *of the series are the quotient mods A_i/A_{i+1}. The number of nontrivial factors in a series are called the* **length**. *Two series of A are* **equivalent** *if there is a one-to-one isomorphic correspondence between the nontrivial factors of these two series.*

Def. *A* **composition series** *for a unitary left R-module A is a series of R-modules $A = A_0 \supset A_1 \supset \cdots \supset A_n = 0$ such that each factor A_k/A_{k+1} is a nonzero module with no proper submodules (i.e. a* **simple module***).*

Thm 3.7. *Any two normal series of a mod A has equivalent refinement. Any two composition series of A are equivalent.*

Proof. (skipped.) □

Thm 3.8. *A nonzero module A has a composition series if and only if A satisfies both ACC and DCC.*

Proof. $\Longrightarrow$: If A has a composition series of length n, then every chain of A has the length at most n.

$\Longleftarrow$: Suppose A satisfies ACC and DCC. For any $C \leq A$, denote S_C be the set of all submods B of C such that $B \neq C$. Then $S_C \neq \emptyset$ when $C \neq 0$. Since A satisfies ACC, all submods of A satisfy ACC and thus satisfy the maximal conditions. Let $A = A_0$. Let

$$A_{k+1} = \begin{cases} \text{the maximal element of } S_{A_k}, & \text{if } A_k \neq 0; \\ 0, & \text{if } A_k = 0. \end{cases}.$$

Then $A = A_0 \supsetneq A_1 \supsetneq A_2 \supsetneq \cdots$. Since A satisfies DCC, there is n such that $A_n = A_{n+1} = \cdots = 0$. Verify that $A_0 \supset A_1 \supset \cdots \supset A_n$ is a composition series of A.

□

3.2 Prime and Primary Ideals, Primary Decompositions

(VIII.2, VIII.3) All rings are commutative rings with identity. All modules are unitary modules.

Ex. *If R is a PID, then every ideal I has the form (a) for $a = p_1^{n_1} \cdots p_r^{n_r}$. So I has the primary decomposition*

$$I = (p_1^{n_1})(p_2^{n_2}) \cdots (p_r^{n_r}) = (p_1^{n_1}) \cap (p_2^{n_2}) \cap \cdots \cap (p_r^{n_r})$$

where $(p_i^{n_i}) = (p_i)^{n_i}$ is a power of prime ideal.

In general, primary decompositions exist for certain ideals and submodules.

3.2.1 Radical and Primary Decompositions of Ideals

We define the radical of an ideal.

Def. *Let I be an ideal of R. The* **radical** *(or* **nilradical***) of I is*

$$Rad\, I := \bigcap_{\substack{P \text{ prime} \\ P \supseteq I}} P.$$

The radical of the zero ideal is called the **nilradical of** *R.*

Ex. *In* $\mathbf{Z}$*, $Rad\,(12) = (2) \cap (3) = (6)$.*

The elements of $\operatorname{Rad} I$ can be described.

Thm 3.9. *$Rad\, I = \{r \in R \mid r^n \in I \ \text{ for some } \ n > 0\}$.*

Proof. If $r^n \in I$ for some $n > 0$, then $r^n \in P$ for every prime ideal $P \supseteq I$. So $r \in P$ and thus $r \in \operatorname{Rad} I$. Therefore, $\{r \in R \mid r^n \in I\} \subseteq \operatorname{Rad} I$.

Conversely, suppose $t^n \notin I$ for all $n > 0$. The set $S = \{t^n \mid n \in \mathbf{Z}^+\}$ has no intersection with I. Let T_I be the set of all ideals that contain I and have no intersection with S. Then $T_I \neq \emptyset$. By Zorn's Lemma, there is a maximal element M in T_I. We claim that M is prime. Suppose there are ideals X and Y such that $XY \subseteq M$ but $X \nsubseteq M$ and $Y \nsubseteq M$. Then $(X + M)(Y + M) \subseteq M$ and $X + M \supsetneq M$, $Y + M \supsetneq M$. There exist $t^m \in X + M$ and $t^n \in Y + M$. Then $t^{m+n} \in (X + M)(Y + M) \subseteq M$, which contradicts $M \in T_I$. So M is a prime ideal that contains I, and $t \notin M$. Therefore $t \notin \operatorname{Rad} I$.

□

Ex. *The nilradical of R is:* $Rad(0) = \{r \in R \mid r^n = 0 \text{ for some } n > 0\}$.

Thm 3.10. *If $I, I_1, I_2, \cdots, I_n$ are ideals of R, then*

1. $Rad(Rad\, I) = Rad\, I$;
2. $Rad(I_1 I_2 \cdots I_n) = Rad(\bigcap_{j=1}^n I_j) = \bigcap_{j=1}^n Rad\, I_j$;
3. $Rad(I^m) = Rad\, I$.

Maximal ideals and prime ideals are the most important ideals in commutative rings. The next important ideals are primary ideals.

Def. *An ideal Q ($\neq R$) in R is* **primary** *if for any $a, b \in R$:*

$$ab \in Q \text{ and } a \notin Q \implies b^n \in Q \text{ for some } n > 0.$$

Ex. *Every prime ideal is primary.*

Thm 3.11. *$Q \lhd R$ is primary $\implies P := Rad\, Q$ is prime. One says that Q* **is primary for** *P.*

Ex. *In $\mathbf{Z}$, let p be a prime, then the primary ideals $(p), (p^2), (p^3), \cdots$ are primary for (p).*

Ex. *In $\mathbf{Z}[x, y]$, the ideals $(x^2, y), (x^2, y^2), (x^2, y^3), \cdots$, are all primary ideals for the prime ideal (x, y) (exercise).*

Thm 3.12. *If $Q_1, Q_2, \cdots, Q_n$ are primary ideals for the prime ideal P, then $\bigcap_{i=1}^n Q_i$ is also a primary ideal for P.*

Def. *An ideal $I \lhd R$ has a* **primary decomposition** *if $I = \bigcap_{i=1}^n Q_i$ with each Q_i primary. If no Q_i contains $\bigcap_{j \neq i} Q_j$ and the radicals of the Q_i are all distinct, then the primary decomposition is said to be* **reduced**.

Thm 3.13. *If $I \lhd R$ has a primary decomposition, then I has a reduced primary decomposition.*

3.2.2 Primary Decompositions of Modules

The primary decomposition for ideals may be extended to modules.

Def. *Let B be an R-module. A submodule A ($\lneq B$) is* **primary** *if*

$$r \in R,\ b \notin A \text{ and } rb \in A \implies r^n B \subset A \text{ for some positive integer } n.$$

Ex. *A primary ideal Q of R is primary as a submodule of R.*

Thm 3.14. *Let A be a primary R-submodule of B. Then*

$$Q_A = \{r \in R \mid rB \subset A\}$$

is a primary ideal in R.

Proof. Suppose $rs \in Q_A$ but $s \notin Q_A$. There is $b \in B$ such that $sb \notin A$. However, $r(sb) = (rs)b \in A$. Then $r^n B \subseteq A$ for some n, since A is primary. Thus $r^n \in Q_A$ and Q_A is primary. □

In Theorem 3.14,

$$P = \operatorname{Rad} Q_A = \{r \in R \mid r^n B \subset A \text{ for some } n > 0\}$$

is a prime ideal of R. We call A a **P-primary submodule of B.**

Def. *Let B be an R-module. A submodule C of B has a* **primary decomposition** *if $C = \bigcap_{i=1}^{n} A_i$ with each A_i a P_i-primary submodule of B for some prime ideal P_i of R. If no A_i contains $\bigcap_{\substack{j=1 \\ j\neq i}}^{n} A_j$ and if the ideals $P_1, \cdots, P_n$ are all distinct, then the primary decomposition is* **reduced**.

Thm 3.15. *If a submodule B of C has a primary decomposition, then B has a reduced primary decomposition.*

(Exercise. c.f. Theorem 3.13)

Which modules have primary decompositions? The following theorem provides a partial answer.

Thm 3.16. *Let B be a Noetherian R-module. Then every submodule A ($\neq B$) has a reduced primary decomposition.*

Idea: If C is a maximal submodule that does not have a primary decomposition, then we find submodules B_k and D such that $C = B_k \cap D$, where B_k and D have primary decompositions. So C has a primary decomposition. A contradiction.

Sketch of proof: Let $\mathcal{S}$ be the set of all submodules of B that do not have a primary decomposition. Suppose on the contrary, $\mathcal{S} \neq \emptyset$. Since B is Noetherian module, there is a maximal element $C \in \mathcal{S}$. C is not primary. There is $r \in R$ and $b \notin C$ such that $rb \in C$ and $r^n B \nsubseteq C$. Denote $B_n = \{x \in B \mid r^n x \in C\}$. Then $C \subsetneq B_1 \subset B_2 \subset \cdots$. There is k such that $B_k = B_{k+1} = \cdots$. Denote the

submodule $D = r^k B + C$. Clearly $C \subset B_k \cap D$. Conversely, if $x \in B_k \cap D$, then $x = r^k y + c$ for $y \in B$ and $c \in C$. Then $r^{2k} y + r^k c = r^k x \in C$. So $r^{2k} y \in C$ and thus $y \in B_{2k} = B_k$ and thus $x = r^k y + c \in C$. This shows that, $B_k \cap D \subset C$. So $C = B_k \cap D$. Now $C \neq B_k \neq B$ and $C \neq D \neq B$. By the maximality of C in $\mathcal{S}$, B_k and D must have primary decompositions. So does C. A contradiction to $C \in \mathcal{S}$. Therefore, $\mathcal{S} = \emptyset$.

Ex. *If R is a Noetherian ring, then every submodule of a finitely generated R-module has a primary decomposition. In particular, every ideal of R has a primary decomposition.*

3.3 Noetherian Modules and Noetherian Rings

(VIII.4) All rings are commutative with identity. All modules are unitary.

On Noetherian Modules, we present Nakayama's Lemma; On Noetherian Rings, we prove that if R is a Noetherian ring then so are the polynomial rings $R[x_1, \cdots, x_n]$ and the power series ring $R[[x]]$.

3.3.1 Noetherian Modules

The **annihilator** of an R-module B is the following ideal of R:

$$I = \mathrm{Ann}\,(B) = \{r \in R \mid rb = 0 \quad \text{for all} \quad b \in B\}.$$

If $B = (X)$, then $\mathrm{Ann}\,(B) = \bigcap_{x \in X} \mathrm{Ann}\,(x)$.

Lem 3.17. *Let I be the annihilator of a finitely generated R-module B. Then B is a Noetherian [resp. Artinian] module if and only if R/I is a Noetherian [resp. Artinian] ring.*

Sketch of proof (Noetherian part):

1. Suppose R/I is Noetherian. Then B may be viewed as a finitely generated R/I-module. So B is Noetherian.
2. If B is Noetherian. Suppose $B = (b_1, \cdots, b_n)$ and $I_j = \mathrm{Ann}\,(b_j)$. Then $I = \mathrm{Ann}\,(B) = \bigcap_{i=1}^{n} I_j$. There is a monomorphism

$$\theta : R/I \to \prod_{i=1}^{n} R/I_j = \bigoplus_{i=1}^{n} R/I_j$$

Note that $R/I_j \simeq (b_j) \subset B$ is Noetherian. So $\bigoplus_{i=1}^{n} R/I_j$ is Noetherian. So R/I is Noetherian.

Lem 3.18 (Nakayama)**.** *Let J be an ideal of a commutative ring R with identity. The following are equivalent:*

(1) J is contained in every maximal ideal of R.

(2) $1_R - j$ is a unit for every $j \in J$.

(3) If A is a finitely generated R-module and $JA = A$, then $A = 0$.

(4) If B is a submodule of a finitely generated R-module A such that $A = JA + B$, then $A = B$.

Sketch of proof:

(1)⇒(2): If $1-j$ is not a unit for some $j \in J$, then the ideal $(1-j) \neq R$ is contained in a maximal ideal M, then $1 = (1-j)+j \in M$. A contradiction.

(2)⇒(3): Suppose $A = (a_1, \cdots, a_n)$ where n is minimal, and $A = JA$. Then $a_1 = j_1a_1 + \cdots + j_na_n$ for some $j_1, \cdots, j_n \in J$. Then $(1-j_1)a_1 = j_2a_2 + \cdots + j_na_n$. Since $1-j_1$ is a unit, we get $a_1 = (1-j_1)^{-1}j_2a_2 + \cdots + (1-j_1)^{-1}j_na_n$. So $A = (a_2, \cdots, a_n)$. Contradict with n minimal.

(3)⇒(4): $J(A/B) = A/B$. So $A/B = 0$ and thus $A = B$.

(4)⇒(1): For every maximal ideal M of R, $M \subset JR + M \neq R$ (Otherwise $M = R$, a contradiction). So $M = JR + M = J + M$ and thus $J \subset M$.

3.3.2 Noetherian Rings

A commutative ring R with identity is Noetherian if and only if the ideals of R satisfy the maximum condition, if and only if every ideal of R is finitely generated, if and only if every *prime ideal* of R is finitely generated (I.S.Cohen).

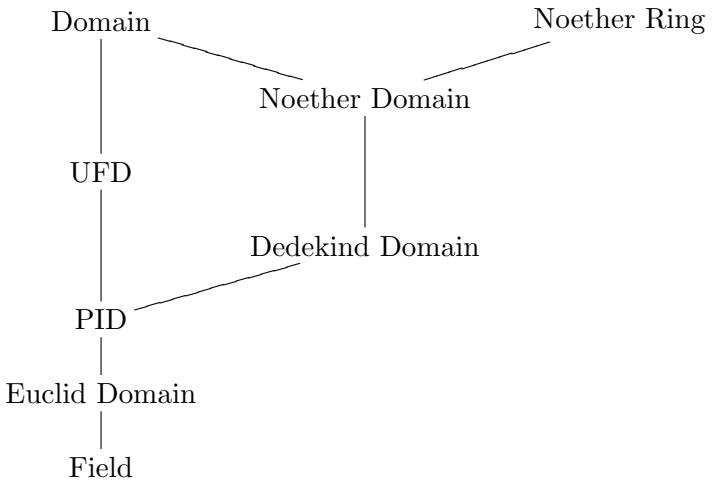
Thm 3.19 (Hilbert Basis Theorem)**.** *If R is a Noetherian ring, then so is $R[x_1, \cdots, x_n]$.*

Sketch of proof: It suffices to show that $R[x]$ is a Noetherian ring. That is, every ideal $J \lhd R[x]$ is finitely generated. Given $J \lhd R[x]$, let $I_n \subset R$ be the set of leading coefficients of polynomials of degree n in J. Then $I_0 \subset I_1 \subset \cdots$ is an ascending chain of ideals in R. There is k such that $I_k = I_{k+1} = \cdots$. The finitely generated R-module $P_k = R + Rx + \cdots + Rx^k$ is Noetherian. So is the submodule $P_k \cap J$. Suppose $P_k \cap J = f_1R + \cdots + f_mR$ for $f_1, \cdots, f_m \in J$. Then $J = f_1R[x] + \cdots + f_mR[x]$ is finitely generated.

Thm 3.20. *If R is Noetherian, then so is $R[[x]]$.*

(The proof is skipped.)

Some Facts about Commutative Rings with Identity:



1. F is a field $\Longrightarrow$ $F[x]$ is a Euclidean domain.
2. R is a UFD $\Longrightarrow$ $R[x_1, \cdots, x_n]$ is a UFD.
3. R is a Noetherian ring $\Longrightarrow$ $R[x_1, \cdots, x_n]$ and $R[[x]]$ are Noetherian rings.
4. An R-module A is a Noetherian module if and only if A is finitely generated and $R/\mathrm{Ann}\,(A)$ is a Noetherian ring. Every submodule of a Noetherian module has reduced primary decomposition.
5. A UFD may not be a PID (e.g. $\mathbf{Z}[x]$).
6. A UFD may not be a Noetherian ring (e.g. $R = \mathbf{C}[x_1, x_2, x_3, \cdots]$, the set of polynomials over ∞ many variables $x_1, x_2, \cdots$).
7. A Noetherian integer domain may not be a UFD. (e.g. $\mathbf{Z}[\sqrt{10}]$ is Noetherian. However, $\mathbf{Z}[\sqrt{10}]$ is not a UFD, since $6 = 3 \cdot 2 = (4 + \sqrt{10})(4 - \sqrt{10})$.)

3.4 Dedekind Domains

(VIII.5, VIII.6)

3.4.1 Ring Extension, Integral Elements

Let R and S be commutative rings with identity.

"S is a **ring extension of** R" $\iff$ $R \leq S$ and $1_R = 1_S$.

Def. *$S \geq R$ ring ext. $u \in S$ is said to be* **integral over** *R, if there is a* monic polynomial *$f(x) \in R[x]$ such that $f(u) = 0$.*

Thm 3.21. *$S \geq R$ ring ext, $u \in S$. The foll are equiv:*

1. *u is integral over R,*
2. *$R[u] = \{f(u) \mid f(x) \in R[x]\}$ is a fin gen R-mod,*
3. *$u \in T$ for some fin gen ring ext $T \geq R$.*

Proof.

1⇒2: Suppose $u^n + a_{n-1}u^{n-1} + \cdots + a_0 = 0$, $a_i \in R$. Then $u^n = -a_{n-1}u^{n-1} - \cdots - a_0$, and $R[u] = R + Ru + \cdots + Ru^{n-1}$ is fin gen.

2⇒3: Let $T = R[u]$.

3⇒1: Suppose $T = Rt_1 + \cdots + Rt_n$. Every $a \in T$ defines an R-mod endomorphism $\varphi_a : T \to T$ by $\varphi_a(t) := at$. Suppose

$$\varphi_u(t_k) = r_{k1}t_1 + \cdots + r_{kn}t_n, \qquad r_{ki} \in R, \quad i = 1, \cdots, n, \ k = 1, \cdots, n.$$

Let $A := [r_{ki}]_{n\times n}$, and $f(x) := \det(xI - A)$ the char polyn of A. Then $f(x)$ is a monic polyn over R. Moreover, $f(A) = 0$, and so $\varphi_{f(u)} = f(\varphi_u) = 0$. So $f(u) = \varphi_{f(u)}(1_R) = 0$ and u is integral over R.

□

Thm 3.22. *$S \geq R$ ring ext. All integral elements of S over R form a ring $\widehat{R}$ with $S \geq \widehat{R} \geq R$.*

Proof. Clearly $R \leq \widehat{R}$. If $u, v \in \widehat{R}$, then $R[u]$ and $R[v]$ are fin gen R-mods, say $R[u] = u_1R + \cdots + u_mR$ and $R[v] = v_1R + \cdots + v_nR$. Then $R[u, v] = (R[u])[v] = \sum_{i=1}^{m}\sum_{j=1}^{n} u_iv_jR$ is also a fin gen R-mod. So $u - v, uv \in R[u, v]$ are both integral over R, i.e. $u - v, uv \in \widehat{R}$. Therefore $\widehat{R} \leq S$ as a subring. □

Def. *R int dom with quotient field $K \geq R$. Then R is called* **integrally closed** *if all integral elements of K over R are in R.*

3.4.2 Fractional Ideals of a Domain

Def. *Let R be an int dom with quotient field K. For $a \in R\backslash\{0\}$ and $\{0\} \neq J \lhd R$. The nonzero R-submodule $a^{-1}J = \left\{\frac{j}{a} \mid j \in J\right\}$ of K is called a* **fractional ideal** *of R.*

Ex. $\{$*ideals of R*$\}$ $=$ $\{$*frac ideals of K that are contained in R*$\}$

Ex. *Every nonzero fin gen R-submod of K is a frac ideal of R.*

Ex. *Let I and J be two frac ideals of R. The followings are also frac ideals of R:*

(i) $IJ = \{\sum_{i=1}^{n} c_i d_i \mid c_i \in I;\ d_i \in J;\ n \in \mathbf{Z}^+\}$.

(ii) $I \cap J$.

(iii) $I + J = \{c + d \mid c \in I;\ d \in J\}$.

Def. *A frac ideal I of R is said to be* **invertible** *if $IJ = R$ for some frac ideal J of R.*

Ex. *Every frac ideal $a^{-1}(b) = (a^{-1}b)R$ is invertible for $b \in R$.*

Remark. *Let I, J, L be frac ideals of R.*

1. *If I is invertible and $IJ = IL$, then $J = I^{-1}(IJ) = I^{-1}(IL) = L$.*
2. *Define*
$$I^{-1} = \{a \in K \mid aI \subseteq R\}.$$
Then I^{-1} is a frac ideal such that
   (a) if $I \subset J$, then $I^{-1} \supset J^{-1}$;
   (b) $(I + J)^{-1} = I^{-1} \cap J^{-1}$;
3. *If I is invertible, then the inverse is unique and is I^{-1}.*
4. *All invertible frac ideals of R form a multiplicative group.*

Lem 3.23. *Let $I, I_1, I_2, \cdots, I_n$ be ideals in an int dom R.*

(i) The ideal $I_1 I_2 \cdots I_n$ is invertible if and only if each I_j is invertible.

(ii) If an invertible ideal $I = P_1 \cdots P_m = Q_1 \cdots Q_n$, where the P_i and Q_j are prime ideals in R, then $m = n$ and (after reindexing) $P_i = Q_i$ for each $i = 1, \cdots, m$.

Proof. 1. Use $(I_1 I_2 \cdots I_n)^{-1} = I_1^{-1} I_2^{-1} \cdots I_n^{-1}$.

2. Induction on m. $m = 1$ is trivial. For $m > 1$, choose a minimal prime ideals among $\{P_1, \cdots, P_n\}$, say P_1. Then $Q_1 \cdots Q_n \subseteq P_1$ implies that $Q_i \subseteq P_1$ for some i, say $Q_1 \subseteq P_1$. Similarly, $P_j \subseteq Q_1$ for some j. By the minimality of P_1, we have $P_j = Q_1 = P_1$. Then $P_2 \cdots P_m = Q_2 \cdots Q_n$. By the induction hypothesis, $m = n$ and $P_i = Q_i$ for $i = 1, \cdots, m$ after reindexing.

□

Now we study invertible frac ideals.

Lem 3.24. *Every invertible frac ideal of an int dom R is a fin gen R-mod.*

Proof: Since $I^{-1}I = R$, there exist $a_i \in I^{-1}$, $b_i \in I$ such that $1_R = \sum_{i=1}^n a_i b_i$. If $c \in I$, then $c = \sum_{i=1}^n (ca_i) b_i \in Rb_1 + \cdots + Rb_n$ since $ca_i \in I^{-1}I = R$. So I is finitely generated by $b_1, \cdots, b_n$.

Thm 3.25. *A frac ideal I of an int dom R is invertible iff I is a projective R-mod.*

(The proof is skipped.)

3.4.3 Structure of Dedekind Domains

Def. *An int dom R is a* **Dedekind domain** *if every ideal I ($\neq R$) is a product of finite many prime ideals: $I = P_1 P_2 \cdots P_n$.*

PID:	Every ideal $I = (a) = (p_1^{s_1} \cdots p_n^{s_n}) = (p_1)^{s_1} \cdots (p_n)^{s_n}$.
Dedekind domain:	Every ideal I is a product of finitely many prime ideals.
Noetherian int dom:	Every ideal I has a primary decomposition.

$\{\text{PIDs}\} \subsetneq \{\text{Dedekind domains}\} \subsetneq \{\text{Noetherian integral domains}\}$.

Thm 3.26. *If R is a Dedekind dom , then every nonzero prime ideal of R is invertible and maximal.*

Proof:

1. Claim: Every invertible prime ideal P is maximal.

   If not, there is $a \in R - P$ such that $P + Ra \neq R$. Then $P \subset P + Ra^2 \subset P + Ra \subsetneq R$. Suppose that $P + Ra^2 = Q_1 \cdots Q_m$ and $P + Ra = P_1 \cdots P_n$ where P_i and Q_j are prime ideals of R. Then $P \subset P_i$ and $P \subset Q_j$. Define $\pi : R \to R/P$ the canonical epimorphism. We have $\pi(Q_1) \cdots \pi(Q_m) = (\pi(a)^2) = (\pi(a))^2 = \pi(P_1)^2 \cdots \pi(P_n)^2$. The principal ideal $(\pi(a)^2)$ is invertible in the integral domain $\pi(R)$. So by Lemma 3.23, $n = 2m$, and after permutation, we may assume that $\pi(P_i) = \pi(Q_{2i-1}) = \pi(Q_{2i})$. Then $P_i = Q_{2i-1} = Q_{2i}$ and thus $P \subset P + Ra^2 = Q_1 \cdots Q_{2n} = P_1^2 \cdots P_n^2 = (P + Ra)^2 \subset P^2 + Ra$. If $p \in P$, then $p = c + ra$ for $c \in P^2$ and $r \in R$. So $ra = p - c \in P$ and thus $r \in P$ and thus $p \in P^2 + Pa$. This shows that $P \subset P^2 + Pa \subset P$. Thus $P = P^2 + Pa = P(P + Ra)$. Since P is invertible, $R = P^{-1}P = P^{-1}P(P + Ra) = P + Ra$. This contradicts to $P + Ra \neq R$.

2. Claim: Every nonzero prime ideal P is invertible and maximal.

   Choose $a \in P \backslash \{0\}$. The principal ideal $(a) = P_1' \cdots P_k'$ is invertible. So each prime ideal P_i' is invertible and so P_i' is maximal. By $P_1' \cdots P_k' = (a) \subset P$ we have some $P_j' \subset P$. This show that $P = P_j'$ is invertible and maximal.

Here is a comprehensive structure thm of Dedekind dom:

Thm 3.27 ($\star$)**.** *The foll conditions on an int dom R are equiv:*

1. *R is a Dedekind dom.*
2. *every proper ideal in R is uniquely a product of a finite number of prime ideals.*
3. *every nonzero ideal in R is invertible. (equiv: i. every frac ideal of R is invertible. ii. the set of all frac ideals of R is a group under multiplication.)*
4. *every ideal in R is projective. (equiv: every frac ideal of R is projective.)*
5. *R is Noetherian, integrally closed and every nonzero prime ideal is maximal.*

Proof.

1⇔2: By definition.

2⇒3: By Thm 3.26 and Lem 3.23.

3⇔4: By Thm 3.25.

3⇒5: Every nonzero ideal is invertible. So the ideal is a fin gen R-mod (Lem 3.24). So R is Noetherian. If $u \in K$ (the quotient field of R) is integral over R, then $R[u]$ is a fin gen R-mod, which must be a frac ideal. By assumption $R[u]$ is invertible. Since $R[u]R[u] = R[u]R$, $R[u] = R$ so that $u \in R$. So R is integrally closed. Finally, if P is nonzero prime but not maximal, then $P \subsetneq M \subsetneq R$ for some ideal M. All nonzero ideals are invertible. Take inverse: $R = R^{-1} \subsetneq M^{-1} \subsetneq P^{-1}$. Multiple all sides by P: $P \subsetneq M^{-1}P \subsetneq R$. So $M^{-1}P \lhd R$. Now $P = M(M^{-1}P)$ but $P \subsetneq M$ and $P \subsetneq M^{-1}P$, a contradiction to P prime.

5⇒2: (A proof is given in VIII.6. Here we briefly sketch an alternative way.) Note that every nonzero ideal in the Noetherian R has a reduced primary decomposition. We will modify this reduced primary decomposition to a product of prime ideals. Let K be the quotient field of R.

(a) Claim: Every nonzero prime ideal P is invertible (cf. Lem VIII.6.9).

Proof: By assumption P is max in R. The frac ideal $P^{-1} = \{a \in K \mid aP \subset R\} \supset R$. So $P \subset P^{-1}P \subset R$. Suppose on the contrary, P is not invertible. Then $P^{-1}P \neq R$ and thus $P^{-1}P = P$. Then P^{-1} is a ring ext of R. Every ideal of the Noether R is fin gen. So is the frac ideal P^{-1}. Then $P^{-1} \geq R$ is a fin gen ring ext. So $P^{-1} = R$ since R is integrally closed. Let

$$\mathcal{F} = \{I \lhd R \mid I \leq P,\ I^{-1} \neq R\}.$$

Then $\mathcal{F} \neq \emptyset$ since $(a) \in \mathcal{F}$ for every $a \in P - \{0\}$. Since R is Noether, there is a max element $M \in \mathcal{F}$. Clearly $\{0\} \subsetneq M \subsetneq P$. We claim that M is prime. Suppose not. Then $ab \in M$ for some $a, b \in R - M$. By $ab \in P$, we may assume that $a \in P - M$ so that $aR + M \leq P$. Then $b(aR + M)M^{-1} \subseteq R$. So $bM^{-1} \subseteq (aR + M)^{-1} = R$. Then $bM^{-1} \subseteq R$ and thus $b \in M$, a contradiction. Hence M is prime, which contradicts the assumption that every nonzero prime ideal is maximal. Therefore, P is invertible.

(b) Claim: If $\mathrm{Rad}\,(Q) = P$ where P is a prime, then $Q = P^k$ for some $k > 0$.

Proof: Suppose not. In Noetherian R, $P = (p_1, \cdots, p_m) = \mathrm{Rad}\,(Q)$ is finitely generated. Suppose $p_i^{n_i} \in Q$ and let $n = \max\{n_1, \cdots, n_m\}$. Then $P^n \subsetneq Q \subset P$. There is k such that $Q \subsetneq P^k$ but $Q \nsubseteq P^{k+1}$. By (a) and Lem 3.23(i), the ideals P and P^k are invertible. So $P^{-k}Q \subsetneq R$ is an ideal. Now $Q = P^k(P^{-k}Q)$ and

$$P = \mathrm{Rad}\,(Q) = \mathrm{Rad}\,(P^k) \cap \mathrm{Rad}\,(P^{-k}Q) = P \cap \mathrm{Rad}\,(P^{-k}Q).$$

Thus $P \subset \mathrm{Rad}\,(P^{-k}Q)$. Since P is maximal, $P = \mathrm{Rad}\,(P^{-k}Q)$ and so $P^{-k}Q \subset P$ and so $Q \subset P^{k+1}$. Contradict to $Q \subsetneq P^{k+1}$.

(c) The ring R is Noetherian. Hence every ideal I has reduced primary decomposition: $I = P_1^{s_1} \cap \cdots \cap P_k^{s_k}$, where P_i are distinct primes. We claim that $I = P_1^{s_1} \cap \cdots \cap P_k^{s_k} = P_1^{s_1} \cdots P_k^{s_k}$ by induction on k.

$k = 1$ is obviously true. Suppose that the claim holds for $k-1$. Denote $Q' = P_1^{s_1} \cap \cdots \cap P_{k-1}^{s_{k-1}} = P_1^{s_1} \cdots P_{k-1}^{s_{k-1}}$. Then

$$Q' \supsetneq P_1^{s_1} \cap \cdots \cap P_k^{s_k} = Q' \cap P_k^{s_k} \supset Q' P_k^{s_k}.$$

Both Q' and $P_k^{s_k}$ are invertible by (a) and Lem 3.23(i). So $R \supsetneq (Q')^{-1}(Q' \cap P_k^{s_k}) \supset P_k^{s_k}$. The ideal $J := (Q')^{-1}(Q' \cap P_k^{s_k})$ has $\mathrm{Rad}\,(J) \supset \mathrm{Rad}\,(P_k^{s_k}) = P_k$. Then $\mathrm{Rad}\,(J) = P_k$ and so $J = P_k^s$ for some $s > 0$ by (b). Then

$$P_k^{s_k} \supsetneq Q' \cap P_k^{s_k} = Q' P_k^s \supset Q' P_k^{s_k}$$

Multiple all sides by $(P_k^{-1})^{s_k}$. Then $R \supsetneq Q' P_k^{s-s_k} \supset Q'$. From $R \supsetneq Q' P_k^{s-s_k}$, we get $P_k^{s_k - s} \supsetneq Q'$. From $Q' P_k^{s-s_k} \supset Q'$, we get $P_k^{s-s_k} \supset R$ and so $R \supset P_k^{s_k - s} \supsetneq Q'$. So $s_k \geq s$. If $s_k > s$, then $P_k \supsetneq Q'$ and so $P_k \supset P_i$ for some $i = 1, \cdots, k-1$, which is impossible since every P_i is maximal and distinct. Therefore, $s = s_k$, and

$$P_1^{s_1} \cap \cdots \cap P_k^{s_k} = Q' \cap P_k^{s_k} = Q' P_k^{s_k} = P_1^{s_1} \cdots P_k^{s_k}.$$

By induction hypothesis, we finish the proof.

□

Ex. *PIDs $\subsetneq$ Dedekind Doms $\subsetneq$ Noether Doms:*

1. $\mathbf{Z}[\sqrt{10}]$ *is a Dedekind domain, but it is not a UFD and so not a PID:*

$$6 = 2 \cdot 3 = (4 + \sqrt{10})(4 - \sqrt{10}).$$

2. *If F is a field, then $F[x_1, x_2]$ is UFD and Noetherian, but not Dedekind, since the prime ideal (x_1) is not maximal.*