Chapter VIII

Artinian rings and modules

Goal: we study certain classes of modules that share some features with finite-dimensional vector spaces over fields. This leads also to a class of rings which turn out to coincide with noetherian rings of dimension 0.

1 - Modules of finite length

Definition - R ring; an R-module M is **simple** if and only if $M \neq \{0\}$ and the only submodules of M are $\{0\}$ and M.

Example - If K is a field, then a K-vector space E is simple $\iff$ $\dim(E) = 1$.

Proposition - If M is simple then the annihilator ideal $\mathrm{Ann}(M) = \{x \in R \mid xM = \{0\}\}$ is maximal in R. In this case, we have for any $m \neq 0$ in M an isomorphism

$$\begin{cases} R/\mathrm{Ann}(M) \xrightarrow{\sim} M \\ x \longmapsto xm. \end{cases}$$

Conversely, if $\mathfrak{m} \subset R$ is maximal, then $R/\mathfrak{m}$ is a simple R-module.

<u>Proof.</u> If $\mathfrak{m} \subset R$ is maximal, then the submodules of $R/\mathfrak{m}$ correspond to ideals $I \subset R$ s.t. $\mathfrak{m} \subset I \subset R$; only $I = \mathfrak{m}$ and $I = R$ have this property, corresponding to the $\{0\}$ and $R/\mathfrak{m}$ submodules, so $R/\mathfrak{m}$ is simple.

Suppose M is simple. For $m \neq 0$ in M, $Rm \subset M$ must be equal to M, so we get an isomorphism

$$\begin{cases} R/\{x \in R \mid xm = 0\} \xrightarrow{\sim} M \\ x \longmapsto xm \end{cases}$$

The ideal $I = \{x \in R \mid xm = 0\}$ must be maxi-
-mal (otherwise R/I has a submodule which is non-zero and not equal to R/I), and moreover

$$I = \mathrm{Ann}(M)$$

because x generates M, as we have seen.

$\square$

<u>Note</u>: if $\mathrm{Ann}(M)$ is maximal, M is not necessarily simple (<u>ex.</u> R field, $M = R^2$ with $\mathrm{Ann}(M) = \{0\}$).

<u>Lemma.</u> ("Schur's Lemma")

If $u : M \longrightarrow N$ is R-linear and $u \neq 0$, then (i) if M is simple, then u is injective

(ii) if N is simple, then u is surjective

(iii) if M, N are simple, then u is an iso-
-morphism.

<u>Proof.</u> In (i), $\mathrm{Ker}(u) \subset M$ is a submodule

not equal to M, so equal to $\{0\}$; in (ii), $\mathrm{Im}(u) \subset N$ is a submodule different from $\{0\}$ so equal to N; and (iii) combines both.

$\square$

<u>Definition</u> – Let M be an R-module. The <u>length of M</u> is the supremum of the lengths k of all chains

$$M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_k \subset M$$

of submodules. It is either in $\mathbb{N}$ or $+\infty$, and is denoted $\ell_R(M)$.

<u>Examples</u> – (1) If R is a field, then $\ell_R(M)$ is either $+\infty$ or $\dim(M)$ when it is finite; so M has finite length if and only if $\dim_R(M)$ is finite.

(2) $\mathbb{Z}$ has infinite length has a $\mathbb{Z}$-module, (although it is free of rank 1): the chains

$$2^k\mathbb{Z} \subset 2^{k-1}\mathbb{Z} \subset \cdots \subset 2\mathbb{Z} \subset \mathbb{Z}$$

have arbitrarily large length.

(3) A simple R-module has length 1, and conversely: $\{0\} \subsetneq M$ is then the only chain in M.

(4) $\ell(M) = 0 \iff M = \{0\}$.

<u>Lemma.</u> Let $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ be a short exact sequence of R-modules. Then M has finite length if and only if M' and M'' have finite length, and then

$$\ell_R(M) = \ell_R(M') + \ell_R(M'').$$

(In particular, if M has finite length and $N \subset M$, then N and M/N have finite length)

<u>Proof.</u> If M has finite length, so does M' since any chain in M' gives a chain in M by applying f, which is injective. And also M'' has finite length since a chain in M'' gives one in M by taking $g^{-1}(M''_i)$ for each term. (This

remains strict because $g(g^{-1}(M''_i)) = M''_i$)

Conversely, suppose M' and M'' have finite length and let $M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_m$ be a chain in M. Define $M'_i = f^{-1}(M_i)$ and $M''_i = g(M_i)$. We have

$$M'_0 \subset \cdots \subset M'_m$$

$$M''_0 \subset \cdots \subset M''_m$$

but some steps could be equalities. However, it is not possible that $M'_i = M'_{i+1}$ and $M''_i = M''_{i+1}$ at the same time (if it is the case then for $x \in M_{i+1}$, we find $y \in M_i$ s.t. $g(x) = g(y)$; then $x - y \in \mathrm{Im}(f)$ so $x - y = f(z)$ for some $z \in f^{-1}(M_{i+1}) = M'_{i+1}$, hence $z \in M'_i$ and $x = y + f(z) \in M_i$, so we conclude that $M_{i+1} = M_i$, contradiction). This means that the length m' of the strict chain deduced from

(M'_i) and the length m'' of the strict chain deduced from (M''_i) [by dropping non-strict inclusions, e.g. $M'_0 \subsetneq M'_1 = M'_2 \subsetneq M'_3$ becomes $M'_0 \subsetneq M'_1 \subsetneq M'_3$ of length 2] satisfy $m' + m'' \geq m$. Hence

$$m \leq \ell_R(M') + \ell_R(M'')$$

so M has finite length $\ell_R(M) \leq \ell_R(M') + \ell_R(M'')$.

To show that there is equality, pick chains

$$\{0\} = M'_0 \subsetneq \cdots \subsetneq M'_{\ell(M')} = M'$$

$$\{0\} = M''_0 \subsetneq \cdots \subsetneq M''_{\ell(M'')} = M''$$

and note that

$$f(M'_0) \subsetneq \cdots \subsetneq f(M'_{\ell(M')}) = g^{-1}(M''_0) \subsetneq \cdots$$
$$\subsetneq g^{-1}(M''_{\ell(M'')}) = M$$

is a chain in M of length

$$\ell_R(M') + \ell_R(M''),$$

so $\ell_R(M) \geq \ell_R(M') + \ell_R(M'')$. $\square$

Theorem. (Jordan–Hölder) [ACL 6.2.11]

(1) A module M has finite length if and only if it has a finite composition series, i.e. a chain

$$\{0\} = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_\ell = M$$

such that M_i / M_{i-1} is a simple R-module for $1 \leq i \leq \ell$. We then have $\ell = \ell_R(M)$.

(2) If this is the case, then any two composition series $(M_i)_{0 \leq i \leq \ell}$ and $(N_j)_{0 \leq j \leq \ell}$ in M have the same length $\ell = \ell_R(M)$, and there exists a bijection $\sigma : \{1, \dots, \ell\} \longrightarrow \{1, \dots, \ell\}$ and for all i, $1 \leq i \leq \ell$, isomorphisms

$$M_i / M_{i-1} \xrightarrow{\sim} N_{\sigma(i)} / N_{\sigma(i)-1}$$

(i.e. the Jordan-Hölder simple factors are unique up to reordering, including for appearing with the same multiplicity)

Proof (1) If M has finite length, then we claim that any chain of length $\ell(M)$ is a composition series. Let $M_0 \subsetneq \dots \subsetneq M_{\ell(M)}$ be such a chain. We must have $M_0 = \{0\}$ and $M_{\ell(M)} = M$ since otherwise we can extend this chain to a longer one. And M_i / M_{i-1} must be simple, because if

$$\{0\} \subsetneq N \subsetneq M_i / M_{i-1}$$

then $$M_{i-1} \subsetneq \pi^{-1}(N) \subsetneq M_i$$ also lengthens the chain (here $\pi : M_i \longrightarrow M_i / M_{i-1}$ is the projection).

Conversely, if we have a composition series

$$\{0\} = M_0 \subsetneq M_1 \subsetneq \dots \subsetneq M_k = M$$

then we claim that $\ell(M_i) = i$ for all i, so $\ell(M) = k$. Indeed, $\ell(M_0) = 0$ and we have short exact sequences

$$0 \to M_{i-1} \longrightarrow M_i \longrightarrow M_i/_{M_{i-1}} \longrightarrow 0$$

which show using the previous lemma that

$$\ell(M_i) = \ell(M_{i-1}) + 1 ,$$

hence the result by induction.

(2) The idea to compare two composition series is to use one to "interpolate" steps between successive modules in the other.

Precisely, let i with $1 \leq i \leq \ell$ given. For $0 \leq j \leq \ell$, let

$$M_{i,j} = M_{i-1} + M_i \cap N_j .$$

Note that

$$M_{i,0} = M_{i-1} \subset M_{i,1} \subset \dots \subset M_{i,\ell} = M_i$$

so in the quotient we have

$$\{0\} \subset M_{i,1}/_{M_{i-1}} \subset \dots \subset M_{i,j}/_{M_{i-1}} \subset \dots \subset M_i/_{M_{i-1}}$$

and since M_i/M_{i-1} is simple, there exists a <u>unique</u> integer $j = \sigma(i)$, $1 \leq \sigma(i) \leq \ell$, such that

$$\begin{cases} M_{i,j-1} = M_{i-1} \\ M_{i,j} = M_i . \end{cases} \qquad (1)$$

Similarly, let $N_{j,i} = N_{j-1} + N_j \cap M_i$. There exists a unique $i = \tau(j)$ such that

$$\begin{cases} N_{j,i-1} = N_{j-1} \\ N_{j,i} = N_j . \end{cases} \qquad (2)$$

The last part of the proof is to show that σ and τ are reciprocal bijections. To do this, we use the following

Claim: for all i and j, there are isomorphisms

$$\begin{array}{ccc} M_{i,j}/M_{i,j-1} & \xrightarrow[\sim]{\alpha} & M_i \cap N_j / \underbrace{(M_{i-1} \cap N_j + M_i \cap N_{j-1})}_{= P_{i,j}} \\ & & \wr\big\uparrow \beta \\ & & N_{j,i}/N_{j,i-1} \end{array}$$

induced by

$$\alpha(m+n) = n + P_{i,j}$$

$$\beta(n' + m') = m' + P_{ij}$$

for $\begin{cases} m \in M_{i-1}, & n \in M_i \cap N_j \\ n' \in N_{j-1}, & m' \in M_i \cap N_j \end{cases}$.

If we assume this, it follows from the characterization of σ, τ that $j = \sigma(i)$ if and only if $i = \tau(j)$. This ensures that σ and τ are indeed reciprocal bijections, (because $j = \sigma(\tau(j))$ and $i = \tau(\sigma(i))$ follows ...) and then the Claim and the formulas (1), (2) give an isomorphism

$$M_i / M_{i-1} = M_{i,\sigma(i)} \Big/ M_{i,\sigma(i-1)} \xrightarrow{\sim} N_{\sigma(i)} \Big/ N_{\sigma(i)-1} .$$

So we need only prove the Claim. To do this, we check that α, β are well-defined and construct their inverse isomorphisms. By symmetry, we may consider α only. To see that α is well-defined, we observe that if m_1, m_2 are in M_{i-1}, n_1, n_2 in $M_i \cap N_j$ and $m_1 + n_1 = m_2 + n_2$, then $n_1 - n_2 = m_2 - m_1$ is in $M_{i-1} \cap N_j \subset P_{ij}$, so

$$n_1 + P_{ij} = n_2 + P_{ij},$$

as we wanted. Now we construct the inverse

$$M_i \cap N_j / P_{ij} \xrightarrow{\gamma} M_{i-1} + M_i \cap N_j / M_{i-1} + M_i \cap N_{j-1}$$

by $m + P_{ij} \longmapsto m + M_{i,j-1}$.

This is well-defined because

$$P_{ij} = M_{i-1} \cap N_j + M_i \cap N_{j-1} \subset M_{i-1} + M_i \cap N_{j-1}.$$

Finally

$$\alpha(\gamma(m + P_{ij})) = \alpha(m + M_{i,j-1}) = m + P_{ij}$$

$$\gamma(\alpha(m + n + M_{i,j-1})) = \gamma(n + P_{ij}) = n + M_{i,j-1}$$
$$= m + n + M_{i,j-1}$$

(because $m \in M_{i-1} \subset M_{i,j-1}$)

$\square$

Examples -

(1) If K is a field, and E a finite-dim. K-vector space, then a composition series is a sequence $\{0\} \subset E_1 \subset \dots \subset E_{\dim(K)} = E$ with $\dim_K(E_i) = i$ for all i. (Such objects are called "flags"; they are very important in Lie theory and its applications.)

We see here that there are usually <u>many</u> composition series (uncountably many, for instance, if $K = \mathbb{R}$ or $\mathbb{C}$ and $\dim M \geq 2$), but the successive quotients are of course all isomorphic to K.

(2) Let $R = \mathbb{Z}$. Then an abelian group M is a $\mathbb{Z}$-module of finite length if and only if M is finite. If M has n elements and

$$n = p_1^{k_1} \cdots p_m^{k_m} \quad , \quad p_i \text{ distinct primes}, \ k_i \geq 1$$

then the composition series for M all have exactly k_i quotients isomorphic to the simple module $\mathbb{Z}/p_i\mathbb{Z}$. [Because if we have a chain

$M_0 \subset \dots \subset M_n \subset M$, then it is easy

to prove by induction that the size of

M_n is $\mathrm{Card}(M_0)\,\mathrm{Card}(M_1/M_0)\dots\mathrm{Card}(M_n/M_{n-1})$]

In particular, this shows that different modules can have composition series with the same set of successive quotients (with multiplicity), for instance

$$\underbrace{\mathbb{Z}/4\mathbb{Z} \supset 2\mathbb{Z}/4\mathbb{Z}}_{\text{quotient } \mathbb{Z}/2\mathbb{Z}} \supset \{0\} \qquad 2\mathbb{Z}/4\mathbb{Z} \supset \{0\}: \text{ quotient } \mathbb{Z}/2\mathbb{Z}$$

$$\overbrace{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \supset \mathbb{Z}/2\mathbb{Z} \times \{0\}}^{\text{quotient } \mathbb{Z}/2\mathbb{Z}} \supset \{0\} \qquad \mathbb{Z}/2\mathbb{Z} \times \{0\} \supset \{0\}: \text{ quotient } \mathbb{Z}/2\mathbb{Z}$$

If we apply the Jordan-Hölder Theorem to $M = \mathbb{Z}/n\mathbb{Z}$, the same argument actually also implies the existence and uniqueness of factorization into prime powers (i.e, that $\mathbb{Z}$ is a UFD).

2 - Artinian modules and rings

Definition - R ring.

(1) An R-module M is artinian if one of the two following equivalent conditions hold

(i) Any non-empty set of submodules of M has a minimal element

(ii) Any decreasing sequence

$$M \supset M_0 \supset M_1 \supset \dots \supset M_n \supset \dots$$

is stationary: there exists n_0 s.t. $M_n = M_{n_0}$ for $n \geq n_0$. [The equivalence follows from the proof of (ii) $\Leftrightarrow$ (iii) in the Prop. on p. 3 of Chapter IV, in particular see the remark on p. 5]

(2) The ring R is artinian if it is artinian as a module over itself

Examples. (1) A field, or more generally any ring with finitely many ideals, is artinian.

(2) Any simple module is artinian.

(3) $\mathbb{Z}$ is not artinian since

$$\mathbb{Z} \supsetneq 2\mathbb{Z} \supsetneq 4\mathbb{Z} \supsetneq \cdots \supsetneq 2^n\mathbb{Z} \supsetneq \cdots$$

In fact, this last example immediately generalizes to the following result, which shows that artinian and noetherian rings are very different!

Proposition. Let R be an artinian ring.

(1) R has only finitely many maximal ideals

(2) If R is an integral domain, then R is a field.

Proof. (1) If $(m_1, \dots, m_k, \dots)$ are pairwise distinct maximal ideals in a ring R (arbitrary) then $R \supset m_1 \supset m_1 \cap m_2 \supset \cdots \supset m_1 \cap \dots \cap m_k$ is a strict chain (for instance, because we can deduce from the Chinese Remainder Theorem that

$$R/_{m_1 \cap \cdots \cap m_k} \xrightarrow{\sim} R/_{m_1} \times \cdots \times R/_{m_k}$$

and the RHS is a ring with exactly k maximal ideals, namely $R/_{m_1} \times \cdots \times \underset{\substack{\uparrow \\ j\text{-th place}}}{\{0\}} \times \cdots \times R/_{m_k}$).

So if R is artinian, we cannot find infinitely many distinct maximal ideals.

(2) Let $a \in R$. Then the chain

$$R \supset aR \supset a^2R \supset \cdots \supset a^nR \supset \cdots$$

implies the existence of $n \geq 0$ such that

$$a^nR = a^{n+1}R, \text{ in particular}$$

$$a^{n+1} = a^n b$$

for some $b \in R$. If $a \neq 0$ and R is an integral domain, then this implies $ab = 1$, so a is invertible.

$\square$

We also have the standard property:

<u>Proposition.</u> Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules. Then M is artinian if and only if M' and M'' are artinian.

The proof is left as an exercise (it is similar to the case of noetherian modules).

<u>Corollary.</u> Any finite direct sum of artinian modules is artinian.

It is also easy to prove the following:

<u>Proposition.</u> Let $S \subset R$ be a multiplicative set. If M is an artinian R-module, then $S^{-1}M$ is an artinian $S^{-1}R$-module. In particular, if R is an artinian ring, then $S^{-1}R$ is also artinian.

(See ACL 6.4.6 for the proof if needed.)

Similarly, for $I \subset R$ ideal, the ring R/I is artinian.

[ACL 6.4.8]

Proposition. Let M be an R-module. Then

M has finite length if and only if M is artinian and noetherian.

Proof. Suppose that M has finite length. Then any sequence $M_0 \subset \cdots \subset M_n \subset \cdots$ must be stationary [because $\ell(M_n) \leq \ell(M)$, so we have $\ell(M_n) = \ell(M_{n_0})$ for some n_0 and $n \geq n_0$; and $M_n \subset M_{n+1}$ with $\ell(M_n) = \ell(M_{n+1})$ implies $M_n = M_{n+1}$, from

$$\ell(M_n) + \ell(M_{n+1}/M_n) = \ell(M_{n+1})\;]$$

and similarly for a decreasing sequence. So M is both noetherian and artinian.

Conversely, assume that M is artinian and noetherian. Let X be the set of $M' \subset M$ with finite length. The set X is not empty since $\{0\} \in X$; since M is noetherian, there exists a maximal element

$M' \in X$. If $M' = M$, we are done. Otherwise, the set Y of modules $M'' \supsetneq M'$ is not empty (it contains M); since M is artinian, there exists a minimal $M'' \in Y$. But then M''/M' must be simple (otherwise we can find N s.t. $M' \subsetneq N \subsetneq M''$ and $N \in Y$ is smaller than M''), and from

$$0 \to M' \longrightarrow M'' \longrightarrow M''/M' \longrightarrow 0$$

we deduce that M'' has finite length, which contradicts the maximality of M'.

$\square$

Example. (1) Any finitely-generated $\mathbb{Z}$-module which is infinite is an example of a noetherian, non-artinian, module.

(2) Let $M = \mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$; then M is an artinian $\mathbb{Z}$-module of infinite length (next exercise sheet).

Now comes the main theorem of this section, a quite surprising one:

Theorem (Akizuki-[Hopkins-Levitzki]) [ACL 6.4.11 6.4.14]

A ring R is artinian if and only if R is noetherian of dimension 0.

Proof. In both directions, we will deduce from the assumption that R has finite length as an R-module; by the proposition above, this will imply that R is noetherian (resp. artinian) if it was assumed to be artinian (resp. noetherian).

(1) Assume first that R is artinian. We first check that $\dim(R)=0$, or in other words that any prime ideal $p \subset R$ is maximal. Indeed the quotient is an integral domain, and is artinian also, so it is a field, so the ideal p is maximal.

It remains to prove that R is noetherian, and we do this by showing that $\ell_R(R)$ is finite. For this purpose, let $m_1, \dots, m_k$ be the finitely many prime ideals in R, and let $J = m_1 \cap \dots \cap m_k$ be the Jacobson radical. We will use the decreasing sequence

$$\begin{array}{ccccccccc}
R \supset m_1 \supset m_1 m_2 \supset \cdots \supset m_1 \cdots m_k = J \\
J^2 \subset \cdots\cdots \subset m_1 m_2 J \subset m_1 J \\
m_1 J^2 \supset \cdots \cdots \supset J^d
\end{array}$$

for $d \geq 1$ (we have $m_1 \cdots m_k = J$ because $I_1 I_2 = I_1 \cap I_2$ for ideals s.t. $I_1 + I_2 = R$: clearly $I_1 I_2 \subset I_1 \cap I_2$, and conversely if $x \in I_1 \cap I_2$ and $1 = x_1 + x_2$ with $x_i \in I_i$, then $x = x x_1 + x x_2 \in I_1 I_2$). Note that the successive quotients are always of the form $I/_{mI}$ for some ideal $I \subset R$ and some maximal ideal. This quotient is an artinian $R/_m$ - vector space, so it is finite - dimensional (if E is a K - vector space with infinite dimension then $\{F \subset E \mid \dim(F) = +\infty\}$ is $\neq \emptyset$ and has no minimal element). So we see from the sequence of ideals above that $\ell_R(R)$ is finite provided we can show that $J^d = \{0\}$ for some integer $d \geqslant 1$. (We can expect this to be true, because there exists d s.t. $J^{d+1} = J^d$ by the artinian property, and $J^d = \{0\}$ would follow from Nakayama's Lemma if we knew that J is finitely-generated)

To prove that $J^d = \{0\}$ if $J^{d+1} = J^d$, let $X = \{I \subset R \mid IJ^d \neq \{0\}\}$. If $J^d \neq \{0\}$, then X is not empty since $I = J \in X$ then. In this case, there exists a minimal ideal $I \in X$. Since IJ^d is not zero, there exists $x \in I$ such that $xJ^d \neq \{0\}$; but then $xR \subset I$ is in X, so $xR = I$ by minimality. Also, we have $(IJ)J^d = IJ^{d+1} = IJ^d$ which is non-zero so $IJ \subset I$ is in X, and so by minimality $IJ = I$. Now Nakayama's Lemma applies (since $I = xR$) to imply $I = \{0\}$, but that is impossible.

(2) Conversely, we assume that R is noetherian of dimension zero, and will show that $\ell_R(R) < +\infty$ to deduce that R is noetherian. We proceed by contradiction: let $X = \{ I \subset R \mid \ell(R/I) = +\infty \}$; if $\ell(R) = +\infty$, then $X \neq \emptyset$ ($\{0\} \in X$), and therefore X has a <u>maximal</u> element I. So R/I has infinite length but R/I' has finite length if $I' \supsetneq I$. We now observe that by replacing R by R/I, which is still noetherian of dimension zero, we may as well assume that $I = \{0\}$. The key step is to deduce then that R is an <u>integral domain</u>. Indeed, if this is the case, then R is a field (since $\dim(R) = 0$), which is a

contradiction since we would have $\ell_R(R) = 1$.

To prove the claim, let a and b be elements of R such that $ab = 0$.

We then have a short exact sequences:

$$0 \longrightarrow bR \longrightarrow R \longrightarrow R/bR \longrightarrow 0$$

and a surjective map $\begin{cases} R/aR \longrightarrow bR \\ x \longmapsto bx \end{cases}$, which is well-defined since $ab = 0$. Since R has infinite length, either bR or R/bR has infinite length. If R/bR has infinite length, we must have $b = 0$ (since otherwise $bR \neq \{0\}$). If bR has infinite length, then R/aR also, which means that $a = 0$. This concludes the proof.

$\square$

3 _ The Principal Ideal Theorem

Properties of artinian rings will now be used to prove Krull's "Hauptidealsatz".

We recall the statement:

Theorem (Krull). Let R be a noetherian ring and $a \in R$ which is not a unit.

(1) There exist <u>minimal</u> prime ideals $p \supset aR$

(2) For any such prime ideal, we have $ht(p) \leq 1$, with equality if a is not a zero divisor.

Part (1) is a special case of the following more general fact (with $I = aR \neq R$ since $a \notin R^\times$):

Proposition. Let R be any ring and let $I \subset q$ be an ideal $I \subsetneq R$ and a prime ideal q containing I [such q always exist since I is contained in some maximal ideal].

There exists a prime ideal p s.t. $I \subset p \subset q$ and such that p is minimal for inclusion with this property.

Proof. This is an application of Zorn's Lemma: let $\mathcal{O}$ be the ordered set of prime ideals p with $I \subset p \subset q$, ordered by reverse inclusion. So $\mathcal{O} \neq \emptyset$ ($q \in \mathcal{O}$) and we claim that any totally ordered subset has an upper-bound. Indeed, let $X \subset \mathcal{O}$ be such a set; define $\tilde{p} = \bigcap_{p \in X} p$; then $\tilde{p}$ is an ideal s.t. $I \subset \tilde{p} \subset p$ for all $p \in X$, and it only remains to prove that $\tilde{p}$ is prime.

Suppose then that $ab \in \tilde{p}$ and $a \notin \tilde{p}$. Let $p \in X$. Then $ab \in p$, which is prime, so there are two cases:

(i) $a \in p$; since $a \notin \tilde{p}$, we can then find $p_1 \subset p$ in X with $a \notin p_1$, and then $ab \in p_1$, so $b \in p_1$, and so $b \in p$ also.

(ii) or $b \in p$.

In case case, we got $b \in p$, so $b \in \bigcap_{p \in X} p = \tilde{p}$.

Thus we can use Zorn's Lemma and conclude that $\mathcal{O}$ has a maximal element, which is precisely what we wanted.

$\square$

Now we come to the proof of (2). Let $a \in R - R^\times$ and let $p \supset aR$ be a minimal prime ideal containing a. Assume there is a prime $q \subsetneq p$ (if there is none, then $ht(p) = 0$, so we are done) and let q_1 be a prime ideal with $q_1 \subset q \subsetneq p$.

We need to prove that $q = q_1$.

<u>Step 1</u> - We may assume $q_1 = \{0\}$ and R local with maximal ideal p (i.e. R is a noetherian local integral domain with maximal ideal p).

Indeed, replace first (R, a, p, q, q_1) by $(R/q_1, a+q_1, p/q_1, q/q_1, \{0\})$ to reduce to R integral domain (still noetherian), then in that case replace $(R, a, p, q, \{0\})$ by $(R_p, a, pR_p, qR_p, \{0\})$ to have a local integral domain (still noetherian, although we did not prove that in Chapter IV — see below for the simple argument).

Step 2 – It suffices to prove that $q^n = \{0\}$ for some $n \geqslant 1$. Indeed, in an integral domain, $I^n = \{0\} \iff I = \{0\}$, since it implies $a^n = 0$ for all $a \in I$, so $a = 0$.

Step 3 – For $n \geqslant 1$, let

$$s_n = q^n R_q \cap R \subset R.$$

Then the s_n are ideals and we have:

(i) $s_{n+1} \subset s_n$ and $q^n \subset s_n$ for all $n \geqslant 1$

(ii) $s_n = \{ x \in R \mid \exists\, y \notin q,\ xy \in q^n \}$

(indeed, if $\begin{cases} xy \in q^n \\ y \notin q \end{cases}$ then $x = \frac{xy}{y} \in q^n R_q \cap R$

and if $x = \frac{a}{b}$ with $a \in q^n$ and $b \notin q$ then $xb = a \in q^n$)

(iii) $s_n R_q = q^n R_q$

(indeed, $q^n R_q \subset s_n R_q$ since $q^n \subset s_n$ and if $x \in s_n$ and $y \notin q$, then for $z \notin q$ s.t. $xz \in q^n$, we have $\frac{x}{y} = \frac{xz}{yz} \in q^n R_q$)

Step 4. The ring $R/_{aR}$ is artinian.

Indeed, $R/_{aR}$ is noetherian and since p is the unique prime ideal containing aR (because it is minimal containing aR and a maximal ideal), it has a unique prime ideal, which is maximal, so it has dimension 0, and we can apply Akizuki's Theorem.

Step 5. There exists $n \geq 1$ s.t.

$$s_{n+1} + aR = s_n + aR \qquad (1)$$

and

$$s_n = s_{n+1} + p\, s_n \qquad (2)$$

Indeed, in the Artinian ring $R/_{aR}$, the decreasing sequence $(s_n + aR)/_{aR}$ is stationary, so there exists $n \geq 1$ s.t.

$$(s_n + aR)/_{aR} = (s_{n+1} + aR)/_{aR}.$$

which is the same as (1).

To deduce (2), note first that $s_{n+1} + p\, s_n \subset s_n$.

Conversely, let $x \in s_n$. By (1), there exists $y \in s_{n+1}$ and $b \in R$ such that $x = y + ab$. We claim that $b \in s_n$; then since $a \in p$, we get $x \in s_{n+1} + p s_n$, obtaining (2). To check the claim, note $ab = x - y \in s_n$, so by (ii) in Step 3, there exists $c \notin q$ such that $abc \in q^n$. On the other hand $a \notin q$ (otherwise p would not be minimal containing a), so $ac \notin q$ and $(ac)b \in q^n$ gives $b \in s_n$, as claimed.

Step 6. With the same value of n, we have $s_{n+1} = s_n$.

Indeed, from $s_n = s_{n+1} + p s_n$ we get

$$s_n / s_{n+1} = p \; s_n / s_{n+1}$$

hence $s_n / s_{n+1} = \{0\}$ by Nakayama's Lemma (since R is local so p is the Jacobson radical of R).

Step 7. Again for the same n, we have $q^n = \{0\}$.

Indeed if $s_n = s_{n+1}$ we get

$$q^n R_q = s_n R_q = s_{n+1} R_q = q^{n+1} R_q$$

hence (since qR_q is the Jacobson radical of R_q) by Nakayama's Lemma again, we have $q^n R_q = \{0\}$ and $q^n \subset q^n R_q$ (because R is an integral domain) is also zero.

This finishes the proof that $ht(p) \leq 1$.

We get equality easily if R was an integral domain to start with, since then

$$\{0\} \subsetneq aR \subset p$$

shows that $ht(p) \geq 1$. The general case, for a not a divisor of zero is a bit more involved and we omit the proof.

$\square$

Here is a nice corollary of the Principal Ideal Theorem, which was already mentioned:

Corollary. Let R be a noetherian integral domain. Then R is a UFD $\Leftrightarrow$ every prime ideal of height 1 is principal.

Proof. We already saw in Chapter VI that in a UFD, the prime ideals of height 1 are principal.

Conversely, suppose the condition holds, for R a noetherian integral domain. It is classical that the noetherian condition (even that increasing sequences of principal ideals are stationary) suffices to prove existence of factorization in irreducibles, and that uniqueness amounts to proving that if $a \in R$ is irreducible, then aR is a prime ideal. But let $p \supset aR$ be a minimal prime ideal; by the Principal Ideal Theorem, p has height 1, so by assumption we have $p = bR$ for some $b \in R - R^\times$. Then $aR \subset bR$ implies $b \mid a$

which means that $a = bu$ and $u \in R^\times$ since $b \notin R^\times$. Then $aR = bR = p$ is prime.

$\square$

Another consequence of the Principal Ideal Theorem is the following, which we will not prove:

Theorem. [ACL 9.4.3]

Let R be noetherian and let $p \subset R$ be a prime ideal. Then

(i) $ht(p)$ is finite

(ii) $ht(p)$ is the smallest $n \geq 0$ such that:

(a) $\exists\, (a_1, \dots, a_n) \in R^n$ with $a_i \in p$ for all i

(b) p is a minimal prime ideal with the property (a).

Corollary. If R is a noetherian local ring, then $\dim(R) < +\infty$ (since $\dim(R) = ht(m)$).

We now prove the simple property about localization of noetherian rings used in step 1:

<u>Proposition</u> – Let R be a noetherian ring, $S \subset R$ multiplicative. Then $S^{-1}R$ is noetherian.

<u>Proof</u>. Let $I \subset S^{-1}R$ be an ideal and $J = \varphi^{-1}(I)$, where $\varphi : R \longrightarrow S^{-1}R$ is the canonical morphism. Let $(x_1, \dots, x_n)$ in R be generators of J. We claim that $\left(\frac{x_1}{1}, \dots, \frac{x_n}{1}\right)$ generate I.

Indeed, let $x = \frac{a}{s} \in I$. Then $sx = \frac{a}{1} \in I$ so $a \in J$. Write

$$a = \sum_{i=1}^{n} b_i x_i , \qquad b_i \in R$$

then

$$x = \sum \frac{b_i}{s} \cdot \frac{x_i}{1}$$

hence the result.

$\square$