Chapter III

Constructions of rings

<u>Goal:</u> we will present three of the most important general constructions of rings, and describe some of their most important properties.
Each of these constructions plays fundamental roles in commutative algebra.

1 _ Quotient rings [ACL 1.5]

Recall that if R is a ring, $I \subset R$ an ideal, the quotient abelian group R/I has the structure of a ring with

$$\underbrace{(r+I)}_{\text{class of } r \text{ in } R/I}(s+I) = rs + I.$$

This can be characterized by the fact that the quotient morphism $\pi : R \longrightarrow R/I$ is a ring morphism. In particular

<u>Fact</u> - R/I is an R-algebra (with π as structure morphism).

Another way to interpret the properties of R/I is :

(ACL 1.5.3)

<u>Prop.</u> For any ring S, there is a bijection

$$\mathrm{Hom}_{\mathrm{Rings}}(R/I, S) \longrightarrow \{ f : R \underset{\substack{\text{ring} \\ \text{morphism}}}{\longrightarrow} S \mid I \subset \ker(f) \}$$

given by $g \longmapsto g \circ \pi$.

$$\begin{tikzcd} R/I \arrow[r, "g"] & S \\ R \arrow[u, "\pi"] \arrow[ur, "f"'] & \end{tikzcd}$$

(Given f with $I \subset \ker(f)$, we can "pass to the quotient")

Another important property is the fact

that we can understand ideals in R/I:

Prop. [ACL 1.5.4, 1.5.5]

There are reciprocal bijections

$$\{\text{ideals of } R/I\} \rightleftarrows \{\text{ideals of } R \text{ containing } I\}$$

$$J \longmapsto \pi^{-1}(J)$$

$$\pi(J) \longleftarrow J$$

These bijections are compatible with inclusions [e.g. $J_1 \subset J_2 \Rightarrow \pi(J_1) \subset \pi(J_2)$].

Moreover, they preserve the corresponding subsets of prime ideals / maximal ideals:

$$\left\{\begin{Bmatrix}\text{prime}\\ \text{maximal}\end{Bmatrix} \text{ ideals } P \subset R/I\right\} \rightleftarrows \left\{\begin{Bmatrix}\text{prime}\\ \text{maximal}\end{Bmatrix} P \subset R \text{ s.t. } I \subset P\right\}$$

Proof. We explain the last point only:

let $J \subset R$ correspond to $\tilde{J} \subset R/I$

(so $\tilde{J} = J/I$, $J = \pi^{-1}(\tilde{J})$).

There is a morphism of rings

$$R \xrightarrow{\pi_I} R/I \xrightarrow{\pi_{\tilde{J}}} (R/I)/\tilde{J}$$

with kernel

$$\ker(\pi_{\tilde{J}} \circ \pi_I) = \{ r \in R \mid \pi_I(r) \in \tilde{J} \}$$
$$= \pi^{-1}(\tilde{J}) = J$$

so we have an induced isomorphism

$$R/J \xrightarrow{\sim} (R/I)_{\tilde{J}}$$

used to denote "isomorphism"

In particular, each of these rings is an integral domain (resp. a field) if and only if the other one is.

$\square$

Last construction: given an R/I-module M, we can view it as an R-module (by $r \cdot m = \pi(r) m \in M$; this works for any module over an R-algebra S).

This has the property that

$$i \cdot m = 0 \quad , \quad i \in I, \quad m \in M.$$

Conversely, given an R-module N with this property (one says also that $I \subset \mathrm{Ann}_R(N)$) we can define an R/I-module structure by

$$(r+I) \cdot m = rm.$$

For any R-module M, we can define

IM = submodule generated by the $i \cdot m$

and then M/IM is an R/I-module.

3 _ Polynomial rings [ACL 1.3.5]

The second construction is that of general polynomial ring over R: given a set I (maybe infinite) and "indeterminates"/"variables" $(X_i)_{i \in I}$, there is the ring

$$A = R[(X_i)_{i \in I}]$$

of polynomials in these variables. An

element of A is a (finite) linear combi-
-nation, with coefficients in R, of monomials

$$Q = X_{i_1}^{n_1} \cdots\cdots X_{i_k}^{n_k}$$

where $k \geq 0$, $i_1, \ldots, i_k$ are distinct elements of I, $n_i \geq 1$. [The case $k=0$ gives $Q = 1_A$, the unit of A.]

Note that A is an R-algebra with structure morphism $r \longmapsto r \cdot 1_A$; this is injective.

As earlier, there is an abstract inter-
-pretation:

Prop. Given any R-algebra S,
there is a bijection

$$\mathrm{Hom}_{(R\text{-alg})}\left(R[(X_i)], S\right) \longrightarrow \mathrm{Hom}_{(\mathrm{Sets})}(I, S)$$

the set underlying S

$$f \longmapsto \left(i \longmapsto f(X_i)\right).$$

In other words, to give a morphism f of R-algebras [i.e. R-linear] from the polynomial ring to S, it is enough / necessary to give an element s_i of S for each variable X_i; this morphism f is characterized by the fact that

$$f(X_i) = s_i$$

(together with the R-linearity):

$$f\left(r \, X_{i_1}^{n_1} \cdots X_{i_k}^{n_k}\right) = r \cdot s_1^{n_1} \cdots s_k^{n_k}$$

multiplication by R in S

Ex.

$$\begin{aligned} \mathrm{Hom}_{(R\text{-alg})}(R[X], S) &\xrightarrow{\sim} S \\ f &\longmapsto f(X) \end{aligned}$$

bijection of sets

A similar fact is that to give to an R-module M the structure of an $R[(X_i)]$-

module, it is necessary and sufficient to give a family $(u_i)_{i \in I}$ of <u>commuting</u> R-linear maps $M \xrightarrow{u_i} M$, with then

$$X_{i_1}^{n_1} \cdots X_{i_h}^{n_h} \cdot m = (u_1^{n_1} \circ \cdots \circ u_h^{n_h})(m)$$

<u>Ex.</u> $\{R[X]\text{-module structures on } M\} \xrightarrow{\sim} \underset{(R\text{-mod})}{\mathrm{Hom}}(M, M)$.

<u>Definition</u> – (Subalgebra generated by a set)

Let S be an R-algebra and $G \subset S$. We can form the polynomial algebra $A = R[(X_g)_{g \in G}]$ and there is a "canonical" morphism

$$\varphi_G \begin{cases} A \longrightarrow R \\ X_g \longmapsto g \end{cases}$$

One says that the image of φ_G is the subalgebra generated by G; if φ_G is surjective, then one says that <u>S is</u>

generated by G (as an R-algebra).
If there is a finite set G generating S, then S is called finitely-generated.

Ex. (1) $R[X_1, \ldots, X_n]$ is finitely-generated.

(2) If S is finitely-generated over R, then there exists $n \geq 0$ and an ideal $I \subset R[X_1, \ldots, X_n]$ s.t. S is isomorphic to $R[X_1, \ldots, X_n]/I$.

Remark. There is no real relation between ideals of R and ideals of $R[(X_i)]$.

3. Localization [ACL 1.6]

This third construction is probably new. It is a generalization of the construction of the fraction field of an integral domain, but it is much more important.

Def. R ring

A subset $S \subset R$ is multiplicative if $1 \in S$ and $(s_1, s_2 \in S \Rightarrow s_1 s_2 \in S)$

Examples:

(1) Let $a \in R$. Then

$$S = \{ a^n \mid n \geq 0 \} \subset R$$

is a multiplicative set.

(2) Let $P \subset R$ be a prime ideal. Then $R - P$ (the complement of P) is a multiplicative set.

(3) In particular, if R is an integral domain, then $R - \{0\}$ is multiplicative.

(4) $R^\times$ is multiplicative.

(5) If $f: R_1 \longrightarrow R_2$ is a ring morphism and $S_1 \subset R_1$ is multiplicative

(resp. $S_2 \subset R_2$ is multiplicative) then $f(S_1) \subset R_2$ (resp. $f^{-1}(S_2) \subset R_1$) are multiplicative.

Fix now R and a multiplicative subset $S \subset R$. We will define a ring $S^{-1}R$ (in fact an R-algebra) so that the elements are roughly fractions $\frac{r}{s}$ where $s \in S$, $r \in R$.

In fact, we do it abstractly:

<u>Theorem.</u> Let $S \subset R$ be multiplicative.

There exists an R-algebra

$$R \xrightarrow{\varphi} S^{-1}R$$

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[dr, "f \circ \varphi"'] & S^{-1}R \arrow[d, "f"] \\ & A \end{tikzcd}$$

such that there is, for any R-algebra A, a bijection

$$\mathrm{Hom}_{(R\text{-alg})}(S^{-1}R, A) \xrightarrow{\sim} \left\{ g \in \mathrm{Hom}_{(R\text{-alg})}(R, A) \;\middle|\; g(S) \subset A^\times \right\}$$

$$f \longmapsto f \circ \varphi$$

(Intuitively, if $f(S) \subset A^\times$, we can "extend" f to fractions by $f\left(\frac{r}{s}\right) = \frac{f(r)}{f(s)}$).

$f(s)$ is invertible in A

<u>Proof.</u> We give an explicit construction, because it is sometimes useful, but <u>in principle</u> one should try to only use the property of the theorem, which characterizes $S^{-1}R$ up to iso-morphism.

Start with the <u>set</u>

$$X = R \times S$$

and define

(1) A relation $\sim$ on X by

$$(r_1, s_1) \sim (r_2, s_2) \iff \left(\exists\, t \in S,\ t(r_1 s_2 - r_2 s_1) = 0\right)$$

(2) Maps

$$\tilde{\varphi} : R \longrightarrow X$$
$$r \longmapsto (r, 1)$$

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}$$

$$\tilde{+} : X \times X \longrightarrow X$$
$$((r_1, s_1), (r_2, s_2)) \longmapsto (r_1 s_2 + r_2 s_1, s_1 s_2)$$

$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}$$

$$\tilde{\cdot} : \quad X \times X \longrightarrow X$$
$$((r_1, s_1), (r_2, s_2)) \longmapsto (r_1 r_2, s_1 s_2)$$

<u>Then:</u> (i) $\sim$ is an equivalence relation

(ii) $\tilde{\varphi}$, $\tilde{+}$ and $\tilde{\cdot}$ are compatible with $\sim$ and define

$$\varphi : R \longrightarrow X/_\sim \; ; \; +, \cdot : X/_\sim \times X/_\sim \longrightarrow X/_\sim$$

s.t. $X/_\sim$ becomes an R-algebra with the desired properties.

The proof of (i) is where the precise definition of the relation plays a role.

- (<u>Symmetry</u>) $(r,s) \sim (r,s)$ since

$$1 \cdot (rs - sr) = 0$$

- (<u>Reflexivity</u>) $(r_1, s_1) \sim (r_2, s_2) \iff (r_2, s_2) \sim (r_1, s_1)$ is clear

- (<u>Transitivity</u>) Suppose

$$(r_1, s_1) \sim (r_2, s_2) \text{ and } (r_2, s_2) \sim (r_3, s_3).$$

Pick t_1, t_2 s.t

$$t_1(r_1 s_2 - r_2 s_1) = t_2(r_2 s_3 - r_3 s_2) = 0$$

Then

$$(t_1 t_2 s_2) r_1 s_3 = t_2 t_1 r_2 s_1 s_3$$
$$= t_2 r_3 s_2 t_1 s_1$$
$$= (t_1 t_2 s_2) r_3 s_1$$

$\in S$

shows that $(r_1, s_1) \sim (r_3, s_3)$.

(ii) The compatibility is easy

[Ex. if $(r_1, s_1) \sim (r_2, s_2)$

then $(r_1, s_1) \tilde{+} (r_3, s_3) = (r_1 s_3 + r_3 s_1, s_1 s_3)$

$(r_2, s_2) \tilde{+} (r_3, s_3) = (r_2 s_3 + r_3 s_2, s_2 s_3)$

Let t be such that

$$t(r_1 s_2 - r_2 s_1) = 0.$$

Then

$$t\left((r_1 s_3 + r_3 s_1) s_2 s_3 - (r_2 s_3 + r_3 s_2) s_1 s_3\right)$$
$$= t r_2 s_1 s_3^2 + t r_3 s_1 s_2 s_3 - t r_2 s_1 s_3^2 - t r_3 s_1 s_2 s_3$$
$$= 0. \quad]$$

and so is the fact that we get a ring (Note that X itself is <u>not</u> a ring) with

$$0 = \text{class of } (0,1)$$

$$1 = \text{———} \ (1,1)$$

$$-(\text{class of } (r,s)) = \text{———} \ (-r,s)$$

$$= \text{———} \ (r,-s)$$

This being given, note that

$$\varphi(S) \subset (S^{-1}R)^{\times}$$

since
$$[(s,1)]\cdot[(1,s)] = [(s,s)]$$
$$= 1 \qquad [1\cdot(1\cdot s - s\cdot 1) = 0]$$

So the map (of sets)

$$(*)\ \begin{cases} \mathrm{Hom}_{(R\text{-alg})}(S^{-1}R, A) \longrightarrow \mathrm{Hom}_{(R\text{-alg})}(R, A) \\ \qquad f \longmapsto f\circ\varphi \end{cases}$$

$$\begin{tikzcd} S^{-1}R \arrow[r, "f"] & A \\ R \arrow[u, "\varphi"] \arrow[ur] & \end{tikzcd}$$

has the property that

$$(f\circ\varphi)(S) \subset f((S^{-1}R)^{\times})$$
$$\subset A^{\times},$$

and it remains to check that it is bijective.

We construct the inverse: given $g : R \longrightarrow A$ with $g(R) \subset A^\times$, we define

$$\tilde{f} : X \longrightarrow A$$
$$(r,s) \longmapsto g(r)\, g(s)^{-1}$$

and see that it is compatible with $\sim$ (if $(r_1,s_1) \sim (r_2,s_2)$, with $t(r_1 s_2 - r_2 s_1) = 0$, then $g(t)\big(g(r_1)\, g(s_2) - g(r_2)\, g(s_1)\big) = 0$.

and since $g(t)$, $g(s_1)$, $g(s_2)$ are invertible this gives $g(r_1)\, g(s_1)^{-1} = g(r_2)\, g(s_2)^{-1}$)

so we have an induced

$$f : X/_\sim \longrightarrow A$$
$$\frac{r}{s} \longmapsto \frac{g(r)}{g(s)}$$

which one checks is a ring morphism. This defines $g \longmapsto f$, inverse of $(*)$

[Indeed, start with g, then $f \circ \varphi(r) = f\left(\frac{r}{1}\right) = f(r)$; start with f, then let $g = f \circ \varphi$; the

associated $\tilde{f}$ is $(r,s) \longmapsto \dfrac{g(r)}{g(s)} = \dfrac{f(r)}{1} \cdot \left(\dfrac{f(s)}{f(1)}\right)^{-1}$
$= \dfrac{f(r)}{f(s)} = f\left(\dfrac{r}{s}\right)$

This concludes the proof

$\square$

<u>Notation</u>: (1) if $a \in R$ then
$$(\{a^n \mid n \geq 0\})^{-1} R = R_a$$
(2) if $P \subset R$ is prime then
$$(R - P)^{-1} R = R_P$$
(Hopefully without creating confusion...)

<u>Examples</u> (1) Suppose R is an integral domain. Then the structure morphism
$$\varphi : R \longrightarrow S^{-1} R$$
is <u>injective</u> unless $0 \in S$, and $S^{-1}R$ is also a <u>subring</u> of the fraction field
$$\mathrm{Frac}(R) = (R - \{0\})^{-1} R$$
(Indeed more generally, we have

$\ker(\varphi : R \longrightarrow S^{-1}R) = \{ r \in R \mid \frac{r}{1} = 0 = \frac{0}{1} \}$

$= \{ r \in R \mid \exists t \in S,\ t.r = 0 \}$

so : (1) $\varphi = 0$ if $0 \in S$

(2) φ is injective $\iff$ S contains no zero divisor]

(2) $\mathbb{Z}_2$ "=" $\mathbb{Z}[\frac{1}{2}]$" $= \{ \frac{a}{b} \in \mathbb{Q} \mid (a,b) = 1$ and b is a power of $2 \}$

Similarly e.g. for $\mathbb{Z}_{10} = \{ \frac{a}{10^n} \mid a \in \mathbb{Z} \}$

(decimals with finitely many digits)

(3) $\mathbb{Z}_{2\mathbb{Z}} = \{ \frac{a}{b} \in \mathbb{Q} \mid (a,b) = 1,\ 2 \nmid b \}$

= rationals with odd denominator

[ACL 2.2.7]

Proposition - Let $S \subset R$ be multiplicative.

There is a bijection, preserving inclusion

$\{ Q \subset S^{-1}R$ prime ideal$\}$

$\longrightarrow \{ P \subset R$ prime ideal s.t. $P \cap S = \emptyset \}$.

given by $Q \longmapsto \varphi^{-1}(Q)$ where
$$\varphi : R \longrightarrow S^{-1}R$$
is the structure morphism.

Note: if R is an integral domain and we identify $S^{-1}R$ with a subring of $\mathrm{Frac}(R)$, then the map above is simply $P \longmapsto P \cap R$.

Proof. We know that $\varphi^{-1}(P)$ is prime. It must satisfy $\varphi^{-1}(P) \cap S = \emptyset$ since otherwise there is $s \in S$ s.t. $\varphi(s) \in P$, which is impossible since $\varphi(s)$ is invertible and $P \neq R$. (Recall: an ideal is equal to R if it contains a unit).

We define a reciprocal bijection to prove that we have a bijection.

Let $P \subset R$ satisfy $P \cap S = \emptyset$.

Then consider $Q \subset S^{-1}R$, the ideal generated by $\varphi(P)$. This is the set of $\frac{r}{s} \in S^{-1}R$ with $r \in P$ (because $\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}$ has this form if $r_i \in P$)

We have $\underline{\varphi^{-1}(Q) = P}$: indeed, $P \subset \varphi^{-1}(Q)$ is clear $[\varphi(P) \subset Q]$ and conversely if $r \in \varphi^{-1}(Q)$ we have

$$\frac{r}{1} = \frac{r_1}{s_1}, \quad r_1 \in P,\ s_1 \in S$$

so $t(rs_1 - r_1) = 0$ for some $t \in S$.

Thus $trs_1 \in P$, and $r \in P$ because $ts_1 \notin P$ (here we need to know that P is prime!)

To check that Q is prime, suppose

$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} \in Q, \quad \text{i.e.} \quad \frac{r_1}{s_1} \frac{r_2}{s_2} = \frac{r}{s}$$

with $r \in P$

Find $t \in S$ with $t(r_1 r_2 s - r s_1 s_2) = 0$.

So $t s_{} r_1 r_2 = t s_1 s_2 r \in P$, so

$r_1 r_2 \in P$, $\notin P$ hence either r_1 or r_2 is in

P. Moreover $1 \notin Q$, since $1 \in Q$ would imply

$1_R \in \varphi^{-1}(Q) = P$, which is not the case.

Finally we need to check that these two maps are inverse bijections:

(1) If we start from P, define Q, then $\varphi^{-1}(Q) = P$, as we just saw.

(2) If we start with $Q \subset S^{-1}R$ prime, define $P = \varphi^{-1}(Q)$, then P is prime. Let Q_1 be the ideal generated by $\varphi(P)$; since $\varphi(P) \subset Q$, we get $Q_1 \subset Q$. Conversely, let $\frac{r}{s} \in Q$. Then $s \cdot \frac{r}{s} = \frac{r}{1} \in Q$ so $r \in \varphi^{-1}(Q) = P$, and $\frac{r}{s} = \frac{1}{s} \cdot \frac{r}{1}$ belongs to Q_1.

$\square$

Examples

(1) We consider the localization R_a for some element $a \in R$. By the proposition we get a bijection

$$\{\text{prime ideals in } R_a\} \xrightarrow{\sim} \{\text{prime ideals } \mathfrak{p} \text{ in } R \text{ s.t. } a \notin \mathfrak{p}\}$$

(indeed, a priori the right-hand side should be

$$\{\text{prime ideals } \mathfrak{p} \subset R \text{ s.t. } \{a^n \mid n \geq 0\} \cap \mathfrak{p} = \emptyset\}$$

but for a prime ideal $\mathfrak{p}$, the condition is equivalent to $a \notin \mathfrak{p}$ (since $a^n \in \mathfrak{p}$ would imply it).

In practical terms, this means that we can view the set of prime ideals such that $a \notin \mathfrak{p}$ as the set of all prime ideals in some ring (namely R_a). This can be very useful.

Let us illustrate this:

<u>Prop.</u> – Let R be a ring. Then

$$\underbrace{\{\text{nilpotent elements of } R\}}_{\text{the "nilradical" of } R} = \bigcap_{\substack{\mathfrak{p} \subset R \\ \text{prime}}} \mathfrak{p}.$$

<u>Proof.</u> If $x \in R$ is nilpotent, then $(\exists n, \; x^n = 0 \in \mathfrak{p}) \Rightarrow x \in \mathfrak{p}$ for all prime ideals $\mathfrak{p}$, so "$\subset$" is true.

Conversely, we must show that if x is <u>not</u> nilpotent, then there is a prime ideal $\mathfrak{p}$ s.t. $x \notin \mathfrak{p}$. But this means that we must find a prime ideal $\mathfrak{q} \subset R_x$. This exists since the condition that x is not nilpotent ensures that the ring R_x is non-zero, so has some prime ideal.

$\square$

Note. The map

$$\{\text{prime ideals in } S^{-1}R\} \longrightarrow \{\text{prime ideals not intersecting } S\}$$

does not respect maximal ideals. For instance if R is an integral domain, then for $R \hookrightarrow \mathrm{Frac}(R) = (R-\{0\})^{-1}R$ the maximal ideal $\{0\} \subset \mathrm{Frac}(R)$ corresponds to the prime ideal $\{0\} \subset R$, which is not always maximal.

(2) Let $q \subset R$ be a prime ideal. With $S = R - q$, we get a bijection

$$\{\text{primes in } R_q = S^{-1}R\} \xrightarrow{\sim} \{\text{primes } p \subset R \text{ s.t. } p \cap S = \emptyset\}$$

Here $p \cap S = p \cap (R - q)$

so $(p \cap S = \emptyset) \iff (p \subset q)$

So the prime ideals of the localization

at q "are" the prime ideals contained in q. This is "complementary" to the case of R/q, whose prime ideals "are" the prime ideals containing q.

We very often use these to restrict attention to these subsets of prime ideals. This is actually the origin of the word "localization". Indeed, note that in R_q, there is a unique maximal ideal, which is the prime ideal corresponding to q; all prime ideals of R_q are contained in this ideal.

Def. (local ring)

A local ring R is a ring such that R contains a unique maximal ideal m. The field R/m is called the residue field

Examples are fields ($m_R = \{0\}$) and localizations R_q at (complements of) prime ideals.

Note. Why "local"? There is a good geometric reason, which can be illustrated by the following example:

Let $R = \{ (a_n)_{n \geq 0} \mid a_n \in \mathbb{C}$ and $\sum_{n \geq 0} a_n z^n$ has > 0 radius of convergence$\}$.

This is a ring with addition/multiplication of power series. Intuitively, this is the ring to use to study "local" properties of holomorphic functions around 0.

Fact: R is a local ring with maximal ideal $m_R = \{ (a_n)_{n \geq 0} \mid a_0 = 0 \}$.

Indeed:

(i) m_R is maximal because

$$m_R = \ker \left(\begin{array}{ccc} R & \longrightarrow & \mathbb{C} \\ (a_n) & \longmapsto & a_0 \end{array} \right)$$

(which is surjective).

(ii) if $(a_n) \notin m_R$ then (a_n) is <u>invertible</u> in R, so any ideal $I \subset R$ is either contained in m_R, <u>or</u> equal to R [indeed, let $f(z) = \sum_{n \geq 0} a_n z^n$; if $a_0 = f(0) \neq 0$, then $1/f$ is holomorphic in a neighborhood of 0, and writing

$$\frac{1}{f(z)} = \sum_{n \geq 0} b_n z^n$$

we get $(a_n)^{-1} = (b_n)$.]

4 - Nakayama's Lemma

We discuss here briefly a basic property of local rings, since it would not fit very well in the next chapter.

Definition. R ring.

The *nilpotent radical* of R is the set of nilpotent elements, or equivalently the intersection of all prime ideals of R.

The *Jacobson radical* of R is the intersection of all *maximal ideals* of R.

Example. R local ring, $m \subset R$ the max. ideal

The nilpotent radical can be complicated; it is $\{0\}$ if R is an integral domain.

The Jacobson radical is m_R.

Prop. (ACL, 2.1.6) R ring, $J \subset R$ Jacobson radical. We have

$$J = \{x \in R \mid 1 - xy \in R^\times \text{ for all } y \in R\}$$

Proof. Let J' be the right-hand side.

(1) $J' \subset J$: indeed if $x \in J'$ and

$m \subset R$ is maximal then we cannot have $x \notin m$ since this would imply that the ideal generated by m and x is R, so

$$\exists y \in R, \exists z \in m, \quad 1 = z + xy$$

hence $z \in m \cap R^\times$, impossible.

(2) $\underline{J \subset J'}$: suppose $x \notin J'$; then there exists $y \in R$ s.t. $1 + xy \notin R^\times$, hence there exists a maximal ideal m s.t. $1 + xy \in m$. We then have $x \notin m$ (so $x \notin J$), since again otherwise $1 \in m$.

□

<u>Remark</u> - If R is a local ring, we also have the useful alternative description

$$m_R = R - R^\times \quad , \text{ or } \quad R^\times = R - m_R .$$

(Indeed, if $x \notin m_R$, then the ideal it generates is not contained in m_R, so must be R, so x is a unit).

Proposition (Nakayama's Lemma) [ACL 6.1.1]

Let R be a ring, M a finitely generated R-module. Let $J \subset R$ be the Jacobson radical. If (and only if)

$$JM = M$$

submodule of M generated by rm, $r \in J$, $m \in M$

then $M = \{0\}$.

Proof. We use induction on the minimal number $n \geq 0$ of generators of M.

If $n = 0$, $M = \{0\}$.

Suppose $n \geq 1$; let $e_1, \dots, e_n$ be a generating set of M. Consider then

$$N = M / Re_1$$

so that N is finitely generated by the $n-1$ elements $\bar{e}_2, \dots, \bar{e}_n$, the classes of e_i modulo e_1. We still have

$$N = JN,$$

so by induction we deduce that $N = \{0\}$, so that $M = Re_1$. Then from $M = JM$ we see that there exists $x \in J$ s.t.

$$e_1 = x e_1$$
$$\Updownarrow$$
$$(1 - x) e_1 = 0$$

Since $1 - x \in R^\times$ (by the characterization of J above!) we conclude $e_1 = 0$ so $M = \{0\}$.

$\square$

<u>Corollary</u> - (R, m_R) local ring

M finitely generated R-module.

(1) $M = \{0\} \iff M/_{m_R M} = \{0\}$

(2) A family $(e_1, \ldots, e_m)$ generates M $\iff (\overline{e_1}, \ldots, \overline{e_m})$ generate $M/_{m_R M}$

Proof. The point is that m_R is the Jacobson radical.

(1) If $M/_{m_R M} = \{0\}$ then $M = m_R M$ so $M = \{0\}$ by Nakayama.

(2) Suppose $(\overline{e_1}, \_\_, \overline{e_m})$ generate $M/_{m_R M}$ (as R-module, or equivalently $R/_{m_R}$-vector space)

Let $N = \langle e_1, \_\_, e_m \rangle \subset M$. Then

$$M/_N = m_R (M/_N)$$

(since for $m \in M$ there is $n \in N$ s.t.

$$n - m \in m_R M)$$

hence $M/_N = \{0\}$ by Nakayama.

$\square$

Remark. This complements the previous remark that if R is a local ring, then $R^\times = R - m_R$.

Fact: if R is a ring and $I \subset R$ an ideal such that $R^\times = R - I$, then

(i) I is maximal

(ii) R is local [with maximal ideal I]

Indeed, if $J \supset I$ is an ideal and $J \neq I$, we can find some $x \in J \cap (R - I)$
$= J \cap R^\times$
so that $J = R$: this proves (i).

And if $J \subset R$ is <u>any</u> ideal and $J \neq R$, we must have

$$\begin{array}{c} J \cap R^\times = \emptyset \\ \parallel \\ J \cap (R - I) \end{array}$$

so that $J \subset I$. This means that I is the <u>only</u> maximal ideal in R.