Part I. Commutative algebra.

Theorem 1.1. There is a one-to-one correspondence {ideals in A/I} $\leftrightarrow$ {ideals in A containing I}.
Proof. Let $\phi : A \to A/I$ be the projection (residue) map. Set-theoretic image and inverse image send ideals to ideals. For arbitrary ideal $J \subset A$ $\phi^{-1}(\phi(J)) =< J, I >$ (which equals J if $I \subset J$) and for $K \subset A/I$ $\phi(\phi^{-1}(K)) = K$ and $I \subset \phi^{-1}(K)$ hence the theorem.

Since for $I \subset J \subset A$ $(A/I)/(\phi(J) = A/J$ canonically (cf. isomorphism theorem for groups) prime ideals correspond to prime ones and maximal ideals correspond to maximal ones. If J is principal then of course $\phi(J)$ is principal but the opposite needs not to be true (say, $I = \phi^{-1}((0))$ is not necessary principal while (0) is).

Remark. The kernel of any ring homomorphism $\phi : A \to B$ is an ideal and the image $\phi(A)$ is isomorphic to $A/\ker(\phi)$. The situation differs from that in group theory since the kernel is an object of different nature (not a ring). In particular the category of (commutative with identity) rings is not abelian.

Operations over ideals. Let $I, J \subset A$ be ideals. Then $I \cap J$ is an ideal. $I+J \stackrel{\text{def}}{=} < I, J >$, this is the smallest ideal containing both I and J. It is easy to see that any $z \in I+J$ could be represented in the form $z = x + y, x \in I, y \in J$ (by definition $z = \sum a_n x_n + \sum b_m y_m$ where $a_n, b_m \in A, x_n \in I, y_m \in J$, then the first sum is in I while the second is in J. Finally, $IJ \stackrel{\text{def}}{=} < \{xy, x \in I, y \in J\} >$. As opposite to the $I + J$ case not all elements of IJ are of the form xy, one also needs linear combinations. Clearly $IJ \subset I \cup J$ but the two need not to coincide.

Definition. $S \subset A$ is multiplicative iff it contains 1 and $a, b \in S \Rightarrow ab \in S$.

For example, if $I \subset A$ is an ideal then $S = \{1+x, x \in I\})$ is multiplicative. There are two most important examples of multiplicative sets. For $h \in A$ let $S_h = \{1, h, h^2, \dots\}$. For prime ideal $\mathfrak{p} \subset A$ let $S_{\mathfrak{p}} = A \setminus \mathfrak{p}$. The last definition could be extended to an arbitrary union (which generally is itself not an ideal) of prime ideals $(A \setminus \cup \mathfrak{p}_\alpha)$.

Definition. $S^{-1}A$ = (set of fractions $\frac{a}{s}, a \in A, s \in S$) quotient by the equivalence relation $\frac{a}{s} \sim \frac{b}{t}$ iff $\exists u \in S$ such that $u(at - bs) = 0$.

The natural map $i_S : A \to S^{-1}A$ sends a to $\frac{a}{1}$. $\ker i_S$ consists of $a \in A$ such that $\exists s \in S$, $sa = 0$. So i_S is always injective if A is an ID. It may happen that A is not an

ID while i_S is still injective. For example, if $S = \{1\}$ then i_S is an identity map. More general, if S contains no zero divisors then i_S is injective. As opposite, if $0 \in S$ then $S^{-1}A$ is a zero ring.

If $S_1 \subset S_2$ then two S_1-equivalent fractions are also S_2-equivalent hence the natural homomorphism $S_1^{-1}A \to S_2^{-1}A$ is defined. If A is an ID and $0 \notin S_2$ then all such homomorphisms are injective since the equivalence relation in the definition above does not depend on S, only the set of fractions does. One may consider the maximal possible S (which consists of all nonzero elements of A). This is $S_{(0)}$ via the notation above. All $S^{-1}A$ for various S become subrings of $A_{(0)} \stackrel{\text{def}}{=} S_{(0)}^{-1}A$ which clearly is a field and is called the the field of fractions. For $S_1 \subset S_2$ one has $S_1^{-1}A \subset S_2^{-1}A$. It is useful to point out that $\mathfrak{p}_1 \subset \mathfrak{p}_2$ leads to $S_{\mathfrak{p}_1} \supset S_{\mathfrak{p}_2}$ hence $A_{\mathfrak{p}_1} \supset A_{\mathfrak{p}_2}$.

If $\mathfrak{p}$ is a prime ideal then attaching $S_{\mathfrak{p}}^{-1}A \stackrel{\text{def}}{=} A_{\mathfrak{p}}$ to A is called localisation near $\mathfrak{p}$. The name is justified since $A_{\mathfrak{p}}$ is always a local ring (one calls the ring local iff it contains the unique maximal ideal). In fact, the set $\mathfrak{p}A_p$ of elements in $A_{\mathfrak{p}}$ representable by the fraction $\frac{x}{y}$ where $x \in \mathfrak{p}$ and $y \notin \mathfrak{p}$ is clearly an ideal. All the elements of $A_{\mathfrak{p}}$ outside this set are invertible hence the ideal is maximal. A proper ideal in $A_{\mathfrak{p}}$ may not contain invertible elements hence may not intersect with $A_{\mathfrak{p}} \setminus \mathfrak{p}A_{\mathfrak{p}}$ hence is contained in $\mathfrak{p}A_{\mathfrak{p}}$.

If $h \in A$ is nilpotent then $S_h^{-1}A = 0$, if h is invertible then $S_h^{-1}A = A$. Generally, there is an isomorphism $\phi : A[T]/((1 - hT)) \stackrel{\sim}{\to} A_h$ ($T \mapsto \frac{1}{h}$). So the "task" of A_h is to make h invertible. The proof is an exercise using the next theorem.

Theorem 1.2. The pair $(S^{-1}A, i_S)$ is universal with respect to the property that $\forall s \in S$ the image $i_S(s)$ is invertible. Precisely this means that for any homomorphism $\phi : A \to B$ such that $\phi(S)$ consists of invertible elements there exists a unique homomorphism $\psi : S^{-1}A \to B$ such that $\phi = \psi \circ i_S$. The pair $(S^{-1}A, i_S)$ is defined by this property up to a unique isomorphism.
Proof. Exercise.

Next statement needs the Zorn Lemma (one may be avoided if A admits certain finiteness property which does often hold).

Theorem 1.3. Let $S \subset A$ be any subset, $I \subset A$ an ideal such that $I \cap S = \emptyset$. Consider all ideals $J \supset I$ such that $J \cap S = \emptyset$. Then there exists some ideal $M \subset A$ which is maximal with respect to this property (this means that $\forall x \notin M \;\; M + (x) \cap S \neq \emptyset$). If S

is multiplicative then M is prime.

Proof. The set of ideals J above is nonempty (it contains I), partially ordered by inclusion and for any chain $J_1 \subset J_2 \subset \dots$ the union $\cup J_i$ is clearly an ideal enjoying the same properties and may serve as an upper bound. By the Zorn Lemma some M does therefore exist. Suppose now S is multiplicative. Let $x, y \notin M$. Then $\exists s_1, s_2 \in S$, $a_1, a_2 \in A$ and $m_1, m_2 \in M$ such that $s_1 = m_1 + a_1 x$ and $s_2 = m_2 + a_2 y$. This means that $st \in M + (xy)$ hence $xy \notin M$.

Taking $S = \{1\}$ one may conclude that any proper ideal I is contained in some maximal ideal.

How do ideals behave under homomorphisms?

Let $\phi : A \to B$ be a homomorphism . If $I \subset A$ is an ideal then $\phi(I) \subset B$ needs not to be an ideal. If $b \notin \phi(A)$ then it may happen that $b\phi(I) \not\subset \phi(I)$. If ϕ is surjective this never happens since $\forall b \;\; b\phi(I) = \phi(aI) \subset \phi(I)$ where $a \in A$ is some preimage of b. Generally to get an ideal in B one needs to consider $B\phi(I) =< \phi(I) >$ - the ideal in B generated by the set $\phi(I)$. The notation is $\phi_*(I)$ or I^e. I^e is considered an "extention" of I with respect to ϕ.

Now let $J \in B$ be an ideal. It is easy to see that $\phi^{-1}(J)$ is an ideal in A, another notation is J^c, the "contraction" of J with respect to ϕ. If ϕ is injective then one may identify J^c with $J \cap \phi(A)$ via ϕ.

What happens if one applies extension after contraction or vice versa?

Set-theoretically suppose $A, B, I \subset A, J \subset B$ are sets, $A \xrightarrow{\phi} B$ a map. Then $\phi^{-1}\phi(I) \supset I$. If ϕ is injective then the equality holds. Accordingly, $\phi\phi^{-1}(J) \subset J$, if ϕ is surjective then the equality holds. The inclusions above still hold for ideals if one replaces ϕ by extension and ϕ^{-1} by contraction. If ϕ is surjective then extension coincides with taking image hence in the second case the equality holds. As opposite the injectivity of ϕ is generally not enough for the equality to hold in the first case.

Example ($I \neq I^{ec}$). Consider $i_S : A \to S^{-1}A$. Let I be a proper ideal in A such that $I \cap S \neq \emptyset$ (in the $A_\mathfrak{p}$ case this means that $I \not\subset \mathfrak{p}$). Such ideal always does exist provided S contains elements other than units. Then I^e contains an invertible element hence $I^e = (1)$ thus $I^{ec} = (1)$.

If $A \stackrel{\phi}{\to} A/K$ then $I^{ec} = I + K$ which certainly needs not to coincide with I.

Example ($J \neq J^{ce}$). This one is more tricky since in both cases above the equality holds. In fact, let $\frac{a}{s} \in J$. Then $\frac{a}{1} = \frac{a}{s}\frac{s}{1} \in J \Rightarrow a \in J^c \Rightarrow \frac{a}{s} = \frac{1}{s}\frac{a}{1} \in < i_S(J^c) >= J^{ce}$. Also in the A/K case $J^{ce} = J$ thanks to surjectivity. Nevertheless one may consider $A = k[X] \stackrel{\phi}{\to} k[X,Y] = B$ of polynomial rings over the field k. Let $J = (X + Y) \subset B$ then $J^c = (0)$ as well as J^{ce}.

Theorem 1.4.
1.$I^{ece} = I^e$. $J^{cec} = J^c$.
2. Let $C \stackrel{\text{def}}{=}$ (set of ideals of A of the form J^c), $E \stackrel{\text{def}}{=}$ (set of ideals of B of the form I^e). Then $I \in C \Leftrightarrow I^{ec} = I$, $J \in E \Leftrightarrow J = J^{ce}$ and there is a one-to-one corespondence $C \leftrightarrows E$ given by the mutually inverse maps of extension and contraction.
3.

$(I_1 + I_2)^e = (I_1^e + I_2^e)$	$(J_1 + J_2)^c \supset (J_1^c + J_2^c)$
$(I_1 I_2)^e = (I_1^e I_2^e)$	$(J_1 J_2)^c \supset (J_1^c J_2^c)$
$(I_1 \cap I_2)^e \subset (I_1^e \cap I_2^e)$	$(J_1 \cap J_2)^c = (J_1^c \cap J_2^c)$

4. If $\mathfrak{P} \subset B$ is prime then $\mathfrak{p} = \mathfrak{P}^c \subset A$ is also prime.

Proof. Exercise.

Remark 1. If $\mathfrak{M} \subset B$ is maximal then its contraction $\mathfrak{M}^c \subset A$ needs not to be maximal. For example let $\mathfrak{M} = \mathfrak{p}A_{\mathfrak{p}} = \mathfrak{p}^e$ be the unique maximal ideal of the localisation of A near the prime ideal $\mathfrak{p}$. Then $\mathfrak{M}^c = \mathfrak{p} \subset A$ which needs not to be maximal.

Remark 2. If $I \subset A$ is prime then $I^e \subset B$ needs not to be prime. In fact, suppose that A is an ID while $K \subset A$ is not prime. Then $(0) \subset A$ is prime while $(0)^e = (0) \subset A/K$ is not. For more interesting example consider a finite extension of fields $F/\mathbf{Q}$. Let $A = \mathbf{Z}, B = \mathcal{O}_F$ the ring of integers in F, $p \in \mathbf{Z}$ a prime number. Then the theory of Dedekind rings gives a formula $((p) \subset \mathbf{Z})^e = \Pi \mathfrak{P}_i^{e_i}$ where $\mathfrak{P}^i$ are different prime ideals in $\mathcal{O}_F$. Calculation of the type of this decomposition is the key algebraic number theory problem.

Remark 3. Neither extension nor contraction needs to be injective on the full set of ideals $I \subset A$ (resp. $J \subset B$) besides they define a bijection between subsets C and E. So for $I \in C$ not only $I = (I^e)^c$ but there may exist other ideals $J \subset B$ such that $I = J^c$. Same for $J \in E$. Consider for example a prime ideal $I = \mathfrak{p} \in C$. Then $\mathfrak{p}^e$ needs not

to be prime. But there always exists some prime ideal $\mathfrak{P} \subset B$ (which may belong to E thus coinciding with $\mathfrak{p}^e$ or not) such that $\mathfrak{p} = \mathfrak{P}^c$. Indeed, $\phi(S_\mathfrak{p} = A \setminus \mathfrak{p}) \subset B$ is clearly a multiplicative set. Moreover, $\phi(S_\mathfrak{p}) \cap \mathfrak{p}^e = \emptyset$ (if not then $\exists s \in S$ such that $\phi(s) \in \mathfrak{p}^e \Rightarrow s \in \phi^{-1}(\mathfrak{p}^e) = \mathfrak{p}^{ec} = \mathfrak{p}$ as $\mathfrak{p} \in C$ - contradiction). By Theorem 3 there exists some $\mathfrak{P} \subset B$ prime containing $\mathfrak{p}^e$ and disjoint from $\phi(S_\mathfrak{p})$ hence $\mathfrak{P}^c$ is disjoint from $S_\mathfrak{p} \Rightarrow \mathfrak{P}^c \subset \mathfrak{p}$. Also $\mathfrak{P} \supset \mathfrak{p}^e \Rightarrow \mathfrak{P}^c \supset \mathfrak{p}^{ec} \supset \mathfrak{p}$ so $\mathfrak{P}^c = \mathfrak{p}$.

Now we apply this to the particular cases.
$\phi : A \to A/K$.
C=(ideals $I \subset A$ such that $I \supset K$). E= (all ideals $J \subset A/K$). If $\mathfrak{p} \subset A$ is prime then generally $\mathfrak{p}^e$ needs not to be prime but if $\mathfrak{p} \in C$ then $\mathfrak{p}^e$ is also prime. Indeed, suppose that $(x \mod K)(y \mod K) \in (\mathfrak{p} \mod K)$. This means that $xy = p + k, p \in \mathfrak{p}, k \in K$. Since $\mathfrak{p} \supset K \quad p + k \in \mathfrak{p} \Rightarrow$ either $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

$i_S : A \to S^{-1}A$ (subcase $S = S_\mathfrak{p}, A = A_\mathfrak{p}, \mathfrak{p} \subset A$ prime). The following properties hold.
1) E= (all ideals $J \subset S^{-1}A$).
2) Define $(I_1 : I_2 \stackrel{\text{def}}{=} (x \in A$ such that $xI_2 \subset I_1)$. Clearly this is an ideal. Then $I^{ec} = \bigcup_{s \in S} (I : (s))$.
3) $C = (I \subset A$ such that no $s \in S$ divides zero in $A/I)$.
Subcase $A_\mathfrak{p}$: $C = (I$ with the property $xy \in I \Rightarrow$ both $x, y \in \mathfrak{p})$.
4) If $\mathfrak{q} \subset A$ is prime then $\mathfrak{q} \in C \Leftrightarrow \mathfrak{p} \cap S = \emptyset$. These ideals are in one-to-one correspondence with prime ideals $\mathfrak{Q} \subset E = S^{-1}A$.
Subcase $A_\mathfrak{p}$: suppose $\mathfrak{q} \in A$ is prime, then $\mathfrak{q} \in C \Leftrightarrow \mathfrak{q} \subset \mathfrak{p}$.
5) $(I_1 \cap I_2)^e = (I_1^e \cap I_2^e)$.

Proof. 1) See example before Theorem 1.4).
2) $x \in I^{ec} \Leftrightarrow \frac{x}{1} = \frac{a}{s}$ for some $a \in I, s \in S \Leftrightarrow (xs - a)t = 0$ for some $t \in s \Leftrightarrow x \in \bigcup_{s \in S} (I : (s))$ (for $\Rightarrow \quad st$ works, for $\Leftarrow \quad t = 1$ works).
3) $I \in C \Leftrightarrow I^{ec} \subset I$ (i.e. $I^{ec} = I$) $\Leftrightarrow (sx \in I$ for some $s \in S \Rightarrow x \in I) \Leftrightarrow$ no $s \in S$ is a zero divisor in A/I.
4) Let $\overline{S}$ be the image of S in $A/\mathfrak{q}$. Then $S^{-1}A/S^{-1}\mathfrak{q} = \overline{S}^{-1}(A/\mathfrak{q})$. The latter ring is either zero or is contained in the field of fractions of the integral domain $A/\mathfrak{q}$ thus is an ID itself. Hence $S^{-1}A/S^{-1}\mathfrak{q}$ is either zero (this happens iff $S \cap \mathfrak{q} \neq \emptyset$) or an ID in which case $S^{-1}\mathfrak{q} = \mathfrak{q}^e$ is prime.
5) Exercise.

Remark 1. $J^c = (1) \Leftrightarrow J = (1)$ for arbitrary $A \xrightarrow{\phi} B$ while $I^e = (1)$ holds iff $1 \in < \phi(I) >$. In the i_S particular case $I^e = (1) \Leftrightarrow I \cap S \neq \emptyset$ (see 2) above). In the $A_\mathfrak{p}$ subcase this means that $I \not\subset \mathfrak{p}$. If $\phi : A \to A/K$ then $I^e = (1) \Leftrightarrow 1 \in I + K$. If this is the case the ideals I and K are called relatively prime or coprime.
Remark 2. Suppose $\mathfrak{p} \subset A$ is prime. In the $A_\mathfrak{p}$ case prime ideals of $A_\mathfrak{p}$ are in one-to-one correspondence with prime ideals $\mathfrak{q} \in A$ such that $\mathfrak{q} \subset \mathfrak{p}$ (other prime ideals of A are killed by the extension map) while in the $A \to A/\mathfrak{p}$ case prime ideals of $A_\mathfrak{p}$ are in one-to-one correspondence with prime ideals $\mathfrak{q} \subset A$ such that $\mathfrak{q} \supset \mathfrak{p}$ (other prime ideals of A are not in the image of the contraction map).
Remark 3. Suppose $\mathfrak{p} \subset A$ and $\mathfrak{q} \subset A$ are both prime and $\mathfrak{p} \supset \mathfrak{q}$. Localise near $\mathfrak{p}$ and then take quotient by $\mathfrak{q}^e$ (the order may be opposite since under the condition $\mathfrak{p} \supset \mathfrak{q}$ the two operations commute). The set of prime ideals of the resulting ring $A_\mathfrak{p}/\mathfrak{q}^e$ will be in one-to-one correspondence with the set of prime ideals $\mathfrak{r} \subset A$ such that $\mathfrak{p} \supset \mathfrak{r} \supset \mathfrak{q}$. In particular when $\mathfrak{p} = \mathfrak{q}$ the ring $A_\mathfrak{p}/\mathfrak{p}^e$ contains just one prime ideal, namely (0), therefore is a field. This field coincides with the field of fractions of the ID $A/\mathfrak{p}$. It is called the residue field of the ideal $\mathfrak{p}$.

The coprime ideals satisfy the Chinese remainder theorem (attributed to Qin Jinshao (1208-1261).

Theorem 1.5.
Suppose the ideals $I_1, I_2, \ldots, I_n$ in A are pairwise coprime. Consider the ring homomorphism $\phi : A \to \prod A/I_i$ which sends $x \in A$ to $(x \mod I_1, \ldots, x \mod I_n)$. Then ϕ is surjective and $\ker(\phi) = \bigcap I_i = \prod I_i$.

Proof. $n = 2$. There exist $x \in I_1$ and $y \in I_2$ such that $x + y = 1$. Let $a_1 \in A, a_2 \in A$ be arbitrary. Then $\phi(xa_2 + ya_1) = (a_1 \mod I_1,\ a_2 \mod I_2)$ hence ϕ is surjective. Clearly $\ker(\phi) = I_1 \cap I_2$. If $c \in I_1 \cap I_2$ then $c = cx + cy \in I_1 I_2$.
$n > 2$. For each $i \geq 2$ choose $x_i \in I_1$ and $y_i \in I_i$ such that $x_i + y_i = 1$. Then $1 = \prod_{i \geq 2}(x_i + y_i) \in I_1 + \prod_{i=2}^{n} I_i$ hence I_1 and $\prod_{i=2}^{n} I_i$ are coprime. By the previous case $A/\prod_{i=1}^{n} I_i = A/I_1 \times A/\prod_{i=2}^{n} I_i$ and the induction works.

We still did not consider taking the union of the ideals. To get an ideal for sure out of $I_1 \cup I_2 \cup \cdots \cup I_n$ one needs to consider the sum $I_1 + I_2 + \cdots + I_n =< I_1 \cup I_2 \cup \cdots \cup I_n >$). The union itself is rarely an ideal.

Example. Suppose $I_1, I_2, \ldots, I_n$ are ideals in A, all but probably two of them being prime. Suppose $I \subset A$ is an ideal such that $I \subset I_1 \cup I_2 \cup \cdots \cup I_n$. Then $\exists i$ such that $I \subset I_i$.
Indeed, WLOG one may suppose that $I_i \not\subset I_j$ for $i \neq j$. Suppose first that $n = 2$. If I is not a subset of either individual I_i then it is possible to choose $x, y \in I$ such that $x \in I_1 \setminus I_2,\ y \in I_2 \setminus I_1$. Then $I \ni x + y \notin I_1 \cup I_2$.
Now suppose $n \geq 3$ and $I_n = \mathfrak{p}$ prime. Then $I \prod_1^{n-1} I_i \not\subset \mathfrak{p}$ since $I_i \not\subset \mathfrak{p}$ for $i < n$ and $I \not\subset \mathfrak{p}$ while $\mathfrak{p}$ is prime. Choose some $x \in I \prod_1^{n-1} I_i$ such that $x \notin \mathfrak{p}$. By induction $\exists y \in I$ such that $y \notin \bigcup_1^{n-1} I_i$. Clearly $x + y$ satsfies the same properties as y. Since $x \notin \mathfrak{p} \quad y$ and $x + y$ cannot both lie in $\mathfrak{p}$ hence $I \not\subset \bigcup_1^n I_i$.

Radicals.

Let $I \in A$ be an ideal. Its radical $\sqrt{I}$ consists of $h \in A$ such that $h^n \in I$ fore some $n \in \mathbf{Z}_{>0}$. Clearly $\sqrt{I}$ is an ideal (use the binomial formula) and $\sqrt{I} \supset I$. Also I is proper/trivial $\Leftrightarrow \sqrt{I}$ is proper/trivial.
The ideal $\sqrt{(0)}$ consists of all nilpotent elements of A and is called nilradical (we will use the notation $\mathfrak{R}(A)$).

Here are some properties of $\sqrt{I}$.

1)$\sqrt{\sqrt{I}} = \sqrt{I}$
2)$\sqrt{I_1 I_2} = \sqrt{I_1 \cap I_2} = \sqrt{I_1} \cap \sqrt{I_2}$.
3)$\sqrt{I_1 + I_2} = \sqrt{\sqrt{I_1} + \sqrt{I_2}}$.
4)If $p \subset A$ is prime then $\forall n \quad \sqrt{\mathfrak{p}^n} = \mathfrak{p}$.
5) $\sqrt{I_1} + \sqrt{I_2} = (1) \Leftrightarrow I_1 + I_2 = (1)$.
6)$\sqrt{J^c} = (\sqrt{J})^c$.

Let us prove, say, 3) (5) is an immediate consequence of it, others are obvious). $\subset$ clear, so consider $\supset$. Suppose $h^n \in \sqrt{I_1} + \sqrt{I_2}$. Then $h^n = g + k, g^l \in I_1,\ k^m \in I_2$. Some power of h^n will then via binomial formula contain either $g^{\text{at least } l}$ or $k^{\text{at least } m}$ hence will sit in $I_1 + I_2$.

The ideal I is called radical iff $\sqrt{I} = I$. Any prime ideal is radical (but of course the opposite is not true). I_1, I_2 are radical$\Rightarrow I_1 \cap I_2$ is radical. Nevertheless the sum of radical ideals needs not to be radical.
Example. Let $A = k[X, Y]$, k a field of characteristic $\neq 2$. Let $I_1 = (X^2 + Y)$, $I_2 = (X^2 - Y)$. Then I_1 and I_2 are both prime hence radical, but $I_1 + I_2$ contains X^2 while it does not contain X.

Theorem 1.6. Suppose $I \in A$ is a proper ideal. Then $\sqrt{I} = \bigcap_{\mathfrak{p} \supset I \text{ prime}} \mathfrak{p}$.

Proof. $\subset$ Suppose $h^n \in I$, $\mathfrak{p} \supset I$ prime. Then $h^n \in \mathfrak{p} \Rightarrow h \in \mathfrak{p}$. $\supset$ Suppose $h \notin \sqrt{I}$. Let $S = (1, h, h^2, \dots)$. Then S is a multiplicative set and $S \cap I = \emptyset$. By Theorem 1.3 there exists a prime ideal $\mathfrak{p} \supset I$ disjoint from S, in particular $h \notin \mathfrak{p}$.

We now define the Jacobcon radical $\mathfrak{J}(I) \stackrel{\text{def}}{=} \bigcap_{\mathfrak{m} \supset I \text{ maximal}} \mathfrak{m}$. We call $\mathfrak{J}((0))$ the Jacobson radical of A and use the notation $\mathfrak{J}(A)$ which never causes a mix up. Clearly $\mathfrak{R}(A) \subset \mathfrak{J}(A)$. We call A Jacobson ring iff $\mathfrak{p} = \mathfrak{J}(\mathfrak{p})$ for all prime ideals $\mathfrak{p} \subset A$. Informally speaking a Jacobson ring contains enough maximal ideals. The famous Hilbert Nullstellensatz states that the ring of polynomials in several variables over the field is Jacobson. This allows to build a bridge between schemes and algebraic varieties.

Both the nilradical and the Jacobson radical are designed to describe "small" elements of the ring A in some way. Clearly nilpotents should be considered as "small". The theorem below shows that $\mathfrak{J}(A)$ also consists of "small" elements.

Theorem 1.7. $x \in \mathfrak{J}(A) \Leftrightarrow \forall a \in A \;\; 1 - ax$ is invertible.
Proof. $\Rightarrow$ If $1 - ax$ is not invertible then $\exists \mathfrak{m} \subset A$ maximal such that $1 - ax \in \mathfrak{m}$ hence $x \notin \mathfrak{m}$. $\Leftarrow$ If $x \notin \mathfrak{m}$ then $\mathfrak{m} + (x) = (1)$ as $\mathfrak{m}$ is maximal. This means that $\exists a \in A$ such that $1 - ax \in \mathfrak{m} \Rightarrow$ not invertible.

Remark. If $x \in \mathfrak{R}(A)$ (i.e. nilpotent) then $(1 - ax)^{-1}$ could be constructed explicitly. Namely the power series $1 + ax + (ax)^2 + \dots$ ends at some point thus defining the inverse.

Spectrum of the ring.

As a set, the spectrum $\operatorname{Spec} A$ of the ring A consists of points $[\mathfrak{p}]$, one for each prime ideal $\mathfrak{p} \subset A$. We often will use the notation $\operatorname{Spec} A = X$.

For any ideal $I \subset A$ define $V(I) \subset X \stackrel{\text{def}}{=} ([\mathfrak{p}]$ such that $\mathfrak{p} \supset I)$. One may extend the definition to arbitrary subsets $T \subset A:\ V(T) \stackrel{\text{def}}{=} V(< T >)$. The following properties hold:
$V((0)) = X;\ V((1)) = \emptyset;\ V(\sum I_\alpha) = \bigcap V(I_\alpha)$ for arbitrary set of indices α. $V(I \cap J) = V(IJ) = V(I) \cup V(J)$. Both equalities for $V(I \cap J)$ are immediate consequences of the definition of prime ideal, the rest is clear.

This means that $V(I)$ may be cosidered as a full set of closed subsets of X for the certain topology on X which is called Zariski topology (for Oscar Zariski (1899-1986), one of the leading algebraic geometers of the XXth century).

One may also define the base of open sets (which of course are all of the form $X \setminus V(I)$). Namely, let $h \in A$, then $X_h \stackrel{\text{def}}{=} X \setminus V((h))$. Clearly $V(I) = \bigcap\limits_{h \in I} V((h))$ for any ideal $I \subset A$ hence $X \setminus V(I) = \bigcup\limits_{h \in I} (X \setminus V((h)) = \bigcup\limits_{h \in I} X_h$.

More properties of $V(I)$.

1) $I \subset J \Rightarrow V(I) \supset \mathrm{V}(J)$ the opposite is not necessary true (see below).
2) $V(\sqrt{I}) = V(I)$.
3) $V(I) = \emptyset \Leftrightarrow I = (1)$. $V(I) = X \Leftrightarrow I \subset \mathfrak{R}(A)$.
4) (cf. 1)) $V(I) \supset V(J) \Rightarrow \sqrt{I} \subset \sqrt{J}$ (in particular, $I \subset \sqrt{J}$).
5) There exists a one-to one correspondence between two sets: (radical ideals $I \subset A) \leftrightarrows$ (closed subsets of X). The map to the right is given by $I \mapsto V(I)$. The map to the left is given by $Z \mapsto \mathrm{I}(Z) \stackrel{\text{def}}{=} \bigcap\limits_{[\mathfrak{p}] \in Z} \mathfrak{p}$. The latter definition could be extended to arbitrary (not necessary closed) subsets $W \in X$ by the same formula. Hopefully the map of sets $W \mapsto \mathrm{I}(W)$ will be not mixed with the ideal I
Proof. 1) follows from the definition; 2) If $\mathfrak{p} \subset A$ is prime then $\mathfrak{p} \supset I \Leftrightarrow \mathfrak{p} \supset \sqrt{I}$; 3) any proper ideal I is contained in some prime ideal, for the rest apply 2) to the zero ideal;
4) apply 2); 5) $\mathrm{I}(V(I)) = \sqrt{I}$ by Theorem 1.6. $V(\mathrm{I}(W)) = \overline{W}$ for general subset $W \subset X$ where $\overline{W} \stackrel{\text{def}}{=} \bigcup\limits_{W \subset Z \text{closed}} Z$ is the topological closure of W.

It is easy to conclude that spectra typically are far from being Hausdorff spaces. Indeed, suppose $[\mathfrak{p}] = z \in X$ is a point. Then after the proof of 5) above $\overline{z} = Z$ where $Z = ([\mathfrak{q}] \mid \mathfrak{q} \supset \mathfrak{p})$. Hence only the points corresponding to maximal ideals are closed so as

a rule Spec A is even not a T1-space. Moreover if A is an ID then the zero ideal is prime so all the points of $X = \text{Spec}\, A$ are contained in the closure of the point $[(0)]$, the latter being in this case named "the generic point" of X.

Remark. There exists a way to make a T1-space (but not T2 i.e Hausdorff) out of Spec A. Consider the subspace Spm $A \subset \text{Spec}\, A$ consisting of all closed (i.e corresponding to maximal ideals) points with the topology of subspace. We call it the maximal spectrum of A. Clearly Spm A is T1. The closed sets of Spm A are of the form $(\overline{[\mathfrak{m}]} \mid \mathfrak{m} \supset I$ and $\mathfrak{m}$ is maximal). If $\mathfrak{p}$ is not maximal then $[\mathfrak{p}]$ is not a point of Spm A but $\overline{[\mathfrak{p}]} \cap \text{Spm}\, A = (\mathfrak{m} \supset \mathfrak{p},\ , \mathfrak{m}$ maximal) is a closed subset.
Sometimes Spm A contains enough points to reflect the structure of A almost adequately. Say, if $A = k[T_1, \ldots, T_n]$ (k an algebraically closed field) then by Hilbert's Nullstellenzatz Spm $A = k^n$ (as sets) and the maximal spectra of qoutient rings correspond to algebraic subsets of k^n. If, say, $k = \mathbf{C}$, then the Zariski topology on k^n is very weak compared to the coordinate one (one needs Grothendieck topologies to establish better relationship) but it is enough to calculate the nontrivial invariants if one considers projective algebraic sets instead of affine ones.

Concerning the open sets we clearly have the properties:
1) $X_f \cup X_g = X_{fg}$.
2) $X_h = \emptyset \Leftrightarrow h \in \mathfrak{R}(A)$.
3) $X_h = X \Leftrightarrow h$ is invertible.
4) $X_f = X_g \Leftrightarrow \sqrt{(f)} = \sqrt{(g)}$.

All the properties above are obvious.

Theorem 1.8.
X (and hence any closed subset $Z \subset X$) is quasicompact. The open subset $U \subset X$ is quasicompact $\Leftrightarrow U = \bigcup X_{h_i}$ (a finite union).
Proof. We prove the second statement (the first then follows as $X = X_1$). Since the sets X_h constitute a base for the topology any U is a union of some collection of X_h's so $\Rightarrow$ follows. $\Leftarrow$ Suppose $X_h \subset \bigcup X_{h_\alpha} \Leftrightarrow V((h)) \supset \bigcap V(h_\alpha) = V(\sum((h_\alpha)) \Leftrightarrow h \in \sqrt{\sum((h_\alpha))} \Leftrightarrow$ $\exists\ m, h_1, \ldots, h_n \mid h^m = \sum_{i=1}^{n} a_i h_i \Rightarrow X_h \subset \bigcup X_{h_i}$. This proves the quasicompactness of a single X_h thus also of a finite union.

Irreducibility.

We first study disconnected spectra. A topological space X is called disconnected if $X = X_1 \cup X_2$ where $X_1 \cap X_2 = \emptyset$ and both X_1 and X_2 are open (and therefore closed). When $X = \operatorname{Spec} A$ is disconnected?

Theorem 1.9. There exists a one-to-one correspondence between the representations below:
1) $X = X_1 \cup \cdots \cup X_n$ disjoint open
2) $A = A_1 \times \cdots \times A_n$ where $A_i \subset A$ are the rings (with same ring operations as in A but with different identity therefore not subrings)
3) $1 = e_1 + \cdots + e_n$ where e_i are orthogonal idempotents (i.e $\forall\ i\ e_i^2 = e_i,\ \ \forall i \neq j\ e_i e_j = 0$).
Proof. We prove 2) $\leftrightarrows$ 3) and 3) $\leftrightarrows$ 1.
2) $\leftrightarrows$ 3) If $A = \prod A_i$ then define e_i to be the element with i-th coordinate 1, others 0. Conversely, if $e_i \in A$ are orthogonal idempotents then each ideal Ae_i is in fact a ring with e_i playing the role of identity. We call this ring A_i. The map $\pi_i : a \mapsto ae_i$ is a ring homomorphism $A \to A_i$. Its kernel I_i consists of the elements $a \in A$ such that $ae_i = 0$. Then the ideals I_i and I_j are relatively prime since $e_i \in I_j$ while $\sum_{r \neq i} e_r \in I_i$. By Chinese remainder theorem the map $A \to \prod A_i$ is surjective. Since $\sum e_i = 1$ its kernel is zero.
3) $\leftrightarrows$ 1) Suppose $\mathfrak{p} \subset A$ is a prime ideal, then $A/\mathfrak{p}$ is an ID. Since $(e_i \bmod \mathfrak{p})(e_j \bmod \mathfrak{p}) = 0$ for $i \neq j$ just one of e_i's is nonzero $\bmod \mathfrak{p}$. Hence X is a disjoint union of open subsets X_{e_i}. Conversely, start with the disjoint decomposition $X = X_1 \cup X_2$, both X_1 and X_2 being open and closed (the general case follows by induction). Let $X = V(I_1)$, $X_2 = V(I_2)$, then $I_1 + I_2 = (1)$ since X_1 is disjoint from X_2, and $I_1 \cap I_2 \subset \mathfrak{R}(A)$ since the union is the entire X. Choose $a \in I_1$ and $b \in I_2$ so that $a + b = 1$, then $ab \in \mathfrak{R}(A) \Rightarrow a^m b^m = 0$ for some m. No prime ideal $\mathfrak{p}$ may contain both a^m and b^m (otherwise it should contain both a and b which contradicts to $a + b = 1$). This means that $(a^m) + (b^m) = (1)$ hence $ra^m + sb^m = 1$ for some $r, s \in A$. Define $e_1 \stackrel{\text{def}}{=} ra^m,\ \ e_2 \stackrel{\text{def}}{=} sb^m$. Clearly $X_1 = V(I_1) \subset V((ra^m))$ and $X_2 = V(I_2) \subset V((sb^m))$. Since $V((ra^m)) \cap V((sb^m)) = \emptyset$ and $X_1 \cup X_2 = X$ the equalitiies $X_1 = V((e_1))$ and $X_2 = V((e_2))$ hold, so $X_1 = X_{e_2}$ and $X_2 = X_{e_1}$.

Now we check what happens if X_1 and X_2 are not necessary disjoint. The topological space X is called irreducible if it is not a union of two proper closed subsets $\Leftrightarrow$ all the open subsets of X are dense.

Theorem 1.10. Let $X = \operatorname{Spec} A$.
1) If $z \in X$ then $\overline{z}$ is an irreducible closed set.
2) If $Z \subset X$ is an irreducible closed set then $Z = V(\mathfrak{p})$ for a prime ideal $\mathfrak{p} \subset A$ and $[\mathfrak{p}]$ is a unique generic point of Z.
Proof. 1) If not then both components are closed hence contain $\overline{z}$ which is their union.
2) Let $I = \mathrm{I}(Z)$, so $Z = V(I)$ and $I = \sqrt{I}$. Suppose I is not prime. Then there exist $f, g \in A$ such that $fg \in I$ but both f, g are not in I, so both $J \stackrel{\text{def}}{=} I + (f)$ and $K \stackrel{\text{def}}{=} I + (g)$ are strictly greater than I. Prove that $J \cap K = I$. In fact, if $h = a_1 f + I_1 = a_2 f + i_2$ then $h^2 \equiv a_1 a_2 fg \mod I \Rightarrow h^2 \in I \Rightarrow h \in I$ since I is radical. One concludes that $V(I) = V(J) \cup V(K)$. The radical ideal $I = \bigcap_{\mathfrak{p} \supset I} \mathfrak{p}$ hence there exists some $\mathfrak{p}$ such that $\mathfrak{p} \supset I$ but $f \notin \mathfrak{p}$ so $V(I) \neq V(J)$. For the same reason $V(I) \neq V(K)$. This contradicts our assumption so I is prime and $[I]$ is a generic point for $Z = V(I)$. If $[\mathfrak{q}]$ were another generic point for Z then $[\mathfrak{q}] \in Z \Rightarrow \mathfrak{q} \supset I$. For the same reason $I \supset \mathfrak{q}$ so $I = \mathfrak{q}$.

Finally we have the one-to one correspondences (given by $Z = V(I), I = \mathrm{I}(Z)$):

radical ideals of $A \leftrightarrows$ closed subsets of X
prime ideals of $A \leftrightarrows$ irreducible closed subsets of X
maximal ideals of $A \leftrightarrows$ one-point closed subsets of X

Maps of spectra.

Let $A \stackrel{\phi}{\to} B$ be a homomorphism of rings. It defines a homomorphism $Y = \operatorname{Spec} B \stackrel{f}{\to} X = \operatorname{Spec} A$ by the formula $[\mathfrak{q}] \stackrel{f}{\mapsto} [\mathfrak{q}^c]$ (recall that $\mathfrak{q}^c = \phi^{-1}(\mathfrak{q})$ is prime provided $\mathfrak{q}$ is prime).

Theorem 1.11.
1) $f^{-1}(X_h) = Y_{\phi(h)}$. In particular, the map f is continuous.
2) $I \subset A$ an ideal $\Rightarrow \underline{f^{-1}(V(I))} = V(I^e)$.
3) $J \subset B$ an ideal $\Rightarrow \overline{f(V(J))} = V(J^c)$.
4) ϕ is surjective $\Rightarrow f$ defines a homeomorphism $Y \stackrel{\sim}{\to} V(\ker \phi) \subset X$.
5) ϕ is injective $\Rightarrow f(Y) \subset X$ is dense. More precisely, $f(Y)$ is dense $\Leftrightarrow \ker \phi \subset \mathfrak{R}(A)$.
6) Suppose $A \stackrel{\phi}{\to} B \stackrel{\psi}{\to} C$. Let $Z \stackrel{g}{\to} Y \stackrel{f}{\to} X$ be the corresponding maps of spectra. Then $h = f \circ g$ corresponds to $\eta = \psi \circ \phi$. So $A \mapsto \operatorname{Spec} A$ is a contravariant functor from the category of commutative rings with identity to the category of topological spaces.

Proof. 1) $f^{-1}(X_h) = ([\mathfrak{q}], \mathfrak{q} \subset B \text{ prime and } h \notin \mathfrak{q}^c) = ([\mathfrak{q}], \mathfrak{q} \subset B \text{ prime and } \phi(h) \notin \mathfrak{q}) = Y_{\phi(h)}$.
2) $f^{-1}(V(I)) = ([\mathfrak{q}], [\mathfrak{q}^c] \in V(I)) = ([\mathfrak{q}], \mathfrak{q}^c \supset I) = ([\mathfrak{q}], \phi^{-1}(q) \supset I) = ([\mathfrak{q}], \mathfrak{q} \supset \phi(I)) = ([\mathfrak{q}], \mathfrak{q} \supset (< \phi(I) >= I^e)) = V(I^e)$.
3) $f(V(J)) = ([\mathfrak{q}^c], \mathfrak{q} \supset J)$, so $\overline{f(V(J))} = V(\mathrm{I}\,(f(V(J))) = V(\bigcap\limits_{\mathfrak{q} \supset J} \mathfrak{q}^c) = V((\bigcap\limits_{\mathfrak{q} \supset J} \mathfrak{q})^c) = V((\sqrt{J})^c) = V(\sqrt{J^c}) = V(J^c)$.
4) This is the $A \xrightarrow{\phi} A/K$, resp. $\operatorname{Spec} A/K \xrightarrow{f} \operatorname{Spec} A$ case studied earlier. The only thing to prove is that $f(V(J))$ is a closed subset of $\operatorname{Spec} A$ for any ideal $J \subset A/K$. But $f(V(J)) = V(J^c)$ in this case since prime ideals of A/K are in one-to-one correspondence with prime ideals of A containing K.
5) Apply 3) to the ideal $J = (0) \subset B$.
6) Exercise.

Sheaves.

Let X be a topological space, $Op(X)$ the category whose objects are open subsets of X and morphisms are set-theoretical inclusions, so that $Mor(V, U)$ is empty provided $V \not\subset U$ and $Mor(V, U)$ consists of the single element otherwise.

A presheaf of objects of certain category $\mathcal{A}$ on X is, by definition, a contravariant functor $\mathcal{F} : \ Op(X) \to \mathcal{A}$. In what follows $\mathcal{A}$ will be the category CRings of commutative rings with identity. A sheaf of rings is therefore a collection of rings $\mathcal{F}(U)$ and ring homomorphisms $r_{UV} : \mathcal{F}(U) \to \mathcal{F}(V)$ for each pair of nested subsets $V \subset U$ with the properties that $r_{UU} = \mathrm{Id}$ and for $W \subset V \subset U \ \ r_{UW} = r_{VW} \circ r_{UV}$. The notation $\mathcal{F}(U) = \Gamma(U, \mathcal{F})$ is often used.

The stalk of the presheaf in the point $x \in X$ is given by the formula $\mathcal{F}_x \stackrel{\text{def}}{=} \operatorname{colim}\limits_{U \ni x} \mathcal{F}(U)$.

It makes sense to recall the definition of the colimit above. Sometimes it is also called "direct limit" but it looks better to avoid this name since it is confusing (the colimit is not a "limit" in the category theory language). By definition, the colimit is described by the following universal property. It is a ring $\mathcal{F}_x$ together with fixed homomorphisms $r_{Ux} : \mathcal{F}(U \ni x) \to \mathcal{F}_x$. Given a collection of homomorphisms $\phi_U : \mathcal{F}(U \ni x) \to B$ such that for $V \in U \ \ \phi_U = \phi_V \circ r_{UV}$ where B is some ring, there should exist a unique homomorphism $\psi : \mathcal{F}_x \to B$ such that $\forall U \ni x \ \ \phi_U = \psi \circ r_{Ux}$.

The definition is similar to that of the localisation $S^{-1}A$ of the ring with respect to a multiplicative set. This is by no means coincidence since localisation is also a type of colimit, the $A_{\mathfrak{p}}$ construction being the particular case of the $\mathcal{F}_x$ one.

We now suggest a method to construct the colimit. Consider the disjoint union $\bigcup_{U \ni x} \mathcal{F}(U)$. This is not a ring. Define an equivalence relation on this set: $s \in \mathcal{F}(U) \sim t \in \mathcal{F}(V)$ iff there exists $W \subset U \cap V$ such that $r_{UW}(s) = r_{VW}(t)$. Now one may define the sum or the product of two equivalence classes $s \in \mathcal{F}(U)$ and $t \in \mathcal{F}(V)$ as the equivalence class of the sum/product in $\mathcal{F}(U \cap V)$ of $r_{U\,U\cap V}(s)$ and $r_{V\,U\cap V}(t)$. The definition of the homomorphism r_{Ux} is obvious: it sends $s \in \mathcal{F}(U)$ to its equivalence class. I omit the proofs of the ring structure and of the universal property since they are simple and close to the proof of Theorem 1.2.

Now consider the disjoint union $\Phi = \bigcup_{x \in X} \mathcal{F}_x$. There is a natural projection map $\pi : \Phi \to X$. Define another presheaf $\mathcal{F}^?$ by the formula $\mathcal{F}^?(U)=$ (the set of maps $\sigma : U \to \Phi$ such that $\pi \circ \sigma = \mathrm{Id}_U$). Alternatively speaking the element of $\mathcal{F}^?(U)$ is a collection of the elements $(\sigma_x \in \mathcal{F}_x)$, one for each point $x \in U$. One may add and multiply the collections pointwise since each $\mathcal{F}_x$ is a ring. If $V \subset U$ then the map r_{UV} sends a collection to its part over the subset V.

If one defines a homomorphism of presheaves in a natural way as a morhism of functors (i.e. $\phi : \mathcal{F} \to \mathcal{G}$ is a collection of homomorhisms $\phi_U : \mathcal{F}(U) \to \mathcal{G}(U)$ such that for $r_{UV} \circ \phi_U = \phi_V \circ r_{UV}$ as soon as $V \subset U$) then there is a natural homomorphism $\mathcal{F} \stackrel{\lambda}{\to} \mathcal{F}^?$ which sends $s \in \mathcal{F}(U)$ to the collection of elements $s_x = r_{Ux}(s)$.

The concept of the sheaf comes from the natural question: is it possible to reconstruct the presheaf $\mathcal{F}$ after its image in $\mathcal{F}^?$? In other words, are the rings $\mathcal{F}(U)$ defined by the local data and which kind of local data is suitable?

There are two necessary conditions:
1) The homomorphism $\mathcal{F} \stackrel{\lambda}{\to} \mathcal{F}^?$ must be injective, i.e if $s \in \mathcal{F}(U)$ and all $(s_x, x \in U)$ are zero then $s = 0$.
2) The element $(\sigma_x) \in \mathcal{F}^?(U)$ may come from $\mathcal{F}(U)$ only if $\forall x \in U$ there exists a neighborhood $V : x \in V \subset U$ and an element $t_V \in \mathcal{F}(V)$ such that $\forall y \in V \ r_{Vy}(t_V) = \sigma_y$. Indeed, if $(\sigma_x) = \lambda(s)$ then one may let all (V, t_V) coincide with (U, s).

Define another presheaf $\mathcal{F}^+$ as a subpresheaf of $\mathcal{F}^?$ such that $\mathcal{F}^+(U)$ is a subring of $(\sigma_x) \in \mathcal{F}^?(U)$ satisfying the 2nd condition (to prove that if σ and τ satisfy one then $\sigma+\tau$ and $\sigma\tau$ also do is an easy exercise). We have canonical homomorphism $\mathcal{F} \stackrel{\theta}{\to} \mathcal{F}^+$.

Theorem-definition 1.12. If a presheaf $\mathcal{F}$ satisfies either of two equivalent conditions below it is called a sheaf.
1. $\mathcal{F} \stackrel{\theta}{\to} \mathcal{F}^+$ is an isomorphism.
2. Define a covering $(U_i \hookrightarrow U)$ to be a collection of subsets which cover U (i.e. $\bigcup U_i = U$). Then for any covering the sequence $0 \to \mathcal{F}(U) \to \prod \mathcal{F}(U_i) \rightrightarrows \prod \mathcal{F}(U_i \cap U_J)$ is exact.

The exactness in the middle term means that the colection $(s_i \in \mathcal{F}(U_i))$ equals $(r_{U\ U_i}(s))$ for some $s \in \mathcal{F}(U)$ iff $\forall\, i,j\ \ r_{U_i\ U_i \cap U_j}(s_i) = r_{U_j\ U_i \cap U_j}(s_j)$.

Proof. $\mathcal{F}^+$ obviously satisfies the second condition so $1 \Rightarrow 2$ clear. $2 \Rightarrow 1$ Suppose $\theta(s) = 0$ for some $s \in \mathcal{F}(U)$. This means that $\forall\, x \in U\ r_{Ux}(s) = 0 \Rightarrow \forall\, x \in U\, \exists U \supset V_x \ni x$ such that $r_{U\ V_x}(s) = 0$. Since $(V_x \hookrightarrow U)$ is a covering one concludes that $s = 0$ so θ is injective. Suppose now that $(\sigma_x \in \mathcal{F}_x) \in \mathcal{F}^+(U)$. For each $x \in U$ choose V_x and t_{V_x} such that $\forall y \in V_x\ \ \sigma_y = r_{V_x\ y}(t_{V_x})$. Since $(V_x \hookrightarrow U)$ is a covering and t_{V_x} coincides with t_{V_y} on $V_x \cap V_y$ by the property of $\mathcal{F}^+$ one concludes that $\exists\ t \in \mathcal{F}(U)$ such that $\forall\, x \in U\ \ t_{V_x} = r_{U\ V_x}(t)$ hence $\sigma_x = r_{V_x\ x}(r_{U\ V_x}(t)) = r_{U\ x}(t) \Rightarrow \sigma \in \theta(\mathcal{F})$.

Remark 1. For the general presheaf $\mathcal{F}$ the ring $\mathcal{F}(\emptyset)$ needs not to be zero (one may, for example, set $\mathcal{F}(U) = A$ for all open subsets of X including the empty one, all r_{UV} being identity maps). Nevertheless if $\mathcal{F}$ is a sheaf then $\mathcal{F}(\emptyset)$ is a zero ring. Indeed, the empty product of rings is the zero ring by definition hence $\mathcal{F}^?(\emptyset) = \mathcal{F}^+(\emptyset)$=0.
Remark 2. If a presheaf $\mathcal{F}$ is not a sheaf then the sheaf $\mathcal{F}^+$ is called the associated sheaf to $\mathcal{F}$. Clearly the stalks $\mathcal{F}_x$ and $\mathcal{F}^+_x$ are the same while $\mathcal{F}(U)$ and $\mathcal{F}^+(U)$ may differ.
Remark 3. The presheaf $\mathcal{F}^?$ is obviously a sheaf. If $\mathcal{F}$ is itself a sheaf then $\mathcal{F}^?$ is a first term of so called Godement resolution of $\mathcal{F}$ useful for cohomology.

Example. Suppose A is a topological ring. Let $\mathcal{F}(U)$ be the ring of continuous maps $U \to A$ (zero ring for U empty) with pointwise addition and multiplication and r_{UV} the restriction maps. Then $\mathcal{F}$ is a sheaf (the condition 2 from the theorem above holds obviously) which is called the sheaf of germs of continuous functions with values in A. There are two borderline subexamples. If A carries the trivial topology (only $\emptyset$ and A itself are open) then $\mathcal{F}$ above is the sheaf of germs of all functions while if the topology on A is discrete (i.e. all the subsets are open) then $\mathcal{F}$ is so called constant sheaf ($\mathcal{F}(U)$

coinsides with the ring of maps $U \to A$ which are constant on the connected components of U). The latter sheaf is associated to the presheaf $\mathcal{F}_c$ from the Remark 1 above since $\forall\, x\ (\mathcal{F}_c)_x = A$ so $\mathcal{F}_c^+(U)$ consists precisely of locally constant maps $U \to A$.

The structure sheaf on $\operatorname{Spec} A$**.**

We are now going to define a certain sheaf of rings $\mathcal{O}_X$ on the space $X = \operatorname{Spec} A$ which is called the structure sheaf.

We start with the definition of $\mathcal{O}_X(U)$ for principal open subsets $X_h \subset X$, namely, let $\mathcal{O}_X(X_h) \stackrel{\text{def}}{=} A_h$. To define $r_{X_h\ X_g}$ for which we often will use the notation r_{hg} for shortness recall that $X_g \subset X_h \Leftrightarrow V((g) \supset V((h)) \Rightarrow g \in \sqrt{(h)}$. This means that for some $m > 0$ and $a \in A\ g^m = ah$. Define the homomorphism $r_{hg} :\ A_h \to A_g$ with the formula $\frac{b}{h^n} \stackrel{r_{hg}}{\mapsto} \frac{ba^m}{g^{nm}}$. To check that r_{hg} does not depend on the choice of the fraction representing the element of X_h, that for $X_f \subset X_g \subset X_h\ r_{hf} = r_{gf} \circ r_{hg}$ and, finally, that $r_{gh} = \mathrm{Id}$ provided $X_h = X_g$ (this happens iff $\sqrt{(h)} = \sqrt{(g)}$) is an easy exercise.

We now calculate the stalks of the desired presheaf $\mathcal{O}_X$. Suppose $\mathfrak{p} \in X_h$. This means that $h \notin \mathfrak{P}$ hence $S_h \subset A \setminus \mathfrak{p}$ so the canonical homomorphism $A_h \stackrel{\psi_{h,[\mathfrak{p}]}}{\to} A_{\mathfrak{p}}$ is defined. Consider the "stalk" $\operatorname{co\,lim}\limits_{X_h \ni [\mathfrak{p}]} A_h = \operatorname{colim}\limits_{h \notin \mathfrak{p}} A_h ='' (\mathcal{O}_X)''_{\mathfrak{p}}$.

Remark. We use the quotes sign since the colimit is taken not with all open neighborhoods of the point $[\mathfrak{p}]$ but only with principal ones. Nevertheless if we succeed in giving a correct definition of $\mathcal{O}_X$ (what remains is to define $\mathcal{O}_X(U)$ and r_{UV} for general open subsets which are not necessary of the form X_h) then the quotes may be deleted since each $U \ni [\mathfrak{p}]$ is a union of principal open sets and therefore contains some $X_h \ni [\mathfrak{p}]$.

The homomorphisms $\psi_{h.[\mathfrak{p}]}$ obviously commute with r_{hg} as defined above therefore they define a homomorphism $''(\mathcal{O}_X)''_{\mathfrak{p}} \stackrel{\psi_{\mathfrak{p}}}{\to} A_{\mathfrak{p}}$ which in fact is an isomorphism (surjectivity is obvious, injectivity is checked immediately).

We now have enough data to construct the presheaf $\mathcal{O}_X$. Namely, let $\mathcal{O}_X^{\pm}(U) \stackrel{\text{def}}{=}$ ring of collections $(\sigma_{[\mathfrak{p}]} \in A_{\mathfrak{p}})$ with pointwise ring operations such that there exist a covering $(X_{h_\alpha} \hookrightarrow U)$ with principal open sets and the elments $t_\alpha \in A_{h_\alpha}$ which satisfy the following property: $[\mathfrak{p}] \in X_{h_\alpha} \Rightarrow \psi_{h_\alpha,[\mathfrak{p}]}(t_\alpha) = \sigma_{[\mathfrak{p}]}$
For $V \in U$ we define $r_{VU} :\ \mathcal{O}_X^{\pm}(U) \to \mathcal{O}_X^{\pm}(V)$ by taking the subcollection over V instead

of U.

The $\pm$ sign is to emphasize that we use the same property as we did to describe $\mathcal{F}^+$ but with respect only to the principal open sets X_h because (as opposite to the general presheaf $\mathcal{F}$ considered above) the rings $\mathcal{O}_X^{\pm}(U)$ were not yet defined up to this moment. From now on we use notation $\mathcal{O}_X$ for the presheaf $\mathcal{O}_X^{\pm}$.

Theorem 1.13.
1. The presheaf $\mathcal{O}_X$ is a sheaf.
2. $\mathcal{O}_X(X_h) = A_h$.
3. $(\mathcal{O}_X)_{[\mathfrak{p}]} = A_{\mathfrak{p}}$.

Proof. 1. We check the properties of the 2nd definition of the sheaf. Let $U_\alpha \hookrightarrow U$ be a covering. Suppose $(\sigma_{[\mathfrak{p}]}) \in \mathcal{O}_X(U)$ and its restriction to each U_α is zero. Then $\forall\ [\mathfrak{p}] \in U\ \ \sigma_{[\mathfrak{p}]} = 0$ hence $(\sigma_{[\mathfrak{p}]}) = 0$. Given a set of collections $(\sigma_{[\mathfrak{p}]})_\alpha \in \mathcal{O}_X(U_\alpha)$ which agree on intersections one may define the joint colection $(\sigma_{[\mathfrak{p}]}) \in \mathcal{O}_X(U)$. If the particular collections satisfiy the property in the definition of $\mathcal{O}_X^{\pm}$ then the joint collection also does since one may consider the covering of U with X_h which is the union of coverings of particular U_α.
2. We first prove that the natural map $A_h \to \mathcal{O}_X(X_h)$ is injective. By definition the zero element in $\mathcal{O}_X(X_h)$ is represented by some covering $X_{h_\alpha} \hookrightarrow X_h$ together with the elements $t_\alpha \in A_{h\alpha}$ such that $\forall\ X_{h_\alpha} \ni [\mathfrak{p}]\ \ \psi_{h_\alpha,[\mathfrak{p}]}(t_\alpha) = 0$.
Suppose $s \in A_h$ is represented by the fraction $\frac{b}{h^n}$. Define the ideal $Ann(b) \subset A$ by the formula $Ann(b) \stackrel{\text{def}}{=} (c \in A \mid bc = 0)$. Then $s = 0 \Leftrightarrow h \in \sqrt{Ann(b)} \Leftrightarrow$ all prime ideals containing $Ann(b)$ contain h. Suppose that $s \neq 0$. Then there exists some $\mathfrak{p} \subset A$ prime such that $\mathfrak{p} \supset Ann(b)$ but $\mathfrak{p} \not\ni h$ hence $\mathfrak{p} \in A_h$ hence $\mathfrak{p} \in A_{h_\alpha}$ for some α. By assumption $r_{hh_\alpha}(s) = 0$ hence $\psi_{h,[\mathfrak{p}]}(s) = \psi_{h_\alpha,[\mathfrak{p}]}(r_{hh_\alpha}(s)) = 0$. This implies that $\psi_{h,[\mathfrak{p}]}(b) = 0$ as b is a multiple of s. The last statement means that b is annihilated by some element of $A \setminus \mathfrak{p}$ so $\mathfrak{p} \not\supset Ann(b)$ - contradiction.
We now prove that the map $A_h \to \mathcal{O}_X(X_h)$ is surjective. For what follows almost WLOG we may suppose that $h = 1$ (for general h the argument is the same, the notations being more heavy). Suppose the element of $\mathcal{O}_X(X)$ is represented by the collection of the elements $t_{[\mathfrak{p}]} \in A_{\mathfrak{p}}$ such that for some covering $(X_{h_\alpha} \hookrightarrow X)$ and the elements $t_\alpha \in A_{h_\alpha}$ we have $\psi_{h_\alpha,[\mathfrak{p}]}(t_\alpha) = t_{[\mathfrak{p}]}$ as soon as $[\mathfrak{p}] \in A_{h_\alpha}$. We need to find an element $t \in A$ such that $\forall\, \alpha\ \ r_{1h_\alpha}(t) = t_\alpha$.
Choose a finite subcovering $(X_{h_i} \hookrightarrow X)$. It suffices to find t such that $r_{1h_i}(t) = t_i$. Indeed if we find one then for arbitrary X_{h_α} its image in $A_{h_\alpha h_i}$ will coincide with $r_{h_i\ h_i h_\alpha}(t_i)$ for each i hence will be equal to t_α since we already proved the injectivity and t_α and t_i agree

on intersections by assumption.

Let $t_i = \frac{b_i}{h_i^n}$ (one may choose the same n for all i). $r_{h_i\ h_ih_j}(t_i) = \frac{b_ih_j^n}{(h_ih_j)^n}$ while $r_{h_j\ h_ih_j}(t_j) = \frac{b_jh_i^n}{(h_ih_j)^n}$. The two should coincide which means that there exists some m_{ij} such that $(h_ih_j)^{m_{ij}}(b_ih_j^n - b_jh_i^n) = 0$ in A. Suppose M dominates all the m_{ij} and let $N \stackrel{\text{def}}{=} M + n$. Now let $B_i \stackrel{\text{def}}{=} b_ih_i^N$. Then $t_i = \frac{B_i}{h_i^N}$ in A_{h_i} and $B_ih_j^N - B_jh_i^N = 0$ in A. But X is a union of $X_{h_i} = X_{h_i^N}$ hence $\sum a_ih_i^N = 1$ for some $a_i \in A$. Let $t \stackrel{\text{def}}{=} \sum a_iB_i$. Then $\forall\, j\ \ h_j^Nt = \sum a_ih_j^NB_i = \sum a_ih_i^NB_j = B_j$ thus $r_{1h_j}t = t_j$ as desired.
3. See Remark after the definition of the "stalk" of $\mathcal{O}_X$

Remark. The standard maps $r_{Ux} : \mathcal{O}_X(U) \to (\mathcal{O}_X)_x$ coincide with the maps $\psi_{h,[\mathfrak{p}]} : A_h \to A_{\mathfrak{p}}$ provided $U = A_h$ and $x = [\mathfrak{p}],\ h \notin \mathfrak{p}$.

For what follows we need an important property of the homomorphisms of sheaves (which does not hold for the presheaves). Recall that the homomorphism of sheaves is the same as the homomorphism of presheaves, namely the set of homomorphisms $\mathcal{F}(U) \stackrel{\phi_U}{\to} \mathcal{G}(U)$ which commute with the r_{UV} maps in a natural way. It is called an isomorphism iff all ϕ_U are isomorphisms.

Theorem 1.14. Suppose X is a topological space, $\mathcal{F} \stackrel{\phi}{\to} \mathcal{G}$ a homomorphism of sheaves. ϕ is an isomorphism $\Leftrightarrow$ the induced homomorphisms $\mathcal{F}_z \stackrel{\phi_x}{\to} \mathcal{G}_x$ are isomorphisms for all points $x \in X$.
Proof. $\Rightarrow$ obvious. $\Leftarrow$ Suppose all ϕ_x are isomorphisms.
ϕ_U injective: Suppose $s \in \mathcal{F}(U),\ \ \phi_U(s) = 0$. Then $\forall\, x \in U\ \ \phi(s)_x = 0$ in $\mathcal{G}_x \Rightarrow$ (by the assumption) $s_x = 0$ in $\mathcal{F}_x \Rightarrow \exists V_x \subset U$ a neighborhood of x such that $r_{U\,V_x}(s) = 0$ in $\mathcal{F}(V_x)$. Then $s = 0$ since $\mathcal{F}$ is a sheaf and the open sets V_x cover U.
ϕ is surjective: Suppose $t \in \mathcal{G}(U)$, we need to find a preimage of t in $\mathcal{F}(U)$. For each $x \in U$ find a $s_x \in \mathcal{F}_x$ such that $\phi_x(s_x) = t_x$ (possible by the assumption). Let s_x be represented by some $s_{V_x} \in \mathcal{F}(V_x)$ where $V_x \subset U$ is a neighborhood of x. Replacing if needed the neighborhoods V_x by smaller neighborhoods which we still denote V_x one may guarantee that $\phi_{V_x}(s_{V_x}) = r_{U\ V_x}(t)$. Clearly $r_{V_x\ V_x\cap V_y}(\phi(s_{V_x})) = r_{V_y\ V_x\cap V_y}(\phi(s_{V_y}))$ since both are equal to $r_{U\ V_x\cap V_y}(t)$. This means that $\phi(s_{V_x})$ do agree on intersections of the covering $(V_x \hookrightarrow U)$ hence s_{V_x} also do thanks to injectivity of ϕ_U proved above. Since $\mathcal{F}$ is a sheaf there exists $s \in \mathcal{F}(U)$ such that $\forall x \in U\ \ r_{U\ V_x}(s) = s_{V_x}$. Obviously $\phi_U(s) = t$.

Locally ringed spaces.

Suppose $Y \xrightarrow{f} X$ is a continuous map of topological spaces. Let $\mathcal{G}$ be a sheaf on Y. Define the direct image $f_*(\mathcal{G})$ by the formula $f_*(\mathcal{G})(U) = \mathcal{G}(f^{-1}(U))$. Clearly $f_*(\mathcal{G})$ is a presheaf on X which in fact is a sheaf (each covering $(U_i \hookrightarrow U)$ of the open set $U \subset X$ defines a covering $(f^{-1}(U_i) \hookrightarrow f^{-1}(U))$ so both properties of the definition could be checked by direct calculation).

One may calculate the stalks: $(f_*(\mathcal{G}))_x = \operatorname{colim}_{U \ni x} f_*(\mathcal{G})(U) = \operatorname{colim}_{U \ni x} \mathcal{G}(f^{-1}(U)) = \operatorname{co}\lim_{V = f^{-1}(U \ni x)} \mathcal{G}(V)$.

We now define the category of locally ringed spaces (LRS). Each object of LRS is a pair $(X, \mathcal{F})$ where X is a topological space and $\mathcal{F}$ is a sheaf of rings on X satisfying the property: all the stalks $\mathcal{F}_x$ are local rings. For example, the structure sheaf $\mathcal{O}_X$ on $X = \operatorname{Spec} A$ does satisfy this property since $(\mathcal{O}_X)_{[\mathfrak{p}]} = A_{\mathfrak{p}}$, the latter being a local ring.

A morphism $(Y, \mathcal{G}) \to (X, \mathcal{F})$ of locally ringed spaces is a pair (f, ϕ) where $f : Y \to X$ is a continuous map and $\phi : \mathcal{F} \to f_*(\mathcal{G})$ is a local homomorphism of sheaves on X. To define what does "local" mean consider the composition homomorphism of stalks $\mathcal{F}_{f(y)} \to (f_*(\mathcal{G}))_{f(y)} \to \mathcal{G}_y$. The left arrow is induced by ϕ, while the right one is a natural homomorphism of colimits (the neighborhoods of the point y of the form $V = f^{-1}(U \ni f(y))$ constitute a part of the full set of neighborhoods). The homomorphism ϕ is called local iff $\forall\ y \in Y$ the corresponding homomorhisms $\mathcal{F}_{f(y)} \to \mathcal{G}_y$ are local homomorphisms of local rings.

It remains to define a local homomorphism $A \xrightarrow{\phi} B$ of local rings. ϕ is called local iff $\phi^{-1}(\mathfrak{m}_B) = \mathfrak{m}_A$. Since the image of invertible element is invertible $\phi^{-1}(\mathfrak{m}_B) \subset \mathfrak{m}_A$ always so locality means that $\phi^{-1}(\mathfrak{m}_B) \supset \mathfrak{m}_A$ which in turn means that $\phi(\mathfrak{m}_A) \subset \mathfrak{m}_B$. The non-local homomorphisms do exist: consider the inclusion of a local ID to its field of fractions.

It is clear that the composition of local homomorphisms of sheaves is local as well as the Id homomorphism , hence the definition of the category LRS is correct.

Example. Let $(X, \mathcal{F})$ be a locally ringed space, $W \subset X$ an open subset. Then there is a canonical morphism $(W, \mathcal{F}|_W) \to (X, \mathcal{F})$. The map f is the inclusion map $W \hookrightarrow X$ while $\phi_U : \mathcal{F}(U) \to f_*(\mathcal{F}|_W)(U) = \mathcal{F}(U \cap W)$ coincides with the restriction map $r_{U\ U \cap W}$.

Why do we need locality in the definition of the morphism of locally ringed spaces? There is a following reason. Suppose $(X, \mathcal{F})$ is a locally ringed space. Since all $\mathcal{F}_x$ are

local rings the residue fields $k_{\mathcal{F}}(x) \stackrel{\text{def}}{=} \mathcal{F}_x/\mathfrak{m}_{\mathcal{F}_x}$ are defined. Define a sheaf $\overline{\mathcal{F}}$ on X by the formula $\overline{\mathcal{F}}(U) =$ (set of collections of elements $\overline{s_x} \in k_{\mathcal{F}}(x)$) with pointwise addition and multiplication. Then there is a canonical homomorphism of sheaves $\mathcal{F} \to \overline{\mathcal{F}}$. Besides this homomorphism is generally not injective (the elements of $\mathcal{R}(\mathcal{F}(U))$ become zero in $\overline{\mathcal{F}}(U)$) the stalks of $\overline{\mathcal{F}}$ are more simple than those of $\mathcal{F}$ ($\mathcal{F}_x/\mathfrak{m}_{\mathcal{F}_x}$ vs $\mathcal{F}_x$).
Clearly the morphism of locally ringed spaces $(Y, \mathcal{G}) \to (X, \mathcal{F})$ correctly defines the homomorphism of fields $k_{\mathcal{F}}(f(y)) \to k_{\mathcal{G}}(y)$ iff the homomorphism $\mathcal{F}_{f(y)} \to \mathcal{G}_y$ considered above is local. That is where the locality condition comes from.

Example. Let $X = \operatorname{Spec} A$. Then there is a canonical isomorphism of locally ringed spaces $(\operatorname{Spec} \mathcal{O}_h = Y, \mathcal{O}_Y) \stackrel{\sim}{\to} (X_h, \mathcal{O}_X|_{X_h})$.
Indeed, let $i_h : A \to A_h$ be the localisation map. It defines (by extension and contraction) a one-to-one correspondence (prime ideals $\mathfrak{p} \subset A$ such that $h \notin \mathfrak{p}$) $\leftrightarrow$ (prime ideals $\mathfrak{q} \subset A_h$) thus also a bijection of sets $X_h \leftrightarrow \operatorname{Spec} A_h = Y$. After this bijection there also is a bijection $X_{hg} \leftrightarrow Y_{i_h(g)}$ (the prime ideal $\mathfrak{P}$ does not contain hg iff its image in A_h does not contain $\frac{g}{1}$ since h is invertible in A_h). Since $X_h \cap X_g = X_{hg}$ the sets X_{hg} constitute a base of open subsets of X_h. Also any principal subset of $\operatorname{Spec} A_h$ is of the form $Y_{i_h(g)}$ for some g since $(A_h)_{\frac{g}{h^n}} = (A_h)_{\frac{g}{1}}$. We proved that the bijective map of sets $X_h \leftrightarrow \operatorname{Spec} A_h = Y$ is a homeomorphism. Both $\mathcal{O}_X|X_h(X_{hg})$ and $\mathcal{O}_Y(Y_{i_h(g)})$ are canonically isomorphic to A_{hg} so the canonical isomorphisms of stalks are defined which lead to the desired isomorphism of sheaves.

Now we compare the categories CRings vs LRS.

We first define a contravariant functor Crings $\to$ LRS. Suppose $A \stackrel{\Phi}{\to} B$ is a homomorphism of rings. Define the morphism $(f, \phi) : (Y = \operatorname{Spec} B, \mathcal{O}_Y) \to (\operatorname{Spec} A = X, \mathcal{O}_X)$.
Let $f([\mathfrak{q}]) \stackrel{\text{def}}{=} [\mathfrak{q}^c]$ for each point $[\mathfrak{q}] \in Y$. We need to prove that f is continuous and to define a homomorphism $\phi : \mathcal{O}_X \to f_*(\mathcal{O}_Y)$ i.e to define for any open set $U \subset X$ a homomorphism $\phi_U : \mathcal{O}_X(U) \to \mathcal{O}_Y(f^{-1}(U))$.
We start with the principal open sets. Suppose $U = X_h$. Then $f^{-1}(U) = ([\mathfrak{q}] \in Y$ such that $\mathfrak{q}^c \not\ni h) = ([\mathfrak{q}] \in Y$ such that $\mathfrak{q} \not\ni \Phi(h)) = Y_{\Phi(h)}$ (in particular this proves that f is continuous). So we need a homomorphism $\mathcal{O}_X(X_h) = A_h \to B_{\Phi(h)} = \mathcal{O}_Y(f^{-1}(X_h)$. Set $\phi_h(\frac{a}{h^n}) \stackrel{\text{def}}{=} \frac{\Phi(a)}{\Phi(h)^n}$. The homomorphisms just constructed are correctly defined and duly commute with the restriction maps therefore they define the homomorphisms of stalks $\phi_{[\mathfrak{q}]} : A_{\mathfrak{q}^c} \to B_{\mathfrak{q}}$ (recall that it suffices to calculate the colimits with principal open neighborhoods). The latter are clearly local as $a \in \mathfrak{q}^c \Leftrightarrow \Phi(a) \in \mathfrak{q}$.

Theorem 1.15.
Any morphism $(f, \phi) : (Y = \operatorname{Spec} B, \mathcal{O}_Y) \to (X = \operatorname{Spec} A, \mathcal{O}_X)$ could be defined after the unique $A \xrightarrow{\Phi} B$ as described above.
Proof. By the definition of the structure sheaf $\mathcal{O}_X(X) = A$ (same for Y and B). By the definition of the functor above the homomorphism $\Phi : A \to B$ must coincide with ϕ_X. Suppose $\mathfrak{q} \subset B$ is a prime ideal, $[\mathfrak{q}] = y \in Y$ and $f(y) = [\mathfrak{p}], \mathfrak{p} \subset X$. Then the diagram below commutes:

$$\begin{array}{ccc} A & \xrightarrow{\Phi=\phi_X} & B \\ {\scriptstyle r_{1\mathfrak{p}}}\downarrow & & \downarrow{\scriptstyle r_{1\mathfrak{q}}} \\ A_{f(y)} & \xrightarrow{\phi_y} & B_y \end{array}$$

Let $\mathfrak{m}_{B_y} \subset B_y$ and $\mathfrak{m}_{A_{f(y)}} \subset A_{f(y)}$ be maximal ideals of the corresponding stalks. Then $\Phi^{-1}(r_{1\mathfrak{q}}^{-1}(\mathfrak{m}_{B_y})) = \Phi^{-1}(\mathfrak{q})$ while $r_{1\mathfrak{p}}^{-1}(\phi_y^{-1}(\mathfrak{m}_{B_y})) = r_{1\mathfrak{p}}^{-1}(\mathfrak{m}_{A_{f(y)}})$ (since ϕ_y is local) which equals $\mathfrak{p}$. This means that Φ^{-1} and f act on the set of points of Y in the same way. It is obvious (at least on the principal open sets) that the construction above applied to $\Phi = \phi_X$ leads to ϕ.

Remark. While the ring A is reconstructed from the locally ringed space as $\mathcal{O}_X(X)$ it cannot be reconstructed via the topological space X alone. For example, $\operatorname{Spec} A$ and $\operatorname{Spec} A/\mathfrak{R}(A)$ are homeomorphic.

Corollary. The full subcategory of LRS whose objects are of the form $(\operatorname{Spec} A, \mathcal{O}_{\operatorname{Spec} A})$ is equivalent to the category $(\mathrm{CRings})^\circ$.

Noetherian rings and modules.

Theorem-definition 1.16.
1. Suppose A is a ring. The following conditions are equivalent:
a) Any ideal $I \subset A$ is finitely generated $\Leftrightarrow$.
b) Any ascending chain of ideals $I_1 \subset I_2 \subset \dots$ stabilizes (i.e $\exists d$ such that for $i > d\, I_i = I_d$).
c) Any nonempty set of ideals (I_α) contains a maximal element (i.e. $\exists \alpha_0$ such that $I_{\alpha_0} \subset I_\alpha$ implies $I_{\alpha_0} = I_\alpha$).
2. Suppose A is any ring (not necessary of the type described above), M an A-module. Then the following conditions are equivalent:
Any submodule $N \subset M$ is finitely generated $\Leftrightarrow$ any ascending chain of submodules $N_1 \subset N_2 \subset \dots$ stabilizes $\Leftrightarrow$ any nonempty set of submodules contains a maximal ele-

ment.
The ring/module is called Noetherian if it satisfies the equivalent conditions above.

Proof. We suggest a proof for rings, that for modules being basically the same.
a)⇒b) Suppose all ideals are finitely generated. Consider a chain $I_1 \subset I_2 \subset \dots$. Let $I \stackrel{\text{def}}{=} \bigcup I_i$. By assumption I is finitely generated hence all the generators are contained in some I_d, the latter is therefore equal to I.
b)⇒c) Now suppose the ascending chains condition is fulfilled. Consider a nonempty set of ideals I_α. Suppose it contains no maximal elements. Then one may choose I_{α_0}. SInce it is not a maximal element of the set one may choose I_{α_2} such that I_{α_1} is a proper subset of I_{α_2}. Proceeding in that way one constructs the ascending chain of ideals which does not stabilize.
c)⇒a) Finally, suppose maximal elements in the sets of ideals do always exist. Consider an ideal I and the set of all finitely generated ideals $I_\alpha \subset I$. Clearly any maximal element in this set must coincide with I.

Remark 1. The concept is due to Emmy Noether (1882-1935), one of the key persons in the development of commutative algebra.
Remark 2. The second part of the proof uses the so-called axiom of dependent choice which in fact is weaker than the standard axiom of choice (the latter being equivalent to the Zorn's lemma).
Remark 3. The ring is Noetherian ⇔ it is a Noetherian module when considered as a module over itself .
Remark 4. In the Noetherian ring or module any set of generators of an ideal/submodule contains a finite subset still generating it. Indeed, let $I =< (x_\alpha) >$ (assumption) $=< (y_i, 1 \le i \le r) >$ (Noetherian). Represent all y_i as finite linear combinations of some x_α. The total number of generators x_α used in the representations is finite, clearly these x_α generate I.

Properties of Noetherian rings/modules.

1) A is Noetherian ⇒ $B = A/K$ is Noetherian .
2) A is Noetherian ⇒ $B = S^{-1}A$ is Noetherian .

In both cases above the ideals $J \subset B$ enjoy the property $J = J^{ce}$ hence J is generated by the images in B of the generators of J^c.

3) Suppose A is Noetherian , $A \stackrel{\phi}{\to} B$ and B is a finite A-algebra (i.e. B is finitely generated as an A-module). Then B is Noetherian .
Since B is finitely generated as an A-module B is isomorphic (as an A-module) to a quotient module of A^n by some A-submodule $N \subset A^n$. Since A is a Noetherian ring it is also a Noetherian module over itself therefore A^n and A^n/N also are (see property 4) below). So B is a Noetherian module over A hence also over B as elements of A act on B via their images in B. One concludes that B is a Noetherian ring.

Remark. In geometric terms $A \to A/K$ corresponds to the closed embedding of spectra, $A \to A_h$ to the open embedding while the example above to the finite covering $\operatorname{Spec} B \to$ (some closed subset of $\operatorname{Spec} A$), the latter being $\operatorname{Spec} A$ itself provided ϕ is injectve.

4) Suppose A is any ring, $0 \to M' \stackrel{i}{\to} M \stackrel{j}{\to} M'' \to 0$ an exact sequence of A-modules. This means that i is injective, j is surjective and $\operatorname{im}(i) = \ker(j)$, in other words $M'' = M/M'$.
Then:
a) M' and M'' are finitely generated $\Rightarrow M$ is finitely generated.
The opposite is not true: while M'' is clearly finitely generated provided M is, M' needs not, say, it may be some ideal of non-Noetherian A which is not finitely generated over A besides A is generated by 1.
b) M' and M'' are Noetherian $\Leftrightarrow M$ is Noetherian .
To prove a) suppose $N \subset M$ is a submodule. Choose a set of generators $(x_k \in M'', 1 \leq k \leq r)$ of $j(M)$ and some set of their preimages $(\tilde{x}_k \in M)$, one for each x_k. If $y \in M$ then $j(y)$ is a linear combination of x_k, hence y may be sent to M' bu subtraction of the same linear combination of $\tilde{x}_k$. So if one adds some set of generators of M' to the set $(\tilde{x}_k)$ then the joint set will generate M.
To prove b) $\Rightarrow$ consider a submodule $N \subset M$. Then $0 \to N \cap M' \to N \to j(N) \to 0$ is exact and we may use a) as both M' and M'' are Noetherian . $\Leftarrow$ Each submodule of M' is a submodule of M hence finitely generated. If $N \subset M''$ is a submodule then $N = j(j^{-1}(N))$. Since $j^{-1}(N)$ is finitely generated N also is.

The proof of 3) may now be finished by induction as there is an exact sequence of A-modules $0 \to A^{n-1} \to A^n \to A \to 0$.

5) If A is Noetherian then any finitely generated A-module M is Noetherian .
This may be proved by induction on the minimal number of generators. Let $M = < (x_k, 1 \leq k \leq r) >$. Then there is an exact sequence $0 \to Ax_1 \to M \to M/Ax_1 \to 0$.

The module to the left is isomorphic to $A/Ann(x_1)$ hence it is Noetherian as A is Noetherian. The module to the right is generated by the images of x_k, $2 \leq k \leq r$ hence it is Noetherian by the induction hypothesis. Thus by 4) M is Noetherian .

Theorem 1.17.
Suppose A is a Noetherian ring, M a finitely generated A-module. Then there exists a composition series $M = M_r \supset M_{r-1} \supset \cdots \supset M_1 \supset M_0 = 0$ such that all the successive quotients are of the form $M_i/M_{i-1} \simeq A/\mathfrak{p}_i$ where $\mathfrak{p}_i \subset A$ are prime ideals.
Proof. Consider the set of ideals in A of the form $Ann(x)$ where x is a nonzero element of M. Let $I = Ann(x_0)$ be maximal in that set which exists as A is Noetherian . Then I is a prime ideal (easy exercise) which we denote $\mathfrak{p}_1$. Set $M_1 \overset{\text{def}}{=} Ax_0$, then $M_1 \simeq A/\mathfrak{p}_1$ and there is an exact sequence $0 \to M_1 \xrightarrow{i} M \xrightarrow{j} M/M_1 \to 0$. Now choose a submodule $\overline{M_2} \subset M/M_1$ in the same way so that $\overline{M_2} \simeq A/\mathfrak{p}_2$ and set $M_2 = j^{-1}(\overline{M_2})$. Then $M_2/M_1 \simeq \overline{M_2} \simeq A/\mathfrak{p}_2$. Acting as above we obtain a chain of submodules $M_1 \subset M_2 \subset \ldots$ such that all the successive quotients are of desired type. Since M is Noetherian $M_r = M$ for some r.

Theorem 1.18 (Hilbert's Basis).
Suppose A is a Noetherian ring, B a finitely generated (as an algebra) A-algebra. Then B is Noetherian .

Remark. Compare this to the much stronger condition in the property 3 where B is asked to be finitely generated as an $A-module$.

Proof. The assumption means that $B \simeq A[T_1, \ldots, T_n]/I$ where I is some ideal so it suffices to prove the theorem for $B = A[T_1, \ldots, T_n]$ (see property 1). Since $A[T_1, \ldots, T_n] = A[T_1, \ldots, T_{n-1}][T_n]$ it suffices to prove it for $B = A[T]$.
Suppose $J \subset A[T]$ is an ideal. For $i \geq 0$ define the ideal $I_i \subset A$ to be generated by all leading coefficients of polynomials of degree i contained in J. Clearly $I_i \subset I_{i+1}$ (one may just multiply the polynomial with T). Since A is Noetherian the chain of ideals $I_0 \subset I_1 \subset \ldots$ stabilizes which means that all the leading coefficients of all elements of J are contained in some I_d. Choose a finite set of generators (a_k) of the ideal I_d. For each a_k one may choose a polynomial f_k which is contained in J and has leading coefficient a_k. Then $J =< (f_k) >$. Indeed, the terms of an arbitrary $f \in J$ may be killed successively starting from the leading one by subtracting the suitable linear combinations of polynomials f_k.

Remark. Hilbert's original statement was for $B = k[T_1, \ldots, T_n]$, k a field.

Theorem 1.19.(Nakayama's Lemma).
Suppose A is any ring, M a finitely generated A-module, $I \subset A$ an ideal such that $I \subset \mathfrak{J}(A) = \bigcap\limits_{\mathfrak{m} \supset I \text{ maximal}} \mathfrak{m}$. Then $M = IM \Rightarrow M = 0$.

Proof. Suppose $M \neq 0$. Then $M =< (x_1, \ldots, x_n) >$, the number n is supposed to be minimal possible. If $M = IM$ then there exists a presentation $x_1 = \sum\limits_{i=1}^{n} a_i x_i$ where all $a_i \in I$. This means that $(1 - a_1)x_1 = \sum\limits_{i=2}^{n} a_i x_i$. But $1 - a_1$ lies outside all the maximal ideals hence it is invertible in A. This means that x_1 is a linear combination of other x_i's - contradiction.

Remark. The statement of the Lemma is false for general (not necessary finitely generated) A-modules. For example let A be a local ID with maximal ideal $\mathfrak{m}$, $K = A_{(0)}$ its field of fractions. Then $\mathfrak{m}K = K$.

Corollary 1. Under the conditions of the Lemma if $N \subset M$ is a submodule such that $M = N + IM$ then $N = M$. This is clear since one may apply the theorem to the module M/N.

Corollary 2. Suppose A is a local ring, $k \stackrel{\text{def}}{=} A/\mathfrak{m}$ its residue field, M a finitely denerated A-module. Then the elements $x_1, \ldots, x_n$ generate $M \Leftrightarrow$ their images generate the k-vector space $M/\mathfrak{m}M$.
Important particular case: suppose A is a local Noetherian ring. Then the elements $(a_1, \ldots, a_n \in \mathfrak{m})$ generate $\mathfrak{m} \Leftrightarrow$ their images generate the k-vector space $\mathfrak{m}/\mathfrak{m}^2$. The minimal possible number n coincides therefore with $\dim_k \mathfrak{m}/\mathfrak{m}^2$. This is closely related to the geometric concept of the tangent space.

Krull dimension.

Suppose A is a Noetherian ring, $\mathfrak{p} \subset A$ a prime ideal. Define the height $\operatorname{ht}(\mathfrak{p}) \stackrel{\text{def}}{=}$(the greatest length of the chain $\mathfrak{p} = \mathfrak{p}_d \supset \mathfrak{p}_{d-1} \supset \cdots \supset \mathfrak{p}_0$ of prime ideals). Then the Krull dimension $\dim(A) \stackrel{\text{def}}{=} \sup\limits_{\mathfrak{p} \subset A} \operatorname{ht}(\mathfrak{p})$. Make an agreement that dim(zero ring)=-1.

Clearly $\operatorname{ht}(\mathfrak{p}) = \dim(A_{\mathfrak{p}})$ since prime ideals of $A_{\mathfrak{p}}$ are in one-to-one correspondence with prime ideals in A which are contained in $\mathfrak{p}$. For the local Noetherian ring $(A, \mathfrak{m})$ it could be proved that $\dim(A) = \operatorname{ht}(\mathfrak{m}) \leq$ (minimal number of generators of $\mathfrak{m}$) $= \dim_{A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$

(this follows from the Krull's principal ideals theorem which we consider later). In particular this means that $\mathrm{ht}\,(\mathfrak{p})$ is finite. However if A is not local while still Noetherian $\dim(A)$ may be infinite, that is why we used sup instead of max in the definition above.

If the inequality turns to be an equality the local ring A is called regular local ring.

Examples. Suppose A is an ID. Then the ideal $\mathfrak{p}_0$ in the definition of $\mathrm{ht}\,(\mathfrak{p})$ is (0). In this case $\dim(A) = 0 \Leftrightarrow A$ is a field. If A is a principal ideal domain then $\dim(A) = 1$ (provided A is not a field) but the opposite is not true: there exists a class of Noetherian domains, so called Dedekind domains, which are 1-dimensional but not necessary PID; if one adds the property of being integrally closed (see below) then every Noetherian integrally closed 1-dimensional ID is a Dedekind domain.

Theorem 1.20. (Krull intersection).
Suppose A is a Noetherian ring, $I \subset \mathfrak{J}(A)$. Then $\bigcap\limits_{n\geq 1} I^n = (0)$.

Proof. Denote $K \stackrel{\mathrm{def}}{=} \bigcap\limits_{n\geq 1} I^n$. We prove that $IK = K$ then use Nakayama's Lemma. This is in fact true for arbitrary ideal I, not necessary contained in the Jacobson radical. Let $I =< x_1, \ldots, x_r >$. Consider all homogeneous polynomials $f \in A[T_1, \ldots, T_r]$ such that $f(x_1, \ldots, x_r) \in K$, let F be the ideal in $A[T_1, \ldots, T_n]$ generated by these f. Since $A[T_1, \ldots, T_r]$ is Noetherian (Hilbert's Basis) the set of polynomials f contains a finite subset $(f_1, \ldots, f_s)$ which also generates F. The polynomials f_j are homogeneous of degrees, say, d_j. Set $d \stackrel{\mathrm{def}}{=} \max(d_j)$.
Suppose $y \in K$, this, in particular, means that $y \in I^{d+1}$ hence there exists a homogeneous polynomial f of degree $d+1$ such that $f(x_1, \ldots, x_r) = y$. Using the set of generators of F just constructed one gets $f = \sum\limits_{j=1}^{s} g_j f_j$. Since f is homogeneous of degree $d+1$ one may suppose that all g_j are homogeneous of degrees $d + 1 - d_j$ (other terms in the sum cancel out). All these degrees are positive by the choice of d hence $\forall j \;\; g_j(x_1, \ldots, x_r) \in I$ thus $y \in IK$.

Remark 1. If $I \subset \mathfrak{R}(A)$ a stronger property holds. Namely, $(\mathfrak{R}(A))^n = (0)$ for some n. In fact for any ideal $I \subset A$ there exists n such that $I \supset (\sqrt{I})^n$ (choose a set of generators $\sqrt{I} =< x_1, \ldots, x_n >$, then $x_i^{d_i} \in I$ hence $(\sum a_i x_i)^{\sum d_i} \in I$, so take $n = \sum d_i$).

Remark 2. The statement of the theorem is not true for nonnoetherian rings. For example, let $X = \mathbf{R}$ with usual topology, $\mathcal{F}$ the sheaf of germs of $\mathbf{R}$-valued C^∞ - functions on X. Then $\mathcal{F}_0$ is a local ring, the maximal ideal $\mathfrak{m}$ consisting of germs $s_0 \in \mathcal{F}_0$ such that $s_0(0) = 0$. It is easy to prove that $\bigcap_{n=1}^{\infty} \mathfrak{m}^n$ consists of the germs of functions with all derivatives zero in $x = 0$ (try!). The function $\exp(-1/x^2)$ is of that kind and is not zero in either neighborhood of 0.

Primary decomposition.

Let A be any ring. A proper ideal $I \subset A$ is called primary iff the following property holds:
If $xy \in I$ then either $x \in I$ or $y \in \sqrt{I}$ (or both).
The equivalent formulation is: In the ring A/I all zero divisors are nilpotent.

Remark. The close-looking property that $(A/I)^{\mathrm{red}} \stackrel{\mathrm{def}}{=} (A/I)/\mathfrak{R}(A/I)$ is an ID) $\Leftrightarrow$ ($\mathfrak{R}(A/I)$ is a prime ideal) $\Leftrightarrow$ ($\sqrt{I}$ is prime) is strictly weaker.
Example. Suppose k is a field, $A = k[X, Y, Z]/(XY - Z^2)$, $I =< \overline{X}, \overline{Z} >^2$. Then $\sqrt{I} =< \overline{X}, \overline{Z} >$. Since $\overline{XY} = \overline{Z}^2$, $\overline{XY} \in I$. As $\overline{X} \notin I$ and $\forall n$ $\overline{Y}^n \notin I$ the ideal I is not primary while $\sqrt{I}$ is prime.

Properties of primary ideals.

1) If I is primary then $\sqrt{I}$ is the smallest prime ideal containing I. The ideal I is after that called "$\mathfrak{p}$-primary". So I is $\mathfrak{p}$-primary iff $\mathfrak{p} = \sqrt{I}$ and the property $xy \in I \Rightarrow$ either $x \in I$ or $y \in \mathfrak{p}$ holds.
Proof: exercise

2) Suppose $\sqrt{I} = \mathfrak{m}$ is maximal. Then I is $\mathfrak{m}$-primary.
Indeed, if $\mathfrak{p}$ is prime and $\mathfrak{p} \supset I$ then $\mathfrak{p} \supset \sqrt{I}$ hence $\mathfrak{p} = \sqrt{I}$ the latter being maximal. The prime ideals in A/I are in one-to-one correspondence with prime ideals in A containing I thus A/I is local with maximal ideal $\sqrt{I}/I = (\sqrt{I})^e$ which clearly coincides with $\mathfrak{R}(A/I)$. All the zero divisors in the local ring are not invertible hence lie in the maximal ideal.

3) For any $A \stackrel{\phi}{\to} B$ and $J \subset B$ primary $J^c \subset A$ is primary.
Proof: exercise.

4) Suppose $I \subset \mathfrak{p} \subset \sqrt{I}$ ($\mathfrak{p}$ *a priori* not necessary prime) and the property $xy \in I \Rightarrow$either $x \in I$ or $y \in \mathfrak{p}$ holds. Then $\mathfrak{p} = \sqrt{I}$ and I is $\mathfrak{p}$-primary.
Indeed, since the basic property holds for $\mathfrak{p}$ it also holds for $\sqrt{I}$ hence I is primary and $\sqrt{I}$ is therefore prime. It remains to check that $\mathfrak{p} = \sqrt{I}$. Let $x \in \sqrt{I}$. Then $x^n \in I$ (choose n minimal). If $n = 1$ then $x \in I \subset \mathfrak{p}$. Otherwise $x = x^{n-1} \times x$. The first factor is not in I as n is minimal hence the second factor is in $\mathfrak{p}$ by the supposed property.

5) Fix $\mathfrak{p} \subset A$ prime. A finite intersection $I = \bigcap_{i=1}^{n} I_i$ of $\mathfrak{p}$-primary ideals is primary.
Since all I_i are $\mathfrak{p}$-primary, $\mathfrak{p} = \sqrt{I_i}$ for each i hence $\sqrt{I} = \bigcap \sqrt{I_i} = \mathfrak{p}$ (see property 2 of radicals). If $xy \in I$ and $y \notin \mathfrak{p}$ then $\forall i \ x \in I_i$ thus $x \in I$.

6) If I is $\mathfrak{p}$-primary and $x \in A \setminus I$ then $(I : x)$ is $\mathfrak{p}$-primary.
If $y \in (I : x)$ then $xy \in I$. Since $x \notin I$ and I is $\mathfrak{p}$-primary, $y \in \mathfrak{p}$. This means that $\sqrt{I} = \mathfrak{p} \supset (I : x) \supset I$, so $\mathfrak{p} = \sqrt{(I : x)}$. Now $zt \in (I : x) \Rightarrow xzt \in I \Rightarrow$either $t \in \mathfrak{p}$ or $xz \in I \Rightarrow z \in (I : x)$. One concludes $(I : x)$ is $\mathfrak{p}$-primary.

Let $I \in A$ be an arbitrary ideal. Its representation in the form $I = \bigcap_{i=1}^{n} I_i$ where all I_i are primary is called a primary decomposition. The primary decomposition is called minimal iff all $\mathfrak{p}_i = \sqrt{I_i}$ are distinct and neither of I_i may be omitted (i.e neither I_i contains the intersection of the remaining ones).
Clearly if I admits some primary decomposition it also admits a minimal one (extra I_i may be deleted from the list while the I_i with the same radical may be combined via property 5)).

They say that the prime ideals $\mathfrak{p}_i = \sqrt{I_i}$ belong to I or are accociated with I.

Remark. Any prime ideal $\mathfrak{p} \supset I$ contains at least one of the $\mathfrak{p}_i$. Indeed, $\mathfrak{p} \supset \bigcap I_i \supset \prod I_i$. Being prime it therefore contains some of I_i hence also the related $\mathfrak{p}_i$.

Theorem 1.21.
Suppose $I = \bigcap_{i=1}^{n} I_i$ is a minimal primary decomposition. Let $\mathfrak{p}_i = \sqrt{I_i}$. Then the set $(\mathfrak{p}_1, \ldots, \mathfrak{p}_n)$ coincides with the set ($\sqrt{(I : x)}$ which are prime, x runs through $A \setminus I$).
Proof. Suppose $x \in A$, then $\sqrt{(I : x)} = \bigcap_{i=1}^{n} \sqrt{(I_i : x)}$. If $x \in I_i$ then $\sqrt{(I_i : x)} = (1)$ otherwise $\sqrt{(I_i : x)} = \mathfrak{p}_i$ (property 6) hence $\sqrt{(I : x)} = \bigcap_{i \ |: x \notin I_i} \mathfrak{p}_i$.

If $\sqrt{(I:x)}$ is prime then it must contain some of the $\mathfrak{p}_i$ (since it contains their product) therefore it coincides with that $\mathfrak{p}_i$. Since the prime decomposition is minimal $\forall\, i \exists x \notin \mathrm{I}_i$ such that $x \in \bigcap\limits_{j\neq i} I_j$ so that $\mathfrak{p}_i$ is the only candidate for $\sqrt{(I:x)}$.

Corollary. If I admits a primary decomposition then the set $(\mathfrak{p}_1, \ldots, \mathfrak{p}_n)$ depends only on I, not on the choice of the decomposition.

The ideal I is called irreducible if $I = J \cap K$ implies either $I = J$ or $I = K$.

Theorem 1.22. Suppose A is Noetherian

1. If $I \subset A$ is a proper ideal then there exists a decomposition $I = \bigcap\limits_{i=1}^{n} I_i$ where all I_i are irreducible.
2. Every irreducible proper ideal in A is primary.

Proof. 1. Let $\mathfrak{S} \subset$ (proper ideals of A) consist of all ideals which cannot be decomposed in that way. Suppose $\mathfrak{S}$ is nonempty. Let $I \in \mathfrak{S}$ be a maximal element (exists since A is Noetherian). $I \in \mathfrak{S} \Rightarrow I$ is not irreducible $\Rightarrow I = J \cap K$, both J and K strictly greater than $I \Rightarrow J, K \not\subset \mathfrak{S} \Rightarrow J$, K decomposable $\Rightarrow I = J \cap K$ also decomposable $\Rightarrow$ contradiction.
2. Suppose I is irreducible. Let $B = A/I$. To prove I is primary it suffices to prove that in the ring B if $xy = 0$ and $y \neq 0$ then $x \in \mathfrak{R}(B)$. Suppose $xy = 0$ and $y \neq 0$ while x is not a nilpotent, then all the ideals in the increasing chain of ideals $((0):x) \subset ((0):x^2) \subset ((0):x^3) \subset \ldots$ are nontrivial. Since B is Noetherian (as A is) the chain stabilizes, so $((0):x^d) = ((0):x^{d+1})$.
Consider the ideal $J = (y) \cap (x^d)$. We claim that $J = (0)$. Indeed, if $z \in J$ then $zx = 0$ (since z is a multiple of y) and $z = cx^d \Rightarrow cx^{d+1} = 0 \Rightarrow c \in ((0):x^{d+1}) \Rightarrow c \in ((0):x^d) \Rightarrow cx^d = 0 \Rightarrow z = 0$. This means that (0) is reducible in B hence I reducible in A which contradicts the assumption.

Remark 1. In a Noetherian ring every ideal I contains some power of its radical. Indeed, choose the finite set (x_i) of generators of $\sqrt{I}$, so that $x_i^{d_i} \in I$. Any element of $\sqrt{I}$ is of the form $\sum a_i x_i$ hence each monomial in the product of a sufficient number of the elements of that kind will contain a power of some x_i exceeding d_i. Hence all the monomials will sit in I.
In particular this means that any $\mathfrak{p}$-primary ideal contains some $\mathfrak{p}^n$ for some n. However the opposite is true only for $\mathfrak{m}$-primary ideals, $\mathfrak{m}$ maximal (i.e. if I is proper and $I \supset \mathfrak{m}^n$ then I is $\mathfrak{m}$-primary). Indeed, suppose $\mathfrak{p}$ belongs to I (recall that I is decomposable since A is Noetherian). Then $I \subset \mathfrak{p} \Rightarrow \mathfrak{m}^n \subset \mathfrak{P} \Rightarrow \mathfrak{m} \subset \mathfrak{p} \Rightarrow \mathfrak{p} = \mathfrak{m}$. Since $\mathfrak{p}$ is unique I is

$\mathfrak{p}$-primary i.e. $\mathfrak{m}$-primary.
For the general $\mathfrak{p}$ accociated with I the above is false: there may exist non-primary $I \supset \mathfrak{p}^n$. Even $\mathfrak{p}^n$ itself may be not primary. See the example after the definition of primary ideal.
Remark 2. In the minimal primary decomposition all the $\mathfrak{p}_i$ are uniquely defined, but the I_i themselves generally are not.
Remark 3. Mimimal elements in the set of primes associated with I are called isolated or minimal, others are called embedded. So $\mathfrak{p}_i$ is embedded means that there exists $\mathfrak{p}_j$ such that $\mathfrak{p}_i \supset \mathfrak{p}_j$. The name is of course related to geometry ($\mathfrak{p}_i \supset \mathfrak{p}_j \Leftrightarrow V(\mathfrak{p}_i) \subset V(\mathfrak{p}_j) \Leftrightarrow [\mathfrak{p}_i] \in \overline{[\mathfrak{p}_j]}$). The isolated associated primes correspond to irreducible components of $V(I)$ while embedded ones correspond to their irreducible subvarieties. The isolated associated primes may be described after I as follows (A needs not to be Noetherian , but I should be decomposable). They are minimal elements in the set of prime ideals containing I. Indeed, we know that $\mathfrak{p} \supset I \Rightarrow \mathfrak{p} \supset \mathfrak{p}_i$ for some i (see Remark before Theorem 1.21).

Theorem 1.23.
If $\mathfrak{p}_i$ is isolated then I_i is uniquely defined.
Proof. We start with the lemma.
Lemma. Consider $A \xrightarrow{i_S} S^{-1}A = B$. Suppose $I \subset A$ is a $\mathfrak{p}$-primary ideal. If $S \cap \mathfrak{p} \neq \emptyset$ then I^e is trivial, otherwise $I^{ec} = I$.
Indeed, if $s \in S \cap (\mathfrak{p} = \sqrt{I})$ then $s^n \in S \cap I$ for some n hence $S^{-1}I$ is trivial as s^n is invertible in B. If the intersection is void then $\forall\, s\ s \notin \mathfrak{p}$. Since I is $\mathfrak{p}$-primary this means that $as \in I \Rightarrow a \in I$, so $I^{ec} = I$.
We now derive the theorem. Since $\mathfrak{p}_i$ is isolated $\forall\, j\ \ \mathfrak{p}_i \not\supset \mathfrak{p}_j \Rightarrow \mathfrak{p}_j \cap A \setminus \mathfrak{p}_i \neq \emptyset$. Finite intersection commutes with extension (property 5 of i_S), so $I = \bigcap I_i \Rightarrow I^e = \bigcap (I_i)^e \Rightarrow I^{ec} = \bigcap (I_i)^{ec} = I_i$

Integral ring extensions.

Let $A \xrightarrow{\phi} B$ be a homomorphism of the rings.

The ring B is called finite over A iff B is a finitely generated A-module ($a \in A$ acts on B via multiplication with $\phi(a)$).

The element $x \in B$ is called integral over A if it satisfies some equation of the form $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ where all $a_i \in \phi(A)$. The ring B is called integral over A if all $x \in B$ are integral over A.

We often will restrict ourselves with the inclusions $A \hookrightarrow B$ identifying A with its image. Hopefully the proofs below still work in the general case provided one replaces "A" with "the image of A in B".

Properties of integral elements/extensions (we suppose $A \hookrightarrow B$).

1) x is integral over $A \Leftrightarrow$ there exists a faithful A[x]-submodule $N \subset B$ which is finitely generated as an A-module. (a module N is called faithful iff its annihilator equals zero). If x is integral over A then consider the A-submodule $N =< 1, x, x^2, \ldots, x^{n-1} > \subset B$. Clearly all the powers of x are in N hence $N = A[x]$ (obviously faithful). Conversely, let $N \subset B$ be a finitely generated A-submodule, say, $N =< e_1, \ldots, e_n >$. Since N is an $A[x]$-module $xN \subset N$. This means that there is a system of n linear equations $xe_i = \sum_{i=1}^{n} a_{ij} e_j$ with $a_{ij} \in A$. Consider the $(n \times n)$-matrix C with entries $c_{ij} = a_{ij}$ for $i \neq j$ and $c_{ii} = a_{ii} - x$. If E is a column with entries e_J then the equations above lead to $CE = 0$. This implies $(\det C)e_j = 0$ for all j (exercise in linear algebra) so that $(\det C)N = 0$. But N is $A[x]$-faithful hence $\det C = 0$. Since $\det C$ is a monic polynomial in x up to a sign x is integral over A.