Commutative Algebra.

History: David Hilbert - a series of papers on invariant theory, 1888-1891

Example: Let k be a field, $k[X_1, .., X_n]$ a polynomial ring. Let Σ be the symmetric group on $\{1, .., n\}$. Σ acts on $k[X_1, .., X_n]$ by permuting the variables.
So, for $g \in \Sigma$, $f \in k[X_1, .., X_n]$, have $(gf)(X_1, .., X_n) = f(X_{g^{-1}(1)}, .., X_{g^{-1}(n)})$
Σ acts via ring automorphisms. Look for the ring of invariants, ie, the set of polynomials fixed under the action of Σ.
This is the ring of symmetric polynomials, call it S.
Let $f_1(X_1, .., X_n) = X_1 + \cdots + X_n$
$f_2(X_1, .., X_n) = \sum_{i<j} X_i X_j$
$f_n(X_1, .., X_n) = X_1 \cdots X_n$.
S is generated as a ring by $f_1, .., f_n$, and so there is a canonical map from $k[Y_1, .., Y_n] \to S$, $Y_i \mapsto f_i$. This is a ring isomorphism.
Hilbert showed that this ring of invariants is finitely generated, and similarly for many other groups.

Hilbert proved 4 major theorems: (i) Basis theorem
(ii) Nullstellensatz.
(iii) polynomial nature of the Hilbert function
(iv) Syzygy theorem. (beginning of the homological theory of polynomial rings).

History: 1921. Emmy Noether extracted the key property required by Hilbert's Basis Theorem, namely that a (commutative) ring is Noetherian if every ideal is finitely generated.

Basis Theorem: Let R be a commutative Noetherian ring. Then the ring $R[X]$ of polynomials in one variable is also Noetherian.

Corollary: Let k be a field. Then $k[X_1, .., X_n]$ is Noetherian.

Noether developed the theory of ideals in Noetherian rings.

Link between Commutative Algebra and Algebraic Geometry.

Given $f \in \mathbb{C}[X_1, .., X_n]$, there is a function $\mathbb{C}^n \to \mathbb{C}$, $(a_1, .., a_n) \mapsto f(a_1, .., a_n)$, a polynomial function. Different polynomials yield different functions, and so $\mathbb{C}[X_1, .., X_n]$ may be viewed as the ring of polynomial functions on complex affine n-space.
For a subset $I \subset \mathbb{C}[X_1, .., X_n]$, define the set of common zeroes, $Z(I)$, to be

$Z(I) = \{(a_1,..,a_n) \in \mathbb{C}^n : f(a_1,..,a_n) = 0 \ \forall f \in I\}$, an algebraic subset of $\mathbb{C}^n$.

Remark: (i) one can replace I by the ideal generated by I and get the same algebraic set. Similarly, replacing an ideal by a generating set of the ideal leaves the algebraic set unchanged.
Basis theorem therefore implies that any algebraic set is the set of common zeroes of a finite set of polynomials.

(ii) $\bigcap_j Z(I_j) = Z(\sum I_j)$
$\bigcup_{j=1}^n Z(I_j) = Z(\prod_{j=1}^n I_j)$, (the product of ideals), for an ideal I_j.
So, we may define a topology on $\mathbb{C}^n$ with closed sets = algebraic sets.
This is the Zariski topology; it is coarser than the usual classical topology on $\mathbb{C}^n$.

For a subset $X \subset \mathbb{C}^n$, we can define $I(X) = \{f \in \mathbb{C}[x_1,..,x_n] : f(a_1,..,a_n) = 0 \ \forall (a_1,..,a_n) \in X\}$.
This is an ideal of $\mathbb{C}[x_1,..,x_n]$, and it is radical, ie if $f^n \in I(X)$, some $n \geq 1$, then $f \in I(X)$.

Nullstellensatz: The correspondance $\{I \to Z(I) \atop I(X) \leftarrow X\}$ gives a bijection between the radical ideals of $\mathbb{C}[x_1,..,x_n]$ and the algebraic subsets of $\mathbb{C}^n$.

1. Noetherian Rings: definition and examples.

R, a commutative ring with a 1.

(1.1): Let M be a (left) R-module. The following are equivalent:
(i) All submodules of M, including itself, are finitely generated. (fg).
(ii) Ascending chain condition (ACC): there are no strictly increasing infinite chains of submodules.
(iii) Maximum condition on submodules: any non-empty set $\mathcal{S}$ of submodules of M has a maximal element L. Ie, if $L \leq L'$, $L' \in \mathcal{S}$, then $L = L'$.

Proof: (i) $\Rightarrow$ (ii): Suppose there is a strictly ascending chain: $N_1 \subsetneq N_2 \subsetneq N_3 \subsetneq \cdots$
Let $N = \bigcup N_i$. (i) $\Rightarrow$ N is fg, by $m_1,..,m_s$, say. Each m_i lies in some N_{j_i}. Set $s = \max j$, then $N \subseteq N_s$ - $\#$

(ii) $\Rightarrow$ (iii): Assume (ii). Pick $M_1 \in \mathcal{S}$. If it is maximal, we're done. If not, there is $M_2 > M_1$. If M_2 maximal, done, else there is $M_3 > M_2$. Etc...
(ii) $\Rightarrow$ this process must stop.

(iii) $\Rightarrow$ (i): Let $N \subset M$ be a submodule and let $\mathcal{S}$ be the collection of its fg submodules. Observe it is non-empty: the zero submodule is in $\mathcal{S}$.
(iii) $\Rightarrow$ $\mathcal{S}$ has a maximal member, L.
Claim $L = N$: if $x \in N$, then $L + Rx \in \mathcal{S}$. Maximality of L ensures $x \in L$.

Definition: An R-module satisfying (i), (ii) or (iii) is called **Noetherian**.

(1.2): Let N be a submodule of M. Then M is Noetherian iff N and M/N are.

Proof: ($\Rightarrow$): Suppose M is Noetherian, so all its submodules are fg. This property is inherited by N. Submodules of M/N are all of the form Q/N where Q is a submodule of M containing N. If M is Noetherian, then Q is fg, by $m_1, \dots, m_r$, say. Then $m_1+N, \dots, m_r+N$ generate Q/N.

($\Leftarrow$): Suppose N and M/N are Noetherian. Suppose $L_1 < L_2 < L_3 < \cdots$ is a strictly ascending chain of submodules of M. Set $X_i = (L_i+N)/N$, $N_i = L_i \cap N$. These give ascending chains of submodules of M/N and N respectively. Neither of these chains can contain infinitely many strict inequalities. Thus, $\exists\, s$ such that $X_i = X_s$, $N_i = N_s$ $\forall\, i \geq s$. So $L_i + N = L_s + N$, $N_i = N_s$ $\forall i \geq s$. Pick $l \in L_i$. Then $l + N \in (L_s + N)/N$. So, there is $l' \in L_s$ such that $l - l' \in N \cap L_i = N \cap L_s$. So $l \in L_s$. Thus $L_i = L_s$ for $i \geq s$ - $\ast$.

(1.3): If M, N are R-modules, then $M \oplus N$ is Noetherian iff M and N are Noetherian.

Proof: $M \cong (M \oplus N)/N$. Apply (1.2).

(1.4): If $M_1, \dots, M_n$ are R-modules, then $M_1 \oplus \cdots \oplus M_n$ is Noetherian iff each M_i is.

Proof: (1.3) and induction on n.

(1.5): If M is Noetherian then any module image is Noetherian.

Proof: Have $\theta: M \to N$, so $\operatorname{Im}\theta \cong M/\ker\theta$. Apply (1.2)

(1.6): Suppose M can be expressed as a sum of finitely many submodules, not necessarily as a direct sum, $M = M_1 + \cdots + M_n$, then M is Noetherian iff each M_i is.

Proof: The M_i are submodules, and hence (1.2) says that they are Noetherian if M is. Also, one can define a map: $M_1 \oplus \cdots \oplus M_n \to M$, $(m_1, \dots, m_n) \mapsto m_1 + \cdots + m_n$. Apply (1.4), (1.5) to get that if the M_i are Noetherian then M is.

Definition: A ring is **Noetherian** if it is Noetherian as a (left) R-module. Observe that the submodules are the ideals.

Examples: (i) Fields.

(ii) principal ideal domains, such as $k[X]$ where k is a field; $\mathbb{Z}$.

(iii) $\{q \in \mathbb{Q} : q = m/n$ where $p \nmid n$, fixed prime $p\}$. This is a **Localisation** of $\mathbb{Z}$. Localisations of Noetherian rings are Noetherian.

(iv) $k[X_1, X_2, \dots]$, with infinitely many indeterminates, is not Noetherian. There is a chain of ideals: $(X_1) < (X_1, X_2) < (X_1, X_2, X_3) < \cdots$

(v) $k[X_1, \dots, X_n]$ is Noetherian - corollary of Basis Theorem.

(vi) $k[[X]]$, formal power series ring, is Noetherian.

(1.7): Let R be a Noetherian ring. Then any f.g. R-module is Noetherian.

Proof: $M = Rm_1 + \cdots + Rm_n$. Observe that there is an R-module map: $R \to Rm_i$; $r \mapsto rm_i$, and so Rm_i is Noetherian by (1.5). So by (1.6), M is Noetherian.

(1.8) - Hilbert's Basis Theorem: Let R be a Noetherian ring. Then $R[X]$ is Noetherian.

Proof: We prove that any ideal is f.g. Let I be an ideal. Define $I(n)$ to be the set of elements of I of degree $\leq n$. $I(n) \neq \phi$, as $0 \in I(n)$. $I(0) \subseteq I(1) \subseteq I(2) \subseteq \ldots$

Let $R(n)$ be the set of coefficients of X^n appearing in elements of $I(n)$.

Claim: $R(n)$ is an ideal of R, and $R(n) \subseteq R(n+1)$.

Proof: Take $a, b \in R(n)$. There are polynomials $f(x) = aX^n +$ lower order terms, $g(x) = bX^n +$ lower order terms, $\in I$. But I is an ideal and so $f \pm g \in I$, $rf \in I$ if $r \in R$ and $Xf \in I$. So $a \pm b \in R(n)$, $ra \in R(n)$, and $a \in R(n+1)$.

But R is Noetherian, and so the ascending chain $R(0) \subseteq R(1) \subseteq \cdots$ terminates, say $R(n) = R(N)$ $\forall n \geq N$. Each $R(n)$ is a f.g. ideal of R. Say, $R(n) = Ra_{n,1} + \cdots + Ra_{n,m_n}$. There are polynomials $f_{n,m}(x) = a_{n,m}X^n +$ lower order terms $\in I$.

The set $\{f_{n,m}(x) : 0 \leq n \leq N,\ 1 \leq m \leq m_n\}$ is finite.

Claim: This generates I.

Proof: By induction on the degree of $f(x) \in I$.

(i) $\deg f = 0$. $f(x) = a$, say. But $I(0) = R(0) = Ra_{0,1} + \cdots + Ra_{0,m_0}$. But $f_{0,m}(x) = a_{0,m}$, so a lies inside the ideal generated by $f_{n,m}(x)$.

(ii) Assume $\deg f = n > 0$ and that the claim is true for polynomials of smaller degree.

(a) $n \leq N$: $f(x) = aX^n +$ lower order terms. $a \in R(n)$, so $a = \sum_m r_{n,m} a_{n,m}$ for some $r_{n,m}$. Define $g(x) = \sum r_{n,m} f_{n,m}(x) = aX^n +$ lower order terms. Then $f(x) - g(x) \in I$ and is of smaller degree. Apply inductive hypothesis.

(b) $n > N$: $f(x) = aX^n +$ lower order terms. $a \in R(n) = R(N)$, $a = \sum r_{N,m} a_{N,m}$. Define $g(x) = \sum X^{n-N} r_{N,m} f_{N,m}(x) = aX^n +$ lower order terms. $f(x) - g(x) \in I$ and is of lower degree. Apply inductive hypothesis.

Remark: In computation, one needs an extra property satisfied by the generating set. A generating set with this property is a Gröbner basis.

(1.9): Finitely generated rings are Noetherian.

Proof: Such rings are images of polynomial rings. If R is generated by $r_1, \ldots, r_n$ then there is a map: $\mathbb{Z}[X_1, \ldots, X_n] \to R$; $X_i \mapsto r_i$. Use (1.5) and (1.8).

Examples of such rings are the group algebras of free abelian groups of finite rank. If A is free abelian, then $\mathbb{Z}A$ has elements $\sum \lambda_a a$, $\lambda_a \in \mathbb{Z}$, only finitely many λ_a non-zero. Addition: $\sum \lambda_a a + \sum \mu_a a = \sum (\lambda_a + \mu_a) a$. Multiplication: $(\sum \mu_b b)(\sum \nu_c c) = \sum_a \left(\sum_{bc=a} \mu_b \nu_c \right) a$. If A is generated as a group by $g_1, \ldots, g_n$, then the group algebra is generated as a ring by $g_1, g_1^{-1}, g_2, g_2^{-1}, \ldots, g_n, g_n^{-1}$.

(1.10): Cohen's Theorem: If every prime ideal in a ring R is f.g., then R is Noetherian.

Proof: Suppose R is not Noetherian and consider the family of non-f.g. ideals, call it $\mathcal{S}$. By assumption, $\mathcal{S}$ is not empty. Wish to apply Zorn's Lemma: if every chain of ideals in $\mathcal{S}$ has an upper bound in $\mathcal{S}$, and $\mathcal{S}$ is non-empty, then $\mathcal{S}$ has a (not necessarily unique) maximal member, I.

We observe that (union of) a chain of non-f.g. ideals is not f.g.: if it were, then the finite number of generators would all lie in some term in the chain, and therefore that term would itself be f.g. - a contradiction.

Now, I is a non-f.g. ideal but all ideals containing it f.g.

Claim: I is prime.

Proof: Suppose we have $a \notin I$, $b \notin I$, but $ab \in I$. Then, $I + Ra \supsetneq I$. So $I + Ra$ is f.g., by $i_1 + r_1 a, \ldots, i_n + r_n a$, say. Consider $J = \{r : ra \in I\}$. $b \in J$, so $J \supsetneq I$. So J is f.g. We prove that $I = Ri_1 + \cdots + Ri_n + Ja$, and hence I is f.g. $\#$.

So, take $t \in I$. Then $t \in I + Ra$, so $t = u_1(i_1 + r_1 a) + \cdots + u_n(i_n + r_n a)$ for some $u_i \in R$. So $t = u_1 i_1 + \cdots + u_n i_n + \underbrace{(u_1 r_1 + \cdots + u_n r_n)}_{\in J} a$, so done.

(1.11): If R is Noetherian then $R[[X]]$ is Noetherian.

Proof: Version (i): as in basis theorem, but consider $R(n)$ = set of trailing coefficients a_n for elements $a_n X^n +$ higher order terms $\in I \cap R[[X]] X^n$.

So one has $R(0) \subseteq R(1) \subseteq \cdots$ (See example sheet).

Version (ii): Use Cohen's Theorem and:

(1.12): Let P be a prime ideal of $R[[X]]$, and θ the map $R[[X]] \to R$; $X \mapsto 0$. Then P is f.g. iff $\theta(P)$ is a f.g. ideal of R.

Proof: Clearly, if P is f.g. then $\theta(P)$ is f.g. Suppose $\theta(P) = Ra_1 + \cdots + Ra_n$.

Case (i): if $X \in P$ then P is generated by $a_1, \ldots, a_n$ and X.

Case (ii): if $X \notin P$, let $f_1, \ldots, f_n$ be power series with constant term $a_1, \ldots, a_n$, in P respectively. We prove $f_1, \ldots, f_n$ generate P. Take $g \in P$, $g = b +$ higher terms. But $b = \sum b_i a_i$, so $g - \sum b_i f_i = g_1 X$, some power series g_1. So $g_1 X \in P$. But P is a prime ideal and so $g_1 \in P$. Similarly, $g_1 = \sum c_i f_i + g_2 X$, $g_2 \in P$. Continuing gives $h_1, \ldots, h_n \in R[[X]]$, $h_i = b_i + c_i X + \cdots$, satisfying $g = h_1 f_1 + \cdots + h_n f_n$.

2. Ideal Structure of Noetherian Rings

Rings are commutative with a 1.

(2.1): The set of nilpotent elements $N(R)$ of R forms an ideal and $R/N(R)$ has no non-zero nilpotent elements.

Proof: If $x \in N(R)$ then $x^m = 0$, some m, and so $(rx)^m = 0$, hence $rx \in N(R)$. If x and $y \in N(R)$, then $x^m = 0$, $y^n = 0$, some m, n. Consider $(x+y)^{m+n-1}$. Expanding binomially gives terms $\lambda x^s y^t$ where $s + t = n + m - 1$, so either $s \geq m$ or $t \geq n$. So all terms are 0, so $x + y$ is nilpotent.

If $x+N$ is nilpotent then $(x+N)^m = N$ for some m, and so $x^m \in N$, and hence x^m is nilpotent. Thus x is nilpotent.

Definition: $N(R)$ is the nilradical of R.

[2.2]: $N(R)$ is the intersection of all the prime ideals of R.

Proof: Let $I = \bigcap_{P, \text{Prime}} P$. If $x \in N$ then $x^m = 0$, so $x^m \in P$ for all primes P. So $x \in P$. Thus $x \in I$, thus $N \subseteq I$.

Suppose x is not nilpotent. Set S = family of ideals J such that for $n > 0$, $x^n \notin J$. S is non-empty as $0 \in S$. A union of a chain of ideals in S is also in S. Zorn's Lemma $\Rightarrow$ there is a maximal member J_i of S. We prove that J_i is prime. Suppose $yz \in J_i$, $y \notin J_i$, $z \notin J_i$. So, ideals $J_i + Ry$, $J_i + Rz$ contain powers of x. So, $x^m \in J_i + Ry$, $x^n \in J_i + Rz$, and hence $x^{m+n} \in J_i + Ryz = J_i$ ⚠. So $I \subseteq N$.

Definition: The radical $\sqrt{I}$ of an ideal I is $\{r \in R$: some power ≥ 1 of r lies in $I\}$.

Thus, $\sqrt{I}/I = N(R/I)$ and $\sqrt{I} = \bigcap_{\text{Prime } P \supseteq I} P$.

Definition: The Jacobson radical $J(R)$ of R is the intersection of all the maximal ideals.

$N(R) \subseteq J(R)$.

Artinian Rings.

Definition: A (commutative) ring is Artinian if it does not contain an infinite strictly descending chain of ideals. Or, equivalently, an non-empty set of ideals has a minimal member.

An R-module is Artinian if it satisfies the analogous properties for submodules.

Examples: (i) $\mathbb{Z}/p\mathbb{Z}$.

(ii) $k[x]/(f)$, $f \neq 0$, k a field.

(iii) $k[X]$ is not Artinian, for we have $(x) > (x^2) > \dots$

Reminder: I is prime $\Leftrightarrow$ $ab \in I$ implies $a \in I$ or $b \in I$.

$\Leftrightarrow$ R/I is an integral domain.

$\Leftrightarrow$ $I_1 I_2 \subseteq I$ implies either $I_1 \subseteq I$ or $I_2 \subseteq I$.

[2.3]: If R is Artinian then every prime ideal is maximal.

Proof: Let P be prime and $x \notin P$. By the descending chain condition, [d.c.c.], $(x) \supseteq (x^2) \supseteq \cdots$ is not strict. So, $(x^n) = (x^{n+1})$ for some n, and so $x^n = yx^{n+1}$, some y. Thus $x^n(1-xy) = 0 \in P$. But $x^n \notin P$ as P is prime. So $1 - xy \in P$.

Thus $y + P$ is the inverse of $x + P$ in R/P. So R/P is a field, hence P is maximal.

Corollary: $J(R) = N(R)$ for Artinian rings R.

(2.4): An Artinian ring contains only finitely many maximal ideals.

Proof: Consider the set of ideals of the form $P_1 \cap \cdots \cap P_n$ for some n, with P_i maximal. (There must be a maximal ideal by Zorn's Lemma). This set has a minimal member (by Artinian property), $P_1 \cap \cdots \cap P_n$, say. Let P be a maximal ideal, and consider $P \cap P_1 \cap \cdots \cap P_n$. Minimality implies $P \cap P_1 \cap \cdots \cap P_n = P_1 \cap \cdots \cap P_n$.
So $P_1 \cdots P_n \leq P_1 \cap \cdots \cap P_n \leq P$. But P is prime, and so some $P_i \leq P$. But P_i is maximal, so $P_i = P$.

Corollary: A radical ideal in an Artinian ring is the intersection of finitely many maximal ideals. (Uses 2.2).

(2.5): In an Artinian ring R, $N(R)$ is a nilpotent ideal.

Proof: Write $N = N(R)$ and consider $N \geq N^2 \geq \cdots$. It must terminate, with $N^k = N^{k+1} = \cdots$, $= I$, say. Suppose $I \neq 0$ and aim for a contradiction. Consider $\mathcal{S}$ = family of ideals J with $IJ \neq 0$. $\mathcal{S}$ is non-empty: $I \in \mathcal{S}$. Any chain of members of $\mathcal{S}$ has a lower bound, namely the intersection of the terms in the chain, in $\mathcal{S}$. This intersection is actually a term of the chain by the Artinian property. Zorn yields a minimal member J_1 of $\mathcal{S}$. There is $x \in J_1$ such that $Ix \neq 0$. So $I(x) \neq 0$ and so $(x) \in \mathcal{S}$. The minimality of J_1 implies $J_1 = (x)$.
Observe $I(Ix) = I^2 x = Ix \neq 0$, and so $Ix \in \mathcal{S}$. Minimality gives $Ix = (x) = J_1$.
Hence there is $y \in I$ such that $yx = x$. So $x = yx = y^2 x = \cdots$ By $y \in I < N$, and so y is nilpotent. So $y^n = 0$, some n, and so $x = 0$ - ⁂.

(2.6): An Artinian ring is Noetherian.

Proof: By (2.4), R has finitely many maximal ideals, $P_1, \ldots, P_n$, and $P_1 \cap \cdots \cap P_n = N = N(R)$.
By (2.5), $N^k = 0$ for some k. So $(P_1 \cdots P_n)^k \leq N^k = 0$. So we have a product of maximal ideals equal to zero. Write $(P_1 \cdots P_n)^k = Q_1 \cdots Q_m$, with $Q_j = P_{i(j)}$, some i. Consider $R > Q_1 \geq Q_1 Q_2 \geq Q_1 Q_2 Q_3 \geq \cdots = 0$.
Each factor $Q_1 \cdots Q_j / Q_1 \cdots Q_{j+1}$ is annihilated as an R-module by Q_{j+1}, and so it may be viewed as an R/Q_{j+1}-module.
Observe $R/Q_{j+1} = k_{j+1}$ is a field, as Q_{j+1} maximal.
Thus the factor is a k_{j+1}-vector space whose subspaces correspond to the ideals of R lying between $Q_1 \cdots Q_j$ and $Q_1 \cdots Q_{j+1}$.
So the d.c.c. for ideals of R translates to give the d.c.c. for subspaces of the vector space $Q_1 \cdots Q_j / Q_1 \cdots Q_{j+1}$. So the vector space is finite dimensional, for if it were infinite dimensional there would be an infinite linearly independent set $x_1, x_2, \ldots$, and subspaces given by $\{x_1, x_2, \ldots\}$, $\{x_2, x_3, \ldots\}$, ... would give an infinite strictly descending chain.
The factors, being finite dimensional, also satisfy the a.c.c. on subspaces, and thus $Q_1 \cdots Q_j / Q_1 \cdots Q_{j+1}$ is a Noetherian R-module.
Apply (1.2) and induction to get that R is Noetherian.

(2.7): If R is Noetherian, then every ideal contains a power of its radical. In particular, $N(R)$ is nilpotent.

Proof: Suppose $x_1, \dots, x_k$ generate $\sqrt{I}$. So, $x_i^{n_i} \in I$, some n_i. Let $n = \sum (n_i - 1) + 1$. Then $(\sqrt{I})^n$ is generated by products $x_1^{r_1} \cdots x_k^{r_k}$ with $\sum r_i = n$. Some $r_i \geq n_i$ and so each product is in I. Hence $(\sqrt{I})^n \subseteq I$.

(2.8): If R is Noetherian, a radical ideal is the intersection of finitely many primes.

Proof: Suppose not, and consider the non-empty set of radical ideals not of this form. Take I to be a maximal member.

Claim: I is prime.

Proof: Suppose I is not prime. Let $J_1 J_2 \subseteq I$, but $J_1 \not\subseteq I$, $J_2 \not\subseteq I$. By replacing J_i by $J_i + I$ we may assume $I \subsetneq J_1$, $I \subsetneq J_2$.
The maximality of I implies $\sqrt{J_1} = Q_1 \cap \cdots \cap Q_m$, $\sqrt{J_2} = Q_1' \cap \cdots \cap Q_n'$.
Set $J = \sqrt{J_1} \cap \sqrt{J_2} = Q_1 \cap \cdots \cap Q_m \cap Q_1' \cap \cdots \cap Q_n'$. So $J^{n_1} \subseteq J_1$, $J^{n_2} \subseteq J_2$, some n_1, n_2, using (2.7). So $J^{n_1+n_2} \subseteq J_1 J_2 \subseteq I$. But I is radical, so $J \subseteq I$.
But all of Q_i, Q_j' contain I, so $J = I$ — #.

Now suppose by (2.8) that our radical ideal $I = P_1 \cap \cdots \cap P_m$, P_i prime. We may remove any P_i from the list if it contains one of the others, and so we may assume that $P_i \not\subseteq P_j$ for any i, j. If P prime with $I \subseteq P$, then $P_1 \cdots P_n \subseteq P_1 \cap \cdots \cap P_n = I \subseteq P$, so some $P_i \subseteq P$.

Definition: The minimal primes over an ideal I of a Noetherian ring are those primes P such that if P' is prime and $I \subseteq P' \subseteq P$, then $P' = P$.

Observe that the P_i above are minimal over I.

(2.9): Let I be an ideal over a Noetherian ring. Then $\sqrt{I}$ is the intersection of the minimal primes over I, and I contains a finite product of the minimal primes over I.

Proof: Each (minimal) prime over I contains $\sqrt{I}$. So the primes minimal over I are precisely the minimal ones over $\sqrt{I}$. The discussion above says that $\sqrt{I}$ is the intersection of these. Thus their product lies in $\sqrt{I}$, and (2.7) gives the last statement.

Example (iii) of the list of examples of Noetherian rings is a ring with prime ideals (0) and (p), and maximal ideal (p). $J(R) = \bigcap \{\text{maximals}\} = (p)$, $N(R) = \bigcap \{\text{primes}\} = (0)$.

Recall the Nullstellensatz: bijection: $\{\text{radical ideals of } \mathbb{C}[x_1, \dots, x_n]\} \longleftrightarrow \{\text{algebraic sets} \subset \mathbb{C}^n\}$.
$(a_1, \dots, a_n)$ is a common zero of all $f \in I$, a radical ideal, iff $I \subseteq (x_1 - a_1, \dots, x_n - a_n)$.
Observe this latter ideal is maximal; it's the kernel of the map $\mathbb{C}[x_1, \dots, x_n] \to \mathbb{C}$, $x_i \mapsto a_i$.

Now consider $\bigcap_{(a_1,\dots,a_n) \text{ is a common zero of all } f \in I} (X_1 - a_1, \dots, X_n - a_n)$. This is radical.

The bijective statement in Nullstellensatz implies that this radical ideal is the same as I. Thus $I = \bigcap (X_1 - a_1, \dots, X_n - a_n)$ = intersection of maximals. Moreover, all maximals are of the form $(X_1 - a_1, \dots, X_n - a_n)$.
Also, for any ideal J_1 of $\mathbb{C}[X_1, \dots, X_n]$, $N(\mathbb{C}[X_1, \dots, X_n]/J_1) = J(\mathbb{C}[X_1, \dots, X_n]/J_1)$.

3. Localisation

All rings R are commutative with a 1.

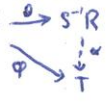
Let S be a <u>multiplicatively closed</u> subset of R, ie S is (i) closed under multiplication, and (ii) $1 \in S$.

Define a relation '$\equiv$' on $R \times S$ by: $(r_1, s_1) \equiv (r_2, s_2)$ iff $(r_1 s_2 - r_2 s_1)x = 0$, some $x \in S$.
This is an equivalence relation: (i) reflexive, and (ii) symmetric are clear.
(iii) transitive: take $(r_1, s_1) \equiv (r_2, s_2)$, $(r_2, s_2) \equiv (r_3, s_3)$. So, $\exists\ x, y \in S$ such that $(r_1 s_2 - r_2 s_1)x = 0$, $(r_2 s_3 - r_3 s_2)y = 0$. (first) $\times s_3 y$ - (second) $\times s_1 x$ gives $(r_1 s_3 - r_3 s_1) s_2 xy = 0$, and S is multiplicatively closed, so $s_2 xy \in S$.

Denote the set of equivalence classes by $S^{-1}R$, where the equivalence class of (r,s) is written r/s. $S^{-1}R$ can be made into a ring:
addition: $[r_1/s_1] + [r_2/s_2] = (r_1 s_2 + r_2 s_1)/s_1 s_2$, multiplication: $(r_1/s_1)(r_2/s_2) = (r_1 r_2)/(s_1 s_2)$.
$\exists$ ring homomorphism $\theta: R \to S^{-1}R$, $r \mapsto r/1$

<u>Examples</u>: (i) fraction field of an integral domain.
(ii) $S^{-1}R$ is the zero ring iff $0 \in S$.
(iii) If I is an ideal of R then can take $S = 1 + I = \{1 + r : r \in I\}$.
(iv) If P is a prime ideal then let $S = R \setminus P$. This is multiplicatively closed as P is prime. Write R_P for $S^{-1}R$ in this case. The process of passing from R to R_P is called <u>localisation at P</u>.

$S^{-1}R$ has a universal property:

<u>(3.1)</u>: Let $\varphi: R \to T$ be a ring homomorphism with $\varphi(s)$ a unit in T $\forall\ s \in S$.
Then $\exists$ a unique ring homomorphism $\alpha: S^{-1}R \to T$ such that


commutes.

<u>Proof</u>: <u>Uniqueness</u>: Suppose α exists, $\alpha: S^{-1}R \to T$ with $\varphi = \alpha \circ \theta$.
Then, $\alpha(r/1) = \alpha(\theta(r)) = \varphi(r)$ $\forall r$, $\alpha(1/s) = \alpha((s/1)^{-1}) = (\alpha(s/1))^{-1} = \varphi(s)^{-1}$, using that $\varphi(s)$ is a unit. So $\alpha(r/s) = \varphi(r)(\varphi(s))^{-1}$, so α is uniquely determined.
<u>Existence</u>: Let $\alpha(r/s) = \varphi(r)(\varphi(s))^{-1}$. Must show this gives a well-defined map.
Suppose $(r_1/s_1) = (r_2/s_2)$. Then $\exists\ x \in S$ with $(r_1 s_2 - r_2 s_1)x = 0$. So $(\varphi(r_1)\varphi(s_2) - \varphi(r_2)\varphi(s_1))\varphi(x) = 0$.
But $\varphi(x)$ is a unit, so $\varphi(r_1)\varphi(s_2) = \varphi(r_2)\varphi(s_1)$, so $\varphi(r_1)(\varphi(s_1))^{-1} = \varphi(r_2)(\varphi(s_2))^{-1}$.

Let M be a (left) R-module, S multiplicatively closed $\subseteq R$.
Define '$\equiv$' on $M \times S$ by: $(m_1, s_1) \equiv (m_2, s_2)$ iff $x(s_2 m_1 - s_1 m_2) = 0$ for some $x \in S$.
This is an equivalence relation, with m/s an equivalence class. The set of equivalence classes, $S^{-1}M$, is an $S^{-1}R$-module.

Example: $S = R \setminus P$, where P is a prime ideal. In this case, write M_P for $S^{-1}M$.
The elements r/s with $r \in P$ form an ideal of R_P; this is the unique maximal ideal. (For, if r/s is such that $r \notin P$ then $r \in S$, so r/s is a unit in R_P).

A ring with a unique maximal ideal is called Local.

Example: (i) $R = \mathbb{Z}$, $P = (p)$, p prime. $R_p = \{ m/n : p \nmid n \} \subset \mathbb{Q}$.
(ii) $R = k[X_1, \dots, X_n]$, k a field, $P = (X_1 - a_1, \dots, X_n - a_n)$. R_P is a subring of $k(X_1, \dots, X_n)$, the field of rational functions on k^n. R_P is the subring of rational functions defined at $(a_1, \dots, a_n)$ and the unique maximal ideal consists of those functions with value 0 at $(a_1, \dots, a_n)$.

If $\theta : M_1 \to M$ is a R-module map, then $S^{-1}\theta : S^{-1}M_1 \to S^{-1}M$, $m_1/s \mapsto \theta(m_1)/s$ is an $S^{-1}R$-module map.
A sequence of R-modules $M_0 \to M_1 \to \cdots \xrightarrow{\theta} M_i \xrightarrow{\varphi} \cdots$ is exact at M_i if $\operatorname{im}\theta = \ker\varphi$.
A short exact sequence is of the form $0 \to M_1 \xrightarrow{\theta} M \xrightarrow{\varphi} M_2 \to 0$ with exactness at M_1, M, M_2, and so θ is injective, φ is surjective. So $M_2 \cong M/M_1$.

Localisation is exact, ie:

(3.2): If $M_1 \xrightarrow{\theta} M \xrightarrow{\varphi} M_2$ is exact at M, then $S^{-1}M_1 \xrightarrow{S^{-1}\theta} S^{-1}M \xrightarrow{S^{-1}\varphi} S^{-1}M_2$ is exact at $S^{-1}M$.
Proof: Since $\ker\varphi = \operatorname{im}\theta$, we have $\varphi \circ \theta = 0$. So, $(S^{-1}\varphi) \circ (S^{-1}\theta) = S^{-1}(0) = 0$, so $\operatorname{im}(S^{-1}\theta) \subseteq \ker(S^{-1}\varphi)$.
Now suppose $m/s \in \ker(S^{-1}\varphi) \subset S^{-1}M$. So $\varphi(m)/s = 0$ in $S^{-1}M_2$, and there is $t \in S$ with $t\varphi(m) = 0$ in M_2. But $t\varphi(m) = \varphi(tm)$, since φ is an R-module map.
So $tm \in \ker\varphi = \operatorname{im}\theta$ and so $tm = \theta(m_1)$ for some $m_1 \in M_1$. Hence in $S^{-1}M$,
$m/s = \theta(m_1)/ts = S^{-1}\theta(m_1/ts) \in \operatorname{Im} S^{-1}\theta$.

(3.3): Let N be a submodule of M. Then, $S^{-1}(M/N) \cong S^{-1}M / S^{-1}N$.
Proof: We have a short exact sequence, $0 \to N \hookrightarrow M \xrightarrow{\pi} M/N \to 0$, and from (3.2) we know $0 \to S^{-1}N \to S^{-1}M \to S^{-1}(M/N) \to 0$ is exact.

If I is an ideal of R, then $S^{-1}I$ is an ideal of $S^{-1}R$.

(3.4): (i) Every ideal of $S^{-1}R$ is of the form $S^{-1}I$ for some ideal I of R.
(ii) The prime ideals of $S^{-1}R$ are in 1-1 correspondance $P \longleftrightarrow S^{-1}P$ with the prime ideals of R which don't meet S.
Proof: (i) Let J be an ideal of $S^{-1}R$, and $r/s \in J$. Then $r/1 \in J$. Let $I = \{ r : r/1 \in J \}$.

Thus $r \in I$. Clearly, $J \subseteq S^{-1}I$. If $r \in I$ then $r/1 \in J$ and hence $r/s \in J$. So $S^{-1}I \subseteq J$.

(ii) Let Q be a prime of $S^{-1}R$, $P = \{r \in R : r/1 \in Q\}$

Claim P is prime: if $xy \in P$, then $xy/1 \in Q$, and so either $x/1$ or $y/1 \in Q$.

P does not meet S: otherwise $(s/1)(1/s) = 1/1 \in Q$ for some $s \in S \cap P$.

Conversely, suppose $(r/s)(x/y) \in S^{-1}P$. Then $rx/sy \in S^{-1}P$, and so $(rx)z \in P$, some $z \in S$. So $rx \in P$ since $z \notin P$. So $r \in P$ or $x \in P$, and so $r/s \in S^{-1}P$ or $x/y \in S^{-1}P$.

(3.5): If R is a Noetherian ring then $S^{-1}R$ is Noetherian

Proof: Take a chain of ideals in $S^{-1}R$, $J_1 \subseteq J_2 \subseteq \cdots$. By (3.4), we know this is of the form $S^{-1}I_1 \subseteq S^{-1}I_2 \subseteq \cdots$, I_j ideals of R where $I_j = \{r \in R : r/1 \in J_j\}$. Consider the chain $I_1 \subseteq I_2 \subseteq \cdots$. R is Noetherian by supposition, and so this chain terminates, ie $I_j = I_{j+1} = \cdots$, some j. So, $S^{-1}I_j = S^{-1}I_{j+1} = \cdots$.

Definition: A property $\mathcal{P}$ is local if: R has property $\mathcal{P} \Leftrightarrow R_P$ has property $\mathcal{P}$ $\forall$ primes P.

(3.6): The following are equivalent:

(i) $M = 0$

(ii) $M_P = 0$ for all primes P.

(iii) $M_Q = 0$ for all maximals Q.

Proof: (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) trivial.

So, suppose (iii) holds and $M \neq 0$. Take $0 \neq m \in M$. The annihilator of m, $\{r \in R : rm = 0\}$, is a proper ideal of R. So it is contained in a maximal ideal Q. Consider $m/1 \in M_Q$. By assumption, $M_Q = 0$, so $m/1 = 0$, and so $sm = 0$ for some $s \in S = R \setminus Q$. $\#$, as Q contains the annihilator of m.

(3.7): Let $\varphi : M \to N$ be an R-module map. The following are equivalent:

(i) φ injective

(ii) $\varphi_P : M_P \to N_P$ is injective for all primes P

(iii) $\varphi_Q : M_Q \to N_Q$ is injective for all maximals Q.

Proof: (i) $\Rightarrow$ (ii) - by exactness of localisation

(ii) $\Rightarrow$ (iii) - fine.

(iii) $\Rightarrow$ (i): Let $M_1 = \ker \varphi$. Then $0 \to M_1 \to M \xrightarrow{\varphi} N \to 0$ is exact at M_1 and M. So (3.2) gives $0 \to (M_1)_Q \to M_Q \xrightarrow{\varphi_Q} N_Q \to 0$ is exact at $(M_1)_Q$ and M_Q, for maximal Q. Thus $(M_1)_Q = \ker \varphi_Q$. But $\ker \varphi_Q = 0$ by supposition. So $(M_1)_Q = 0$ for all Q. Then apply (3.6).

(3.8): Let P be a prime ideal of R and S be a multiplicatively closed subset of R with $S \cap P = \emptyset$. By (3.4) we know that $S^{-1}P$ is a prime of $S^{-1}R$. Then $(S^{-1}R)_{S^{-1}P} \cong R_P$. In particular, if Q is a prime ideal of R with $P \subseteq Q$, then set $S = R \setminus Q$ and we get $(R_Q)_{P_Q} \cong R_P$.

Proof: We have ring homomorphisms $\theta_1 : R \to S^{-1}R$, $\theta_2 : S^{-1}R \to (S^{-1}R)_{S^{-1}P}$. Let $\varphi = \theta_2 \circ \theta_1$, a ring homomorphism $R \to (S^{-1}R)_{S^{-1}P}$, with $\varphi(s')$ a unit for all $s' \in S' = R \setminus P$.

[Proof: all elements r/s of $S^{-1}R$ not in $S^{-1}P$ map to units of $(S^{-1}R)_{S^{-1}P}$, and if $s' \in S'$ then $s^{-1}/1$ is not in $S^{-1}P$. (If it were, there would be $x \in S$ with $xs' \in P$. But P is prime and $s' \notin P$, so $x \in P$, but $S \cap P = \phi$).]

So apply (3.1), to give a unique ring homomorphism such that $\begin{array}{ccc} R & \xrightarrow{\theta_2} & R_P \\ & \searrow^{\varphi} & \downarrow \alpha \\ & & (S^{-1}R)_{S^{-1}P} \end{array}$ commutes.

α is surjective: since all elements of $(S^{-1}R)_{S^{-1}P}$ are of the form $\varphi(r)\varphi(s)^{-1}$ for some $r \in R$, $s' \in S'$ - (*)

α is injective: suppose $r/s' \in \ker \alpha \subseteq R_P$. Then, $r/1 \in \ker \alpha \subseteq R_P$ and hence $r \in \ker \varphi$. But if $\varphi(r) = 0$ then $(r/1)(x/y) = 0$ in $S^{-1}R$ for some $x/y \notin S^{-1}P$, and so $sr x = 0$ for some $s \in S$, $x \notin P$. But $S \cap P = \phi$ and so $sx \notin P$ and we have $y \in S'$ such that $ry = 0$. - (**)
Hence $r/s' \in R_P$ is the zero of R_P.

Remark: Properties (*) and (**) of φ ensure more generally that a map α from (3.1) is an isomorphism.

4. Tensor Products.

R - commutative ring with a 1. L, M, N, T : R-modules.

Definition: $\varphi: M \times N \to L$ is bilinear if: (i) $\varphi(r_1 m_1 + r_2 m_2, n) = r_1 \varphi(m_1, n) + r_2 \varphi(m_2, n)$
(ii) $\varphi(m, r_1 n_1 + r_2 n_2) = r_1 \varphi(m, n_1) + r_2 \varphi(m, n_2)$.

Idea of tensor products is to reduce the study of bilinear maps to that of linear (ie, R-module) maps.
If $\varphi: M \times N \to T$ is bilinear and $\theta: T \to L$ is linear then $\theta \circ \varphi$ is bilinear.
Thus composition with φ gives a well-defined function φ^* from $\{R\text{-module maps}\}$ to $\{\text{bilinear maps}\}$.

Definition: A bilinear map $\varphi: M \times N \to T$ is universal if this function φ^* is a (1-1) - correspondance for all L.

If this happens, the study of bilinear maps $M \times N \to L$ is reduced to the study of linear maps $T \to L$.

(4.1): (i) Given R-modules M, N, $\exists$ R-module T and universal map $\varphi: M \times N \to T$.
(ii) Given two universal maps $\varphi_1: M \times N \to T_1$, $\varphi_2: M \times N \to T_2$, then there is a unique isomorphism $\beta_1: T_1 \to T_2$ with $\varphi_2 = \beta_1 \circ \varphi_1$.

Proof: (i) Let F be the free R-module on generators $e_{(m,n)}$ indexed by pairs $(m,n) \in M \times N$. Let X be the R-submodule generated by all the elements of the form $e_{(r_1 m_1 + r_2 m_2, n)} - r_1 e_{(m_1, n)} - r_2 e_{(m_2, n)}$ and $e_{(m, r_1 n_1 + r_2 n_2)} - r_1 e_{(m, n_1)} - r_2 e_{(m, n_2)}$.

Set $T = F/X$ and write $m \otimes n$ for the image of $e_{(m,n)}$ in T. T is generated by elements of the form $m \otimes n$, and $(r_1 m_1 + r_2 m_2) \otimes n = r_1 (m_1 \otimes n) + r_2 (m_2 \otimes n)$, $m \otimes (r_1 n_1 + r_2 n_2) = r_1 (m \otimes n_1) + r_2 (m \otimes n_2)$. Thus $\varphi : M \times N \to T$, $(m,n) \mapsto m \otimes n$ is bilinear.

Any map $\alpha : M \times N \to L$ extends to an R-module map $\bar{\alpha} : F \to L$, $e_{(m,n)} \mapsto \alpha(m,n)$. If α is bilinear then $\bar{\alpha}$ vanishes on all the generators of X, and so on the whole of X. So $\bar{\alpha}$ induces an R-module map $\alpha' : T \to L$ with $\alpha'(m \otimes n) = \alpha(m,n)$, and α' is uniquely defined by this.

(ii) Suppose we have universal maps $\varphi_i : M \times N \to T_i$ $(i = 1, 2)$. Since φ_1 is universal, there is a unique R-module map $\beta_1 : T_1 \to T_2$ with $\varphi_2 = \beta_1 \circ \varphi_1$. Similarly, there is $\beta_2 : T_2 \to T_1$ with $\varphi_1 = \beta_2 \circ \varphi_2$. Then, $(\beta_2 \circ \beta_1) \circ \varphi_1 = \varphi_1 = \mathrm{id} \circ \varphi_1$. But φ^* is bijective and hence $\beta_2 \beta_1 = \mathrm{id} : T_1 \to T_1$. Similarly, have $\beta_1 \circ \beta_2 = \mathrm{id} : T_2 \to T_2$. Hence β_1 is the required isomorphism.

Definition: T is written as $M \otimes_R N$, the tensor product of M and N over R.

Warning: Not all the elements of $M \otimes N$ are of the form $m \otimes n$. A general element is $\sum_{i=1}^{r} m_i \otimes n_i$.

Example: $R = k$, a field. M, N finite dimensional k-vector spaces, dimensions s, t. $M = k^s$, $N = k^t$. Then $M \times N \to k^{st}$, $((a_1, \dots, a_s), (b_1, \dots, b_t)) \mapsto (a_i b_j)_{1 \le i \le s, 1 \le j \le t}$ is universal and so $M \otimes N \cong k^{st}$.

Example: $\mathbb{Z}/r\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/s\mathbb{Z} \cong \mathbb{Z}/(\mathrm{hcf}(r,s))\mathbb{Z}$.

Remark: One can produce a universal trilinear map, $L \times M \times N \to T$, unique up to isomorphism, denoted by $L \otimes M \otimes N$.

(4.2): There exist unique isomorphisms:

(i) $M \otimes N \to N \otimes M$, $m \otimes n \mapsto n \otimes m$.

(ii) $(M \otimes N) \otimes L \to M \otimes N \otimes L \to M \otimes (N \otimes L)$, $(m \otimes n) \otimes l \mapsto m \otimes n \otimes l \mapsto m \otimes (n \otimes l)$.

(iii) $(M \oplus N) \otimes L \to (M \otimes L) \oplus (N \otimes L)$, $(m,n) \otimes l \mapsto ((m \otimes l), (n \otimes l))$.

(iv) $R \otimes M \to M$, $r \otimes m \mapsto rm$.

Proof: (i) Have map $M \times N \to N \otimes M$, $(m,n) \mapsto n \otimes m$, bilinear. And so we get $M \otimes N \to N \otimes M$, $m \otimes n \mapsto n \otimes m$, linear. Clearly we have the inverse $N \otimes M \to M \otimes N$, $n \otimes m \mapsto m \otimes n$.

(ii) See example sheet.

(iii) Have map $(M \oplus N) \times L \to (M \otimes L) \oplus (N \otimes L)$, $((m,n), l) \mapsto (m \otimes l, n \otimes l)$, bilinear. So, using the universal property, get unique linear maps: $(M \oplus N) \otimes L \to (M \otimes L) \oplus (N \otimes L)$, $(m,n) \otimes l \mapsto (m \otimes l, n \otimes l)$. We show this is an isomorphism by producing an inverse. Have:

$$M \otimes L \xrightarrow{f_1} (M \otimes L) \oplus (N \otimes L) \xleftarrow{f_2} N \otimes L$$
$$\psi_1 \searrow \qquad (M \oplus N) \otimes L \qquad \swarrow \psi_2.$$

Since $M \times L \to (M \oplus N) \otimes L$, $(m,l) \mapsto (m,0) \otimes l$ is bilinear, have $\psi_1 : M \otimes L \to (M \oplus N) \otimes L$, $m \otimes l \mapsto (m,0) \otimes l$

Similarly, have Ψ_2. These Ψ_1 and Ψ_2 combine to give linear
$\Psi: (M\otimes L)\oplus(N\otimes L) \longrightarrow (M\oplus N)\otimes L$, $((m\otimes l_1),(n\otimes l_2)) \mapsto (m,0)\otimes l_1 + (0,n)\otimes l_2$.
Check that Ψ is the required inverse.

(iv) Easy exercise.

(4.3): $\mathrm{Hom}(M\otimes N, L) \cong \mathrm{Hom}(M, \mathrm{Hom}(N,L))$.

Proof: Given a bilinear map, $\varphi: M\times N \to L$, we get $\theta: M \to \mathrm{Hom}(N,L)$, where $m \mapsto (\theta_m: N\to L,\ n\mapsto \varphi(m,n))$.
Conversely, given linear $\theta: M \to \mathrm{Hom}(N,L)$, we get a bilinear map $M\times N \to L$, $(m,n)\mapsto \theta(m)(n)$.
So we have a 1-1 correspondance: (bilinear $M\times N\to L$) $\leftrightarrow$ (linear $M\to \mathrm{Hom}(N,L)$).
But LHS corresponds to the linear maps $M\otimes N \to L$.

Restriction and Extension of Scalars.

If $\varphi: R\to T$ is a ring homomorphism, and N is a T-module, then it may be regarded as an R-module via $rm = \varphi(r)m$, restriction of scalars.
In particular, T itself is an R-module.
Given an R-module M, we can form another R-module $T\otimes_R M$. This can also be viewed as a T-module via $t_1(t_2\otimes m) = (t_1t_2)\otimes m$, extension of scalars.

(4.4): Given R-module M and a multiplicatively closed subset S of R, there is a unique isomorphism $f: S^{-1}R\otimes_R M \to S^{-1}M$, $r/s \otimes m \mapsto (rm)/s$.

Proof: The map $S^{-1}R\times M \to S^{-1}M$, $(r/s, m)\mapsto (rm)/s$ is R-bilinear, and so the universal property yields $f: S^{-1}R\otimes M \to S^{-1}M$. It is surjective.
A general element of LHS is of the form $\sum_{i=1}^{n}(r_i/s_i)\otimes m_i$. Set $s=s_1\cdots s_n$ and $t_i = \prod_{j\neq i} s_j$. Then, $\sum (r_i/s_i)\otimes m_i = \sum (r_it_i/s)\otimes m_i = \sum \frac{1}{s}\otimes r_it_im_i = \frac{1}{s}\otimes \sum r_it_im_i$, so every element of LHS is of the form $\frac{1}{s}\otimes m$.
Suppose $f(\frac{1}{s}\otimes m)=0$. Then $m/s = 0$ in $S^{-1}M$, and so $xm=0$ for some $x\in S$.
So, $\frac{1}{s}\otimes m = \frac{x}{sx}\otimes m = \frac{1}{sx}\otimes xm = \frac{1}{sx}\otimes 0 = 0$. Thus f is injective.

Tensor Products of Maps.

Given $\theta: M_1\to M_2$, $\varphi: N_1\to N_2$, there is an R-module map $\theta\otimes\varphi: M_1\otimes N_1 \longrightarrow M_2\otimes N_2$ where $m_1\otimes n_1 \mapsto \theta(m_1)\otimes\varphi(n_1)$. For: Since $M_2\times N_2 \to M_2\otimes N_2$ is bilinear, then $M_1\times N_1 \to M_2\otimes N_2$, $(m_1,n_1)\mapsto \theta(m_1)\otimes\varphi(n_1)$ is bilinear. The universality of $\otimes$ now gives the required linear map.

Tensor Products of Algebras

Let $\varphi_1 : R \to T_1$ be a ring homomorphism. (Recall T_1 is an R-module). We say that T_1 together with the map φ_1 is an R-algebra.

Given another ring homomorphism $\varphi_2 : R \to T_2$, we can take the tensor product of the R-modules T_1 and T_2 to give $T_1 \otimes_R T_2$. Define a product on $T_1 \otimes T_2$ by $(T_1 \otimes T_2) \times (T_1 \otimes T_2) \to T_1 \otimes T_2$, $(t_1 \otimes t_2)(t_1' \otimes t_2') = t_1 t_1' \otimes t_2 t_2'$. We have to convince ourselves that this is well-defined.

Multiplication $T_i \times T_i \to T_i$, $(t_i, t_i') \mapsto t_i t_i'$ is bilinear, and so there is a corresponding R-module map $T_i \otimes T_i \to T_i$. The composition $(T_1 \otimes T_1) \times (T_2 \otimes T_2) \to T_1 \times T_2 \to T_1 \otimes T_2$ is bilinear, and so we have the corresponding R-module map $(T_1 \otimes T_1) \otimes (T_2 \otimes T_2) \to T_1 \otimes T_2$.

$$(t_1 \otimes t_1') \otimes (t_2 \otimes t_2') \mapsto t_1 t_1' \otimes t_2 t_2'.$$

But from (4.2) we have isomorphisms:

$$\begin{aligned}(T_1 \otimes T_2) \otimes (T_1 \otimes T_2) &\to T_1 \otimes (T_2 \otimes (T_1 \otimes T_2)) \\ &\to T_1 \otimes ((T_2 \otimes T_1) \otimes T_2) \\ &\to T_1 \otimes ((T_1 \otimes T_2) \otimes T_2) \\ &\to T_1 \otimes (T_1 \otimes (T_2 \otimes T_2)) \to (T_1 \otimes T_1) \otimes (T_2 \otimes T_2),\end{aligned}$$

with $(t_1 \otimes t_2) \otimes (t_1' \otimes t_2') \mapsto (t_1 \otimes t_1') \otimes (t_2 \otimes t_2')$

Composing gives our product as a well-defined map.

$1 \otimes 1$ is the multiplicative identity. $T_1 \otimes T_2$ is a ring.

$R \to T_1 \otimes T_2$, $r \mapsto \varphi_1(r) \otimes \varphi_2(r)$ is a ring homomorphism. So $T_1 \otimes T_2$ is an R-algebra.

Examples: (i) k a field, $k[X]$ is a k-algebra. $k[X_1] \otimes_k k[X_2] \cong k[X_1, X_2]$.

(ii) $\mathbb{R}[X]/(X^2+1) \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C}[X]/(X^2+1)$

(iii) $k[X_1]/(f(X_1)) \otimes_k k[X_2]/(g(X_2)) \cong k[X_1, X_2]/(f(X_1), g(X_2))$.

Definition: R a k-algebra, M, N R-modules. Regard $M \otimes_k N$ as an R-module via $r(m \otimes n) = rm \otimes rn$. This is the diagonal action. (cf: sheet 2, question 13).

(4.5): If $M_1 \xrightarrow{\theta} M \xrightarrow{\varphi} M_2 \to 0$ is a sequence of R-modules, then it is exact iff for all R-modules N, $0 \to \mathrm{Hom}(M_2, N) \xrightarrow{\alpha} \mathrm{Hom}(M, N) \xrightarrow{\beta} \mathrm{Hom}(M_1, N)$ is exact.

Proof: ($\Rightarrow$) Let N be an R-module. If $f \in \mathrm{Hom}(M_2, N)$, then $f \circ \varphi \in \mathrm{Hom}(M, N)$. This gives an injective map $\alpha : \mathrm{Hom}(M_2, N) \to \mathrm{Hom}(M, N)$, since if f is non-zero there is $m_2 \in M_2$ with $f(m_2) \neq 0$; but $m_2 = \varphi(m)$ for some m since φ is surjective, and so $f\varphi(m) \neq 0$.

If $g \in \mathrm{Hom}(M, N)$ then $g \circ \theta \in \mathrm{Hom}(M_1, N)$. What is its kernel? Suppose $g\theta$ is the zero map. So $\theta(M_1) \subseteq \ker g$. But exactness gives $\theta(M_1) = \ker \varphi$, so $\ker \varphi \subseteq \ker g$. Then there is $f \in \mathrm{Hom}(M_2, N)$ with $f\varphi = g$. Thus we have exactness at $\mathrm{Hom}(M, N)$.

($\Leftarrow$) Since α is injective for all N, we have φ surjective. Also, $\beta\alpha = 0$, and so $f \circ \varphi \circ \theta = 0$ for any $f : M_2 \to N$. Take N to be M_2 and f to be the identity map.

So $\varphi \circ \theta = 0$, and hence $\operatorname{im}\theta \subseteq \ker\varphi$. Now, take $N = M/\operatorname{im}\theta$ and let $p: M \to N$ be the projection. Then $p \in \ker\beta$ and hence there exists $g: M_2 \to N$ with $p = g \circ \varphi$. Thus $\operatorname{im}\theta = \ker p \supseteq \ker\varphi$.

Remark: It is not true in general that a short exact sequence yields another on applying $\operatorname{Hom}(-, N)$. This leads to cohomology theory.

(4.6): Take $M_1 \xrightarrow{\theta} M \xrightarrow{\varphi} M_2 \to 0$ an exact sequence of R-modules and let N be an R-module. Then $M \otimes N \xrightarrow{\theta\otimes id} M \otimes N \xrightarrow{\varphi\otimes id} M_2 \otimes N \to 0$ is exact. (and, by commutativity of tensor products, $N \otimes M_1 \to N \otimes M \to N \otimes M_2 \to 0$ is exact).

Proof: Let N' be any R-module. Since $\otimes$ is exact, $0 \to \operatorname{Hom}(M_2, \operatorname{Hom}(N, N'))$ $\to \operatorname{Hom}(M, \operatorname{Hom}(N, N')) \to \operatorname{Hom}(M_1, \operatorname{Hom}(N, N'))$ is exact by (4.5). By (4.3), $\operatorname{Hom}(M, \operatorname{Hom}(N, N')) \cong \operatorname{Hom}(M \otimes N, N')$. So, $0 \to \operatorname{Hom}(M_2 \otimes N, N')$ $\to \operatorname{Hom}(M \otimes N, N') \to \operatorname{Hom}(M_1 \otimes N, N')$ is exact. Apply converse part of (4.5) to get result.

Remark: It is not true in general that applying $\otimes N$ to a short exact sequence yields another. This failure leads to the definition of Tor (and homology theory).

5. Integral Dependence

$R \subseteq S$ rings. $x \in S$ is integral over R if it satisfies some monic polynomial with coefficients in R: $x^n + r_{n-1}x^{n-1} + \cdots + r_0 = 0$.

Example: The only elements of $\mathbb{Q}$ integral over $\mathbb{Z}$ are the elements of $\mathbb{Z}$: Suppose $a/b \in \mathbb{Q}$, a, b coprime, and $(a/b)^n + r_{n-1}(a/b)^{n-1} + \cdots + r_0 = 0$. Then $a^n + r_{n-1}a^{n-1}b + \cdots + r_0 b^n = 0$. So b divides a^n, so is ± 1.

S is finite over R if S is a f.g. R-module.
Denote the ring generated by R and $x \in S$ by $R[x] \in S$.

(5.1): The following are equivalent:
(i) $x \in S$ is integral over R.
(ii) $R[x]$ is finite over R.
(iii) $R[x]$ is contained in a subring T of S with T finite over R.

Proof: (i) $\Rightarrow$ (ii): one can reduce any element of the form $a_m x^m + \cdots + a_0$ $(a_i \in R)$ by using the substitution $x^n = -r_{n-1}x^{n-1} + \cdots - r_0$, to give an element of the form $b_{n-1}x^{n-1} + \cdots + b_0$. Thus $x^{n-1}, \ldots, x$ generate $R[x]$ as an R-module.

(ii) $\Rightarrow$ (iii): trivial.

(iii) $\Rightarrow$ (i): consider multiplication by x in the ring T. Take $y_1, \ldots, y_n$ as R-module generators for T. $xy_i = \sum_{j=1}^{n} r_{ij} y_j$, each i. Let $A = (x\delta_{ij} - r_{ij})$. So $A\underline{y} = 0$. Multiply on left by $\operatorname{adj} A$, giving $\det A \, y_j = 0$ for all j. But 1 is an

R-linear combination of the y_j, so $\det A = 0$. But $\det A$ is of the form $x^n + r_{n-1}x^{n-1} + \cdots + r_0$. So x is integral over R. (cf: proof of Nakayama's Lemma (later)).

(5.2): If $x_1, \ldots, x_n \in S$ are integral over R then $R[x_1, \ldots, x_n]$ is finite over R.

Proof: By induction. $n=1$ was (5.1). Suppose $R[x_1, \ldots, x_k]$ is finite over R, generators $y_1, \ldots, y_m$ say. But x_{k+1} is integral over R and hence over $R[x_1, \ldots, x_k]$. Thus $R[x_1, \ldots, x_{k+1}]$ is a finitely generated $R[x_1, \ldots, x_k]$-module, generators $z_1, \ldots, z_t$. Then $\{z_i y_j : 1 \le i \le t, 1 \le j \le m\}$ generate $R[x_1, \ldots, x_{k+1}]$ as an R-module.

Remark: S is of finite type over R if S is generated as a ring by R together with a finite set.

(5.3): The set $T \subseteq S$ of elements integral over R is a subring containing R.

Proof: Clearly every element of R is integral over R. If $x, y \in T$ then by (5.2) $R[x,y]$ is a f.g R-module. So by (5.1) (iii), $x \pm y$ and xy are integral over R.

This T is the integral closure of R. If $T = R$, then R is integrally closed in S. If $T = S$ then T is integral over R. If R is an integral domain, then say R is integrally closed if it is so in its fraction field. (ie, no qualification, ie, no "in S")

(5.4): If $R \subseteq T \subseteq S$ and T is integral over R and S is integral over T, then S is integral over R.

Proof: Take $x \in S$. It satisfies $x^n + t_{n-1}x^{n-1} + \cdots + t_0 = 0$ with $t_i \in T$. The subring $R[t_0, \ldots, t_{n-1}]$ is a f.g. R-module by (5.2), and x is integral over it, so $R[t_0, \ldots, t_{n-1}, x]$ is a f.g. $R[t_0, \ldots t_{n-1}]$-module. So, as in (5.2), $R[t_0, \ldots, t_{n-1}, x]$ is a f.g. R-module. Apply (5.1) (iii)

(5.5): If $R \subseteq S$ and T = integral closure of R in S then T is integrally closed in S.

Proof: By (5.4).

(5.6): Let $R \subseteq T$, T integral over R.

(ii) If J is an ideal of T, then T/J is integral over $R/J \cap R$ $\left(\cong (R+J)/J \subseteq T/J\right)$

(iii) If S is a multiplicatively closed subset of R then $S^{-1}T$ is integral over $S^{-1}R$.

Proof: (ii) If $x \in T$ then $x^n + r_{n-1}x^{n-1} + \cdots + r_0 = 0$ - $\circledast$, some $r_i \in R$. Modulo J we have a monic equation $\bar{x}^n + \bar{r}_{n-1}\bar{x}^{n-1} + \cdots + \bar{r}_0 = \bar{0}$ in T/J, with $\bar{r}_i \in (R+J)/J$.

(iii) Suppose $x/s \in S^{-1}T$. Then $\circledast$ gives $(x/s)^n + (r_{n-1}/s)(x/s)^{n-1} + \cdots + (r_0/s^n) = 0$. So x/s is integral over $S^{-1}R$.

(5.7): Suppose $R \subseteq T$ integral domains with T integral over R. Then T is a field iff R is a field.

Proof: Suppose R is a field. Let $0 \neq t \in T$. Choose equation of least degree of form $t^n + r_{n-1}t^{n-1} + \cdots + r_0 = 0$ with $r_i \in R$. T is an integral domain and so $r_0 \neq 0$, else get $t(t^{n-1} + r_{n-1}t^{n-2} + \cdots + r_1) = 0$ - a shorter equation. So t has inverse $-r_0^{-1}(t^{n-1} + r_{n-1}t^{n-2} + \cdots + r_1) \in T$. So T is a field.

Conversely, suppose T is a field, $0 \neq x \in R$. Then x has inverse x^{-1} in T.
So x^{-1} satisfies some equation $x^{-m} + r_m' x^{-m+1} + \cdots + r_0' = 0$.
So $x^{-1} = -(r_m' + r_{m-1}' x + \cdots + r_0' x^{m-1}) \in R$. Thus R is a field.

(5.8): Let $R \subseteq T$ be rings with T integral over R. Let Q be a prime ideal of T and set $P = Q \cap R$. Then Q is maximal iff P is maximal.

Proof: By (5.6) (i), T/Q is integral over R/P, and both are integral domains. Apply (5.7).

(5.9): Incomparability Theorem: Let $R \subseteq T$ rings with T integral over R. Let $Q \subseteq Q_1$ be prime ideals of T. Suppose $Q_1 \cap R = P = Q \cap R$. Then $Q = Q_1$.

Proof: Apply (5.6) (ii) with $S = R \setminus P$. We have that T_P is integral over R_P. In (3.4), we learnt about prime ideals in a localised ring. There is a prime $S^{-1}P$ in R_P, the unique maximal ideal. Also, there are $S^{-1}Q$ and $S^{-1}Q_1$ in $T_P = S^{-1}T$, also prime. And $S^{-1}Q \cap S^{-1}R = S^{-1}P = S^{-1}Q_1 \cap S^{-1}R$, since $Q \cap R = P = Q_1 \cap R$ (by sheet 2, question 2). By (5.8), $S^{-1}Q$ and $S^{-1}Q_1$ are maximal. But $S^{-1}Q \subseteq S^{-1}Q_1$, and so $S^{-1}Q = S^{-1}Q_1$. By (3.4)(iii), $Q = Q_1$. (ie, "there is a 1-1 correspondance between prime ideals of $S^{-1}T$ and those of T that don't meet S").

(5.10): Lying Over Theorem: Let $R \subseteq T$, rings, T integral over R. Let P be a prime ideal of R. Then there is a prime ideal Q of T with $Q \cap R = P$.

Proof: By (5.6), T_P is integral over R_P. (taking $S = R \setminus P$). Consider . a maximal ideal of T_P. It is of the form $S^{-1}Q$ by (3.4) (i), for some ideal Q of T which is prime by (3.4) (ii). Then $S^{-1}Q \cap S^{-1}R$ is maximal by (5.8), and hence is the unique maximal ideal $S^{-1}P$ of $S^{-1}R$. So $S^{-1}Q \cap S^{-1}R = S^{-1}P$.
So $Q \cap R = P$, (by example sheet or (3.4)).

(5.11): Going Up Theorem (Cohen-Seidenberg 1946):
Let $R \subseteq T$ with T integral over R. Let $P_1 \subseteq P_2 \subseteq \cdots \subseteq P_n$ be a chain of prime ideals in R and $Q_1 \subseteq Q_2 \subseteq \cdots \subseteq Q_m$ such in T, with $m < n$ and $Q_i \cap R = P_i$.
Then the chain $Q_1 \subseteq \cdots \subseteq Q_m$ can be extended to give $Q_1 \subseteq \cdots \subseteq Q_n$ with $Q_i \cap R = P_i$.

Proof: By induction. It's enough to do the case $m = 1$, $n = 2$.
Write $\bar{R}$ for R/P_1, $\bar{T}$ for T/Q_1. Then $\bar{R} \hookrightarrow \bar{T}$ with $\bar{T}$ integral over $\bar{R}$. (5.6).
By (5.10), there is a prime ideal $\bar{Q_2}$ of $\bar{T}$ such that $\bar{Q_2} \cap \bar{T} = \bar{P_2}$.
Lifting back gives a prime Q_2 of T with $Q_2 \cap R = P_2$.

(5.12): Going Down Theorem (Cohen-Seidenberg 1946):
Let $R \subseteq T$ be integral domains, R integrally closed, T integral over R.
Let $P_1 \geq \cdots \geq P_n$ be a chain of prime ideals in R, $Q_1 \geq \cdots \geq Q_m$ such in T, with $m < n$ and $Q_i \cap R = P_i$. Then the choice of Q's may be extended to give $Q_1 \geq \cdots \geq Q_n$ with $Q_i \cap R = P_i$.

Note: The hypotheses are stronger than in the Going Up Theorem.

We need 2 lemmas, and some extra terminology.
If I is an ideal of R, $R \subset T$, x is integral over I if x satisfies $x^n + r_{n-1}x^{n-1} + \cdots + r_0 = 0$ (*) with $r_i \in I$. The integral closure of I in T is the set of such x.

(5.13): Let $R \subset T$ rings with T integral over R, I an ideal of R. Then the integral closure of I in T is the radical $\sqrt{(TI)}$, and this is closed under addition and multiplication.

Proof: If x is integral over I, then (*) implies $x^n \in TI$, thus $x \in \sqrt{(TI)}$.
Conversely, if $x \in \sqrt{(TI)}$, then $x^a = \sum_{i=1}^{n} r_i t_i$, say, $a \in \mathbb{N}$, $r_i \in I$, $t_i \in T$.
But each t_i is integral over R, so (5.2) gives that $M = R[t_1, \ldots, t_n]$ is a fg R-module. Also, $x^a R[t_1, \ldots t_n] \subseteq IM$. Take $y_1, \ldots, y_s$ a generating set for M.
So $x^a y_j = \sum_{k=1}^{s} r_{jk} y_k$ for $r_{jk} \in I$. As in (5.1), we get $\sum_k \underbrace{(x^a \delta_{jk} - r_{jk})}_{= \text{matrix } A} y_k = 0$

Deduce that x^a satisfies an equation of the form $(x^a)^s + \cdots + r_0 = 0$, namely $\det A = 0$. Note that all coefficients are in I. Thus x^a, and hence x, is integral over I.

(5.14): Let $R \subset T$ be integral domains, R integrally closed, and let $x \in T$ be integral over the ideal I of R. Then x is algebraic over the field of fractions K of R, and the minimal polynomial over K, $X^n + r_{n-1}X^{n-1} + \cdots + r_0$ (**) has coefficients $r_{n-1}, \ldots, r_0$ in $\sqrt{I}$.

Proof: x is algebraic over K (from integral dependence on I).
Claim: the coefficients r_i are integral over I.
Proof: Consider the splitting field L of (**) over K. If y is a root of (**) (ie a conjugate of x), then there is a K-automorphism of L where $x \mapsto y$.
$K(x) \xrightarrow{\alpha, \cong} K(y)$, α = embedding of $K[x]$ into L. It may be extended to give an automorphism of L.
So y is integral over I; if x satisfies the monic equation $x^m + r'_{m-1}x^{m-1} + \cdots + r'_0 = 0$, $r'_j \in I$, then applying automorphism gives $y^m + r'_{m-1}y^{m-1} + \cdots + r'_0 = 0$.
The coefficients of (**) are obtained from its roots (in L) by taking sums of products. So by (5.13), these coefficients are integral over I.
Thus the $r_i \in R$, since R is integrally closed, and so by (5.13) (with $T = R$), the $r_i \in \sqrt{I}$, since they lie in the integral closure of I in R.

Proof of (5.12): By induction, it's enough to consider the case $m = 1$, $n = 2$.
So have $P_1 \supseteq P_2$, and Q_1 with $Q_1 \cap R = P_1$. Need $Q_2 \subseteq Q_1$ with $Q_2 \cap R = P_2$.
Let $S_2 = R \setminus P_1$, $S_1 = T \setminus Q_1$, and set $S = S_1 S_2 = \{ rt : r \in S_1, t \in S_2 \}$. This is multiplicatively closed.
For now, assume $TP_2 \cap S = \emptyset$. TP_2 is an ideal of T, and $S^{-1}(TP_2)$ is an ideal of $S^{-1}T$, which is proper by our assumption. $S^{-1}(TP_2)$ lies in some maximal ideal of $S^{-1}T$, which by (3.4) is of the form $S^{-1}Q_2$, for some prime ideal Q_2 of T, with $Q_2 \cap S = \emptyset$ and $TP_2 \subset Q_2$. Hence $P_2 \subseteq TP_2 \cap R \subseteq Q_2 \cap R$, and since $Q_2 \cap S = \emptyset$ and $S_2 = R \setminus P_2 \subseteq S$, we get $P_2 = Q_2 \cap R$.
Similarly, $S_1 = T \setminus Q_1 \subseteq S$, and so $Q_2 \subseteq Q_1$.

Finally, must show $TP_2 \cap S = \emptyset$. Take $x \in TP_2 \cap S$. By (5.13), x is in the integral closure of P_2 in T. So by (5.14) it is algebraic over the field of fractions K of R and its minimal polynomial over K has coefficients in P_2 (P_2 prime $\Rightarrow \sqrt{P_2} = P_2$). But $x \in S$, and so it is of the form $s_1 s_2$ with $s_1 \in S_1$, $s_2 \in S_2$. Say x has minimal polynomial $X^n + r_{n-1}X^{n-1} + \cdots + r_0$, so $s_1 = x/s_2$ has minimal polynomial $X^n + \frac{r_{n-1}}{s_2} X^{n-1} + \cdots + \frac{r_0}{s_2^n}$, and these coefficients are in R [via (5.16) with $I = R$], since $s_1 \in T$ is integral over R. Write these coefficients as r_i'. But $r_i \in P_2$ and $s_2^i \notin P_2$ and so each $r_i' \in P_2$. So by definition, s_1 is integral over P_2, and so by (5.13), s_1 is in $\sqrt{(TP_2)} \cdot \#$, since $s_1 \in S_1 = T \setminus Q_1$ and $TP_2 \subset Q_1$ [and so $\sqrt{(TP_2)} \subset Q_1$].

6. Krull Dimension.

All rings are commutative with a 1.

Definition: The spectrum of R, $\operatorname{Spec} R = \{\text{prime ideals}\}$

The length of a chain of prime ideals $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$ is n.

Krull dimension of $R = \begin{cases} \sup\{n : \exists \text{ chain of prime ideals of length } n\}, \text{ if it exists} \\ \infty \quad \text{otherwise} \end{cases}$

Height of $P \in \operatorname{Spec} R$, $ht(P) = \sup\{n : \exists \text{ chain of primes } P_0 \subsetneq \cdots \subsetneq P_n = P\}$.

Note: Using (3.4), $ht(P) = \dim(R_P)$.

Examples: (i) $\dim R = 0$. Prime ideals are maximal ideals. Artinian rings. Eg. fields. (Example sheet 3: $\dim 0 \Rightarrow$ Artinian).

(ii) $\dim R = 1$. Eg: $\mathbb{Z}$. $0 \subsetneq (p)$, p prime

$k[X]$, k a field.

These are examples of Dedekind rings - integrally closed $\dim 1$ domains. Such rings are the essential ingredients of the theory of algebraic curves and number theory.

(iii) $\dim k[X_1, \ldots, X_n] \geq n$. We have $0 \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \cdots \subsetneq (X_1, \ldots, X_n)$.

(6.1): Height 1 primes of $k[X_1, \ldots, X_n]$ are of the form (f), f irreducible.

Proof: Certainly such an ideal is prime in a unique factorisation domain. Any non-zero P contains such an (f), since if $g \in P$ then one of its irreducible factors does.

if $0 \subsetneq P \subseteq (f)$, then there is h irreducible with $(h) \subsetneq P$. But this would imply f divides h. Irreducibility of f implies $P = (f)$.

(6.2): Let $R \subseteq T$, rings, with T integral over R. Then $\dim R = \dim T$.

Proof: Take a chain of primes in T: $Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_n$. Intersecting with R gives a chain of primes in R: $P_0 \subsetneq \cdots \subsetneq P_n$, with strict inclusions by incomparability.

So $\dim(R) \geq \dim T$.
Conversely, if $P_0 \subsetneq \cdots \subsetneq P_n$ is a chain of primes in R, there is a prime Q_0 lying over P_0 (5.10). Going up (5.11) gives a chain in T.

(6.3): Let $R \subseteq T$, integral domains, T integral over R, R integrally closed.
If Q is a prime of T, then $\mathrm{ht}(Q) = \mathrm{ht}(Q \cap R)$.

Proof: Take a chain $Q_0 \subsetneq \cdots \subsetneq Q_n = Q$. Then intersecting with R gives a (strict) chain ending with $Q \cap R$. So $\mathrm{ht}(Q \cap R) \geq \mathrm{ht}\, Q$.
Conversely, suppose we have $P_0 \subsetneq \cdots \subsetneq P_n = Q \cap R$. Going down theorem yields chain $Q_0 \subsetneq \cdots \subsetneq Q_n = Q$, with $Q_i \cap R = P_i$.

Affine k-algebras (k a field): these are the k-algebras of finite type over k, ie, generated as rings by k and a finite set $x_1, \ldots, x_n$ say, and thus are images of $k[X_1, \ldots, X_n]$, a polynomial algebra.

(6.4): R an affine algebra, integral domain with fraction field K.
Then $\dim R = \mathrm{tr.deg}_k K$.

Transcendence Degree.

$x_1, \ldots, x_n \in K$ are algebraically independent if the ring map $k[X_1, \ldots, X_n] \to K$, $X_i \mapsto x_i$ gives an isomorphism: $k[X_1, \ldots, X_n] \to k[x_1, \ldots, x_n] \subseteq K$.
Consider maximal algebraically independent sets; they all have the same size.
There is a Steinitz Exchange lemma.
There is a translation from linear algebra tactics:

Linear independence $\leftrightarrow$ algebraic independence.
span $\leftrightarrow$ algebraic closure: maximal algebraic extension of the field generated by k and $x_1, \ldots, x_n$.
basis $\leftrightarrow$ transcendence basis.
dimension $\leftrightarrow$ transcendence degree.

Example: (i) $\mathrm{tr}_k k(X_1, \ldots, X_n) = n$. $X_1, \ldots, X_n$ is a maximal algebraically independent set.
(ii) K_1 = fraction field of $k[X_1, \ldots, X_n]/(f)$, $\mathrm{tr}_k K_1 = n-1$, since it is an algebraic extension of $k(X_1, \ldots, \hat{X_i}, \ldots, X_n)$, some x_i appearing in f.

Noether's Normalisation Lemma is the main ingredient in proving (6.4). It is:

(6.5): Let T be an affine algebra. Then T is integral over a subalgebra of the form $R = k[x_1, \ldots, x_r]$ with $x_1, \ldots, x_r$ algebraically independent.

Proof: $r = \mathrm{tr.deg}_k(\mathrm{ff}.T)$. Observe that we may assume $r \geq 1$ (otherwise T is a finite dimensional vector space over k and we can take $R = k$).
Say $T = k[a_1, \ldots, a_n]$. Use induction on n.
Renumber to assume $a_1, \ldots, a_r$ are algebraically independent and each of

$a_{r+1}, \dots a_n$ is algebraically dependent on $a_1, \dots, a_r$ over k. (Nothing to do if $a_1, \dots, a_n$ are algebraically independent.)

Take $f \neq 0 \in k[X_1, \dots, X_r, X_n]$ with $f(a_1, \dots, a_r, a_n) = 0$. $f(X_1, \dots, X_r, X_n)$ is a sum of terms $\lambda_{\underline{l}} X_1^{l_1} \dots X_r^{l_r} X_n^{l_n}$. $\underline{l} = (l_1, \dots, l_r, l_n)$, $l_i \in \mathbb{R}_{\geq 0}$.

Claim: $\exists$ positive integers $m_1, \dots, m_r$ so that $\varphi: \underline{l} \mapsto m_1 l_1 + \dots + m_r l_r + l_n$ is 1-1 for those $\underline{l}$ with $\lambda_{\underline{l}} \neq 0$.

Proof: There are finitely many possibilities for $\underline{d} = \underline{l} - \underline{l}'$ with $\lambda_{\underline{l}} \neq 0$, $\lambda_{\underline{l}'} \neq 0$. Write $\underline{d} = (d_1, \dots, d_r, d_n)$ and consider the finitely many non-zero $(d_1, \dots, d_r)$ obtained. Vectors in $\mathbb{Q}^r$ orthogonal to one of these r-tuples lie in finitely many $(r-1)$-dimensional subspaces.

Pick $(q_1, \dots, q_r)$ with each $q_i > 0$ so that $\sum q_i d_i \neq 0$, for all of the finitely many non-zero $(d_1, \dots, d_r)$. Multiply by a positive integer to get $(m_1, \dots, m_r)$ so that $|\sum_{i=1}^{r} m_i d_i| > |d_n|$ for all of the finitely many $\underline{d}$ with $(d_1, \dots, d_r) \neq 0$.

Thus if $\varphi(\underline{l}) = \varphi(\underline{l}')$ then $d_1 = \dots = d_r = 0$. But then $l_n = l_n'$, and so $\underline{l} = \underline{l}'$.

Now put $g(X_1, \dots, X_r, X_n) = f(X_1 + X_n^{m_1}, \dots, X_r + X_n^{m_r}, X_n)$. This is a sum of terms $\lambda_{\underline{l}} (X_1 + X_n^{m_1})^{l_1} \dots (X_r + X_n^{m_r})^{l_r} X_n^{l_n}$. Different terms have different powers of X_n and there will be a single term of highest power.

As a polynomial in X_n the leading coefficient of g is one of the $\lambda_{\underline{l}}$ and hence in k.

Put $b_i = a_i - a_n^{m_i}$ for $1 \leq i \leq r$ and $h(X_n) = g(b_1, \dots, b_r, X_n)$. This has leading coefficient in k and all coefficients in $k[b_1, \dots, b_r]$. Moreover, $h(a_n) = g(b_1, \dots, b_r, a_n) = f(a_1, \dots, a_r, a_n) = 0$. Divide through by leading coefficient and see that a_n is integral over $k[b_1, \dots, b_r]$.

So $a_i = b_i + a_n^{m_i}$ is also integral over $k[b_1, \dots, b_r]$ for $i \leq r$.

Hence T is integral over $k[b_1, \dots, b_r, a_{r+1}, \dots, a_{n-1}]$. By induction this latter ring is integral over polynomial algebra R. So T is integral over R.

Proof of (6.4): T an affine domain. $\dim T = \text{tr.deg}_k(\text{ff}.T) = r$.

By induction on r. Use (6.5) to get subring $R \cong$ polynomial algebra in r variables. (6.2) says that $\dim R = \dim T$. Clear that $\text{trdeg}(\text{ff}R) = \text{trdeg}(\text{ff}T)$ (Recall example (iii) showed $\dim R \geq r$).

Take chain of primes in R, $P_0 \subsetneq \dots \subsetneq P_s$. We may assume $P_0 = 0$, $P_1 = (f)$ if have $0 \subsetneq P_1$ with $P_1 \geq (f)$ for some irreducible f, since R is a UFD.

So consider $R/(f)$. $\text{tr.deg}(\text{ff}\,R/(f)) = r-1$. Induction gives that $\dim(R/(f)) = r-1$.

So consider chain $P_1/P_1 \subsetneq P_2/P_1 \subsetneq \dots \subsetneq P_s/P_1$ of primes in $R/P_1 = R/(f)$

We get $s-1 \leq \dim R/P_1 = r-1$, so $s \leq r$. Hence $\dim R \leq r$.

(6.6): If Q is a prime of an affine domain T, then $\text{ht}(Q) + \dim(T/Q) = n = \dim T$.

Proof: Let $m = \text{ht}(Q)$ and pick a chain of primes $Q_0 \subsetneq \dots \subsetneq Q_m = Q$ of maximal length. By Noether (6.5), there is a subring R of T with T integral over R and $R \cong$ polynomial algebra. By (6.2), $\dim R = \dim T$. By (6.4), $n = \dim R = \text{trdeg}_k(\text{ff}\,T)$

Write $P_i = Q_i \cap R$. Observe that Q_1 is of height 1. So by (6.3), since R is integrally closed (being a polynomial algebra and hence a UFD), $ht(P_1)=1$. So by (6.1), $P_1 = (f)$, and so $\operatorname{trdeg}(ff(R/P_1)) = n-1$.
Hence by (6.4) $\dim(R/P_1) = n-1$. By induction hypothesis applied to the prime Q/Q_1 in T/Q_1, $ht(Q/Q_1) = m-1$. $\dim(T/Q_1) = \dim(R/P_1) = n-1$, since R/P_1 embeds in T/Q_1 and T/Q_1 is integral over it. And $\dim(T/Q_1/Q/Q_1) = \dim(T/Q)$.
So $m-1 + \dim(T/Q) = n-1$.

(6.7): if Q is a maximal ideal of an affine algebra T, then $ht\,Q = \dim T$ (i.e. $\dim T_Q$).

(6.8) (Nullstellensatz): For an affine algebra T, $J(T) = N(T)$.

Proof: $J(T) = \bigcap_{Q \text{ maximal}} Q$, $N(T) = \bigcap_{Q \text{ prime}} Q$. It is enough to show that each prime is an intersection of maximals. So considering T/Q, Q prime, we may assume T is a domain. Prove result by induction on $\dim T$.
Noether Normalisation (6.5) gives T contains $R \cong$ polynomial algebra with T integral over R. In a polynomial algebra, $0 = \bigcap(f)$, f's irreducible. Consider $R/(f)$. Its dimension $< \dim R = \dim T$. So $J(R/(f)) = 0$, by induction.
Lifting back, in R, $(f) = \bigcap$ maximals. So in R, $0 = \bigcap_{P \text{ maximal}} P$.
By 'Lying Over', there is a prime Q of T with $Q \cap R = P$, for each maximal P of R. Q is maximal by (5.8). So if $J(T) = \bigcap_{Q \text{ maximal}} Q$, $J(T) \cap R = 0$.
Consider the minimal primes over $J(T)$, say $X_1, \dots, X_n$. Some product of them lies in $J(T)$. If we set $Y_i = X_i \cap R$, primes in R. Corresponding product of these lies in $J(T) \cap R = 0$. But R is a domain, so one of the $Y_i = 0$.
Incomparability gives $X_i = 0$. But $J(T) \subseteq X_i$, so $J(T) = 0$.

Remark: If k is algebraically closed, say $\mathbb{C}$, an affine k-domain which is a field is an algebraic extension of k (true for any k), and hence is k itself.
So if Q is maximal in $k[X_1, \dots, X_n]$ we know that $k[X_1, \dots, X_n]/Q \cong k$.
So $k[X_1, \dots, X_n] \longrightarrow k[X_1, \dots, X_n]/Q \cong k$, canonical projection, has kernel of form $(X_1 - a_1, \dots, X_n - a_n)$. Thus maximal ideals are of the form $(X_1 - a_1, \dots, X_n - a_n)$.

Recall: We had the correspondance:

$$\text{radical ideals } I \text{ in } \mathbb{C}[X_1, \dots, X_n] \longleftrightarrow \{(a_1, \dots, a_n) \in \mathbb{C}^n : I \subseteq (X_1 - a_1, \dots, X_n - a_n)\}$$

The correspondance occurs because $I = \bigcap_{I \subseteq (X_1 - a_1, \dots, X_n - a_n)} (X_1 - a_1, \dots, X_n - a_n)$.

(6.9) (Nakayama's Lemma): (i) Let M be a finitely generated R-module, I be an ideal of R. If $M = IM$ then there exists $r \in 1 + I$ with $rM = 0$.
If $I \subseteq J(R)$ then $M = 0$.
(ii) If R is local with unique maximal ideal P, and if $M = PM$ then $M = 0$.
Moreover, a minimal generating set for M is of size = R/P-vector space dimension of M/PM.

Proof: (i) Let $m_1, \dots, m_s$ be generators of M. Then $m_i \in IM$ and so $m_i = \sum x_{ij} m_j$ with $x_{ij} \in I$. So, $\sum (\delta_{ij} - x_{ij}) m_j = 0$. Multiply on the left by the adjugate: $\det(\delta_{ij} - x_{ij}) m_j = 0$ for all j. But this determinant $r \in 1+I$ and so $rM = 0$. All elements of $1 + J(R)$ are units (example sheet 1), and so if $I \subseteq J(R)$ then r is invertible and so $M = 0$.

(i)'-alternative: Suppose $M \neq 0$ and N is a maximal submodule, $0 \leq N \subsetneq M$. Then $M/N \cong R/P$, with P maximal. Thus $PM \leq N \subsetneq M$. But $J(R) \leq P$. So $J(R)M \subsetneq M$. If $I \leq J(R)$, then $IM \subsetneq M$.

(ii) R local, unique maximal ideal P. So $J(R) = P$. By (i), if $PM = M$ then $M = 0$. Take a generating set $m_1, \dots, m_s$ for M. Then $m_1 + PM, \dots, m_s + PM$ generate the vector space M/PM, over field R/P. So they span the vector space, so $s \geq \dim_{R/P} M/PM$

Take a basis of the vector space M/PM, say $m_1' + PM, \dots, m_n' + PM$, and pick $m_1', \dots, m_n'$, preimages in M.

Claim: these generate M. Let $M_1 = Rm_1' + \cdots + Rm_n' \leq M$. Consider M/M_1. This is an R-module and $P(M/M_1) = M/M_1$, since $PM + M_1 = M$. Then M/M_1 is zero and hence $M = M_1$.

(6.10) (Krull's Principal Ideal Theorem): Let R be a Noetherian ring and $a \in R$ a non-unit. Let P be a minimal prime over aR. Then $\operatorname{ht} P \leq 1$.

(6.11): I an ideal of R with minimal prime P. S a multiplicatively closed subset of R with $P \cap S = \phi$. Then $S^{-1}P$ is a minimal prime over $S^{-1}I$.

Proof: By (3.4), $S^{-1}P$ is a prime, and clearly $S^{-1}P \geq S^{-1}I$. Suppose $S^{-1}P$ is not minimal. Then there is a prime Q, $S^{-1}P \subsetneq Q \geq S^{-1}I$.

But (3.4) says that Q is of form $S^{-1}P_1$, with $P_1 \cap S = \phi$. Then $P \supsetneq P_1 \geq I$

Proof of (6.10): a a non-unit. P a minimal prime over Ra. Localise at P.

R_P has maximal ideal PR_P, and it is a minimal prime over $(Ra)_P$, by (6.11). Also, $\operatorname{ht} PR_P = \operatorname{ht} P$. So we replace R by R_P, and assume that R is local with maximal ideal P.

Suppose $\operatorname{ht} P > 1$. So there is a chain of primes $Q' \subsetneq Q \subsetneq P$.

Consider R/Ra. This has unique maximal ideal P/Ra. Moreover, it is also a minimal prime, in fact the only prime, of R/Ra. So $N(R/Ra) = P/Ra$ is nilpotent, so $P^n \leq Ra$ for some n. $R \supsetneq P \geq P^2 \geq \cdots \geq P^n$. Each factor is a finite-dimensional R/p-vector space and hence is Artinian. So R/P^n is Artinian and hence R/Ra is Artinian.

Now consider $I_n = \{ r \in R : r/1 \in S^{-1}Q^n \}$ where $S = R \setminus Q$.

Clearly $I_1 \geq I_2 \geq \cdots$ (*). Hence $(I_1 + Ra)/Ra \geq (I_2 + Ra)/Ra \geq \cdots$ is a descending chain, so terminates, since R/Ra is Artinian. Say $I_m + Ra = I_{m+1} + Ra$, some m.

Next show that (*) terminates: Let $r \in I_m$. Then $r = t + ax$, some $t \in I_{m+1}$, $x \in R$. So $ax = r - t \in I_m$, and $a \notin Q$. In $S^{-1}R$ we have $S^{-1}Q \geq S^{-1}Q^2 \geq \cdots$, and each factor is a $S^{-1}R/S^{-1}Q$. But $ax/1 \in S^{-1}Q^m$, and $a \notin Q$. So $x/1 \in S^{-1}Q^m$, a vector space. So $x \in I_m$.

So $I_m = I_{m+1} + I_m a$. Hence $I_m/I_{m+1} = P(I_m/I_{m+1})$, regarding I_m/I_{m+1} as an R-module, since $a \in P$. Nakayama implies $I_m = I_{m+1}$.
Now $(S^{-1}Q)^m = S^{-1}Q^m = S^{-1}I_m$, $(S^{-1}Q)^{m+1} = S^{-1}Q^{m+1} = S^{-1}I_{m+1}$, so $(S^{-1}Q)^m = (S^{-1}Q)^{m+1}$.
Nakamaya for R_Q gives $(S^{-1}Q)^m = 0$. But by (3.4), $S^{-1}Q'$ is prime, $\subsetneq S^{-1}Q$. #.

(6.12): R Noetherian, I proper ideal, generated by n elements. Then $\mathrm{ht}\, P \leq n$, for each minimal prime P over I.

Proof: By induction on n. $n=1$ is (6.10), so assume $n>1$.
(6.11) $\Rightarrow$ we may assume, by passing to R_P, that R is local with maximal ideal P.
Pick any prime Q maximal subject to $Q \subsetneq P$. We show that $\mathrm{ht}\, Q \leq n-1$.
Since P is minimal over I, $Q \not\supset I$. By assumption there are generators $a_1, \ldots, a_n$ for I, and assume $a_n \notin Q$. P is the only prime containing $Q + Ra_n$.
So as in the proof of (6.10) we have that $R/(Q + Ra_n)$ is Artinian.
The maximal ideal of an Artinian local ring is nilpotent. So there is m such that $a_i^m \in Q + Ra_n$ for all $i \leq n-1$. Write $a_i^m = x_i + r_i a_n$, $x_i \in Q$, $r_i \in R$.
Any prime containing $x_1, \ldots, x_{n-1}$ and a_n contains $a_1, \ldots, a_n$.
Also, $\sum_{i=1}^{n-1} Rx_i \leq Q$.
Claim: Q is a minimal prime over $\sum_{i=1}^{n-1} Rx_i$.
Proof: Write $\bar{R} = R/\sum Rx_i$; add bars for images in $\bar{R}$. The unique maximal ideal $\bar{P}$ of $\bar{R}$ is a minimal prime over $\overline{Ra_n}$. Apply (6.10) to $\bar{P}$: get $\mathrm{ht}(\bar{P}) \leq 1$.
Thus $\bar{Q}$ must be of height 0.
From the claim we can apply induction hypothesis to Q and get $\mathrm{ht}\, Q \leq n-1$.

(6.13): In a Noetherian ring, each prime has finite height. (bounded by the number of generators of the prime).

(6.14): Every local Noetherian ring has finite dimension, $\leq$ minimal number of generators for the maximal ideal $= R/P$ vector space dimension of P/P^2. (by (6.9))

A regular local ring is one where $\dim R =$ vector space dimension of P/P^2.
These are necessarily integral domains (not proved here).

In general, $\dim R$ can be less than v.s.dim P/P^2, but there is an ideal I with P minimal prime over I such that $\dim R =$ minimal number of generators of I. (Converse of general principal ideal theorem).

In geometry, regularity $\leftrightarrow$ non-singularity. Come back later to regular local rings of dimension 1 - "discrete valuation rings".

(6.15): A Noetherian ring satisfies the descending chain condition for primes

7. Valuation Rings

Definition: An integral domain A with field of fractions K is a **valuation ring** of K if for each $0 \neq x \in K$, either $x \in A$ or $x^{-1} \in A$ (or both).

Example: $K = \mathbb{Q}$, $A = \mathbb{Z}_{(p)}$, p prime.

(7.1): Let A be a valuation ring with fraction field K.

(i) A is a local ring.

(ii) If $A \subseteq B \subseteq K$ then B is a valuation ring.

(iii) A is integrally closed

Proof: (i) Let P be the set of non-units of A. Thus $x \in P$ iff $x = 0$ or $x^{-1} \notin A$.
We show P is an ideal.
If $a \in A$, $x \in P$ then $ax \in P$, since otherwise $(ax)^{-1} \in A$ and so $x^{-1} = a(ax)^{-1} \in A$.
If $x, y \in P$ then $x+y \in P$: either $xy^{-1} \in A$ or $x^{-1}y \in A$. If $xy^{-1} \in A$ then $x+y = (1 + xy^{-1})y$, which is of the form ay and so is in P.
Similarly for $x^{-1}y \in A$.

(ii) Trivial.

(iii) Let $x \in K$ be integral over A. Then $x^n + a_{n-1}x^{n-1} + \cdots + x_0 = 0$, some $a_i \in A$.
Suppose $x \notin A$. Then $x = -(a_{n-1} + a_{n-2}x^{-1} + \cdots + a_0 x^{-n+1})$, but this lies in A as x^{-1} does. #.

We aim to prove:

(7.2): Let R be an integral domain with fraction field K. Then the integral closure T of R in K is the intersection of all the valuation rings of K containing R.

Example: $\mathbb{Z}$ is the intersection of $\mathbb{Z}_{(p)}$, p prime, $\subseteq \mathbb{Q}$.

Recipe for valuation rings: Take algebraically closed field F, K field.
Consider pairs (R', φ'), R' = subring of K, φ': $R' \to F$, ring homomorphism.
Partially order: $(R_1, \varphi_1) \leq (R_2, \varphi_2)$ iff $R_1 \subseteq R_2$ and $\varphi_2|_{R_1} = \varphi_1$.
Assume we have pairs. Any ascending chain of pairs has an upper bound of the form (R_0, φ_0), where R_0 is the union of the rings R' in the chain, and φ_0 restricts to R' to give φ'.
Zorn's Lemma says that the family of such pairs has a maximal member, (not necessarily unique), say (A, θ)

(7.3): A is a valuation ring of K.

Proof: **Step 1:** A is a local ring with $\ker \theta = P$ its unique maximal ideal.

Proof: $\theta(A)$ is a subring of F, a field, and so is an integral domain.
So $P = \ker \theta$ is a prime ideal. We can extend θ to a homomorphism

$\varphi: A_P \to F$ for $a \in A$ and $s \in S = A \setminus P$.
$a/s \longmapsto \theta(a)/\theta(s)$

The maximality of (A, θ) implies $A = A_P \subseteq K$. Hence A is a local ring with maximal ideal P.

Next, take $x \neq 0$ in K. We want to show $x \in A$ or $x^{-1} \in A$.

Step2: Either ideal $PA[x]$ of $A[x]$ is proper, or ideal $PA[x^{-1}]$ of $A[x^{-1}]$ is proper.

Proof: Suppose $PA[x] = A[x]$ and $PA[x^{-1}] = A[x^{-1}]$.

Thus, $1 \in PA[x]$, say $1 = a_m x^m + \cdots + a_0$, some $a_i \in P$ - ①

$1 \in PA[x^{-1}]$, say $1 = b_n x^{-n} + \cdots + b_0$, some $b_i \in P$ - ②.

We pick m, n minimal, and may assume $m \geq n$.

Multiply ② by x^n: $(1 - b_0)x^n = b_n + \cdots + b_1 x^{n-1}$ - ③.

But $b_0 \in P$ and so $1 - b_0 \notin P$ and is a unit in A (Step 1).

So ③ gives $x^n = c_n + \cdots + c_1 x^{n-1}$ with $c_i \in P$, so $x^m = c_n x^{m-n} + \cdots + c_1 x^{m-1}$.

Substituting in ① gives an equation contradicting the minimality of m.

Step3: We may assume $I = PA[x] \subsetneq A[x]$. Let $B = A[x]$. We show that $B = A$ and hence $x \in A$.

Proof: Let Q be a maximal ideal of B containing I. Thus $Q \cap A = P$ since $Q \cap A$ is a proper ideal of A and P is in it. Regard A/P as a subring of B/Q. Both are fields, say k, k_1, and $k_1 = k[\bar{x}]$, where $\bar{x}$ is the image of x in k_1. (6.4) gives that k_1 is an algebraic extension of k.

But θ induces a map $\bar{\theta}: k = A/P \to F$, and this extends to a map $\varphi: k_1 \to F$, (F algebraically closed). φ lifts back to give a map $B \to F$ extending θ. The maximality of (A, θ) implies $A = B$.

Proof of (7.2): Let A be a valuation ring of K containing R. A is integrally closed by (7.1)(iii) and hence the integral closure T of R is in A.

Conversely, if $x \notin T$ then $x \notin R[x^{-1}]$. Let $A_1 = R[x^{-1}]$. So x^{-1} is not a unit of A_1, and is therefore contained in a maximal ideal P_1 of A_1.

Let F be the algebraic closure of A_1/P_1. The canonical map $A_1 \xrightarrow{\varphi} A_1/P_1 \subseteq F$ restricts to give a map $R \to F$. By Zorn, there is a maximal pair (A, θ) above (A_1, φ) and (7.3) says A is a valuation ring. Since θ extends φ, $\theta(x^{-1}) = \varphi(x^{-1}) = 0$. So $x \notin A$.

The reason for the terminology 'valuation ring' is that one may associate a non-Archimidean valuation $v: K^\times \to \Gamma$, an ordered abelian group (written additively), satisfying: (i) $v(xy) = v(x) + v(y)$

(ii) $v(x+y) \geq \min(v(x), v(y))$ - ultrametric inequality,

so that $R = \{x \in K: x = 0 \text{ or } v(x) \geq 0\}$, for a valuation ring, and given such a v, R is a valuation ring.

If $\Gamma \cong \mathbb{Z}$ we say R is a discrete valuation ring.

Discrete Valuation Rings.

Examples: (i) $v_p : \mathbb{Q}^\times \to \mathbb{Z}$ where a, b coprime to p, p prime.
$ap^n/b \longmapsto n$, - p-adic valuation.
DVR $\mathbb{Z}_{(p)}$.

(ii) $v_f : k(x)^\times \to \mathbb{Z}$ f irreducible in $k[x]$, g, h coprime to f.
$f^n g/h \longmapsto n$
DVR $k[x]_{(f)}$

A valuation ring A is Local (7.1). Maximal ideal $P = \{a : v(a) > 0\}$.
If $v(a) = v(b)$ then $v(ab^{-1}) = 0$, so ab^{-1} is a unit in A. So $(a) = (b)$.
If $I \neq 0$ is an ideal of A, there is a least k such that $v(a) = k$ for some $a \in I$.
So I contains every b with $v(b) \geq k$. So $I = I_k = \{a : v(a) \geq k\}$.
There is a single chain of ideals in our valuation ring:
$P = I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$, thus A is Noetherian.

Also, $v : K^\times \to \mathbb{Z}$ is surjective (may as well assume this), and so there is x with $v(x) = 1$ and so $P = (x)$. (Have used this above). So $I_k = (x^k)$.
So P is the only non-zero prime ideal. Thus a discrete valuation ring is a Noetherian local domain of dimension 1.

(7.4): Let R be a Noetherian local domain of dimension 1, with unique maximal ideal P, and $k = R/P$, field. The following are equivalent:
(i) R is a discrete valuation ring
(ii) R is integrally closed
(iii) P is principal
(iv) Vector space $\dim_k (P/P^2) = 1$
(v) every non-zero ideal is a power of P.
(vi) $\exists\, x \in P$ such that every ideal is of the form (x^k) for $k \geq 0$.

Proof: (i) $\Rightarrow$ (ii): Done in (7.1).

(ii) $\Rightarrow$ (iii): Let $0 \neq a \in P$. Then $R/(a)$ has only one prime $P/(a)$, its nilradical, so it is nilpotent. So $P^n \subseteq (a)$, some n, $P^{n-1} \not\subseteq (a)$, say.
Choose $b \in P^{n-1}$ with $b \notin (a)$ and let $x = a/b \in K = \text{f.f. } R$. Thus $x^{-1} \notin R$ since $b \notin (a)$, and hence x^{-1} is not integral over R. [R is integrally closed by supposition]
Claim: $x^{-1}P \not\subseteq P$. Suppose $x^{-1}P \subseteq P$. Then P is a $R[x^{-1}]$-module, finitely generated as an R-module, and any non-zero cyclic submodule $\cong R[x^{-1}]$, and f.g. as an R-module, a contradiction.
But $x^{-1}P \subseteq R$ by construction, so $x^{-1}P = R$. So $P = (x)$.

(iii) $\Rightarrow$ (iv): P principal $\Rightarrow$ P/P^2 cyclic and so $\dim_k (P/P^2) \leq 1$. By Nakayama, $P \neq P^2$.

(iv) $\Rightarrow$ (v): If $I \neq 0$ then $P^n \subseteq I$ (as in (ii) $\Rightarrow$ (iii)). But P principal, by Nakayama, say $P = (x)$. $\exists\, r$ such that $I \subseteq P^r$, $I \not\subseteq P^{r+1}$, and hence $\exists\, y \in I$, $y = ax^r$, $y \notin P^{r+1}$. So $a \notin P$, so a is a unit in R. So $x^r \in I$, and hence $P^r \subseteq I$. So $I = P^r$.

(v) ⇒ (vi): By Nakayama, $P \neq P^2$. Take $x \in P \setminus P^2$. But $(x) = P^r$ by hypothesis. So $(x) = P$. Hence $P^r = (x^r)$.

(vi) ⇒ (i): $P = (x)$, and by Nakayama, $P^r \neq P^{r+1}$. Claim R is a valuation ring. If $y \in K = ff R$, $y \notin R$, then consider $\{r \in R : ry \in R\}$, an ideal of R, and so by supposition is (x^k) for some k. So $yx^k \in R \setminus P$ and hence is a unit of R. So inverse of y is in R. So R is a valuation ring.
If $a \in R$ then $(a) = (x^k)$ for exactly one value of k. Define $v(a) = k$.
Extend to $K^\times$ by $v(ab^{-1}) = v(a) - v(b)$.

R an integral domain, $ff = K$. An R-submodule M of K is a fractional ideal of R if $xM \subseteq R$ for some $x \neq 0$, $x \in R$. (Usual ideals of R are fractional).
Every f.g. R-submodule of M is also a fractional ideal: if we have $Rx_1 + \cdots + Rx_n$, then $x_i = y_i z^{-1}$ for some $y_i \in R$, $z \in R$.

An f.g. R-submodule of K is an invertible ideal if there is an R-submodule N of K such that $MN = R$. This N is unique [$\{x \in K : xM \subseteq R\} =: X$, then $N \subseteq X = XMN \subseteq RN = N$], and is a f.g. R-module, and hence is a fractional ideal.

(7.5): Let R be a Noetherian local domain. Then R is a discrete valuation ring iff every non-zero fractional ideal of R is invertible.

M invertible. Then $\exists$ N such that $MN = R$, N unique. $\exists$ $x_i \in M$, $y_i \in N$ with $\sum x_i y_i = 1$. So for $m \in M$, $m = \sum (y_i m) x_i$. $y_i m \in R$. So $\{x_i\}$ generate M. N is invertible, and so is finitely generated too. So we have a group.

Proof of (7.5): Let P be a maximal ideal of discrete valuation ring R. So $P = Rx$, some x. Let M be a fractional ideal, so there is $y \in R$ such that $yM \subseteq R$. Thus yM is an ideal of R, $yM = Rx^r$, say. So $M = Rx^{r-s}$, where $s = v(y)$.
All principal fractional ideals are invertible.
Conversely, it is enough to show every non-zero ideal of R is a power of P.
Suppose false. Consider $\mathcal{S} = \{$non-zero ideals not equal to a power of $P\}$.
Take a maximal member I of $\mathcal{S}$. Then $I \neq P$, and so $I \subsetneq P$. Hence $P^{-1}I \subsetneq P^{-1}P = R$.
$P^{-1}I$ is a proper ideal of R and $P^{-1}I \supseteq I$. But $P^{-1}I \neq I$, since if so, then $I = PI$ and so $I = 0$ by Nakayama. Maximality of I gives that $P^{-1}I$ is a power of P and hence I is a power of P. ⁂

Dedekind Domains.

(7.6): Let R be a Noetherian domain of dimension 1. The following are equivalent:
(i) R integrally closed.
(ii) Every I with $\sqrt{I}$ a maximal ideal Q, is a power of Q.
(iii) Every local ring R_Q with Q maximal is a discrete valuation ring.

A Dedekind domain is one satisfying these three conditions.

Example: integral closure of $\mathbb{Z}$ in any finite extension of $\mathbb{Q}$, ie, the ring of integers in any number field.

For proof of (7.6) we need to know that integral closure behaves well under localisation:

(7.7): Let $R_1 \subseteq R_2$ rings with T = integral closure of R_1 in R_2. S a multiplicatively closed subset of R_1. Then $S^{-1}T$ is the integral closure of $S^{-1}R_1$ in $S^{-1}R_2$.

Proof: By (5.6), $S^{-1}T$ is integral over $S^{-1}R_1$. Conversely, if $r/s \in S^{-1}R_2$ is integral over $S^{-1}R_1$, then have $(r/s)^n + (r_1/s_1)(r/s)^{n-1} + \cdots + (r_n/s_n) = 0$, with $r_i \in R_1$, $s_i \in S$. Let $t = s_1 \cdots s_n$. Multiply by $(st)^n$; get an equation showing that rt is integral over R_1. So $r/s = rt/st \in S^{-1}T$.

Integrality is a local property:

(7.8): R an integral domain. Then R is integrally closed
iff R_P integrally closed for any prime P
iff R_Q integrally closed for any maximal Q.

Proof: Let T = integral closure of R in K = f.f.R. There is an embedding $f: R \to T$, surjective iff R is integrally closed. Get induced map, $f_P: R_P \to T_P$. Since T_P is integral closure of R_P by (7.7), f_P is surjective iff R_P is integrally closed. But f surjective iff f_P is for all primes P
iff f_Q is for all maximals Q.

Proof of (7.6): (i) $\Leftrightarrow$ (iii): (7.8) and (7.4).

(ii) $\Leftrightarrow$ (iii): Suppose all ideals I with $\sqrt{I} = P$ are powers of P (any maximal P). Consider a non-zero ideal J of R_P with $S = R \setminus P$. So $I = \{r \in R : r/1 \in J\}$ is an ideal containing a power of P. So $I = P^m$ for some m by supposition. Hence $J = (S^{-1}P)^m$. Apply (7.4). R_P is a discrete valuation ring. Conversely, let I be such that $\sqrt{I} = P$, maximal. Then $S^{-1}I$ is a non-zero ideal R_P, and so is $(S^{-1}P)^m$ by supposition. So $I = P^m$.
(see sheet at end...)

(7.9): In a Dedekind domain R every non-zero ideal I has a unique factorisation as a product of prime ideals.

Sketch proof: R/I has only finitely many primes, all maximal, so is Artinian (example sheet). So R/I is a direct product of Artinian local rings (example sheet). $I = \cap I_j$, with $\sqrt{I_j}$ = maximal P_j. But in a Dedekind domain, $I_j = P_j^{m_j}$, some m_j. Thus $I = \cap P_j^{m_j}$.

For coprime ideals $\{I_j\}$ (ie $I_j + I_k = R$, $j \neq k$), then $\cap I_j = \prod I_j$.

Proof: By induction $n = 2$: $I_1 + I_2 = R$. So $I_1 \cap I_2 = (I_1 + I_2)(I_1 \cap I_2)$
$= I_1(I_1 \cap I_2) + I_2(I_1 \cap I_2) \subseteq I_1 I_2$. And $I_1 I_2 \subseteq I_1 \cap I_2$, clearly.

In general, assume $\bigcap_{j=1}^{m-1} I_j = \prod_{j=1}^{m-1} I_j = J$. Let $I_j + I_m = R$ for each $j \le m-1$.
So $x_j + y_j = 1$ for some $x_j \in I_j$, $y_j \in I_m$. So $\prod_{j=1}^{m-1} x_j = \prod_{j=1}^{m-1}(1-y_j) \equiv 1 \pmod{I_m}$
So $J + I_m = R$. So $\prod_{j=1}^{m} I_j = J I_m = J \cap I_m$ (by induction), $= \bigcap_{j=1}^{m} I_j$.

(7.10): R Noetherian integral domain. Then R is a Dedekind domain iff all its non-zero fractional ideals are invertible.
Proof: Omitted. Use (7.8) and that invertibility is a local property.

Thus the non-zero fractional ideals form a group, the class group.

8. I-adic Topology

R, commutative ring with a 1.

A filtration is an infinite descending chain $M_0 \supseteq M_1 \supseteq \cdots$ of submodules of a module M.
I an ideal of R. (M_n) is an I-filtration if $IM_n \subseteq M_{n+1}$.
It is a stable I-filtration if $\exists$ N such that for $n \ge N$, $IM_n = M_{n+1}$.
To study stable I-filtrations define the Rees ring $R^* = \bigoplus_{n=0}^{\infty} I^n$, isomorphic to the subring $R + Ix + I^2x^2 + \cdots$ of $R[x]$, via $I^n \leftrightarrow I^n x^n$. It is a graded ring.

A graded ring T is a ring of form $\bigoplus_{n=0}^{\infty} T_n$, where the T_n are additive subgroups and $T_m T_n \subseteq T_{m+n}$ for $m, n \ge 0$. In particular, T_0 is a subring, $T_+ = \bigoplus_{n \ge 1} T_n$ is an ideal of T. (T_n are the components).

If (M_n) is an I-filtration of R-module M, then $M^* = \bigoplus_{n=0}^{\infty} M_n$ is a graded R-module.
A graded T-module N is of form $\bigoplus_{n=0}^{\infty} N_n$, with $T_m N_n \subseteq N_{m+n}$. N_n is a T_0-module.

A homogeneous element is one lying in some component.
A graded T-module map $\theta : N \to N' = \oplus N'_n$ is a module map such that $\theta(N_n) = N'_n$.

(8.1): For a graded ring T, the following are equivalent:
(i) T is a Noetherian ring.
(ii) T_0 is a Noetherian ring and T is of finite type over T_0.
Proof: (i) $\Rightarrow$ (ii): $T_0 \cong T/T_+$ and hence is a Noetherian T-module, so is a Noetherian T_0-module. Ie, T_0 is a Noetherian ring.
T Noetherian implies T_+ is a finitely generated ideal. We may assume, by taking components if necessary, that our finite generating set consists of homogeneous elements, say $x_1, \ldots, x_s$ of degrees $m_1, \ldots, m_s$.
Let T' = subring of T generated by T_0 and $x_1, \ldots, x_s$.
Claim: $T_n \subseteq T'$ for each n.
Use induction: $T_0 \subseteq T'$. Let $n > 0$, and consider T_n, assuming claim for smaller degrees. Take $y \in T_n$. So $y \in T_+$, and hence $y = \sum t_j x_j$ for

some $t_j \in T_{n-m_j}$. But by induction, each $t_j \in T'$. Hence $y \in T'$.

(ii)⇒(i): From Hilbert's Basis Theorem since T is an image of $T_0[x_0, \dots, x_m]$, some m. If R is Noetherian then R^* is Noetherian: it is generated by R and $x_1, \dots, x_s$, where $x_1, \dots, x_s$ (of degree 1 in R^*) generate I as an ideal of R.

(8.2): R Noetherian, M a f.g. R-module, (M_n) an I-filtration for an ideal I. The following are equivalent:

(i) M^* is an f.g. R^*-module.

(ii) (M_n) is a stable I-filtration.

Proof: M is a Noetherian R-module and hence M_n is f.g. R-module, and so $M_0 \oplus \dots \oplus M_n$ is a f.g. R-module. But $M_0 \oplus \dots \oplus M_n$ is the sum of the first few components of M^*. It generates an R^*-submodule of M^*: $M_0 \oplus \dots \oplus M_n \oplus IM_n \oplus I^2M_n \oplus \cdots$ [Note: $I^2M_{n-1} \subseteq IM_n$, since we have an I-filtration]. Call it M_n^*. It is an f.g. R^*-module.
Clearly, $M_0^* \subseteq M_1^* \subseteq \cdots$, and $M^* = \cup M_n^*$. But R^* is Noetherian, and so this chain terminates, so $M^* = M_N^*$ some N, iff M^* is a f.g. R^*-module. (iff M^* is Noetherian). But, $M_N^* = M_{N+r}^*$, $r \geq 0$, is equivalent to $M_{N+r} = I^r M_N$, $r \geq 0$.

(8.3) (Artin-Rees Lemma): R Noetherian with ideal I. Let M be an f.g. R-module and (M_n) be a stable I-filtration of M. Let N be a submodule of M. Then $(N \cap M_n)$ is a stable I-filtration of N.

Immediately, applying this to $(M_n) = (I^n M)$, we get:

(8.4): There is s such that $(I^n M) \cap N = I^{n-s}[(I^n M) \cap N]$ for all $n \geq s$.

Proof of (8.3): Certainly $(N \cap M_n)$ is an I-filtration of N: $I(N \cap M_n) \subseteq IN \cap IM_n \subseteq N \cap M_{n+1}$, since (M_n) is an I-filtration. So $(N \cap M_n)$ yields a graded R^*-module $\oplus N \cap M_n$ of $M^* = \oplus M_n$. But since (M_n) is stable, (8.2) gives that M^* is an f.g. R^*-module, and hence is a Noetherian R^*-module. (since R^* is Noetherian). So $\oplus N \cap M_n$ is an f.g. R^*-module.
(8.2) again gives that $(N \cap M_n)$ is a stable I-filtration.

(8.5) (Krull's Intersection Theorem): R Noetherian with ideal I, M a f.g. R-module. Set $N = \bigcap_{n=0}^{\infty} I^n M$.

(i) There is $r \in 1+I$ with $rN = 0$.

(ii) If $I \subset J(R)$ then $N = 0$.

(iii) If R is an integral domain then $\bigcap_{n=0}^{\infty} I^n = 0$.

(iv) If R is local then $N = 0$.

Proof: (i), (ii): By (8.4), $I^n M \cap N = I^{n-s}[I^n M \cap N]$ for some s, for $n \geq s$.
But RHS $= I^{n-s} N$, LHS $= N$, so $N = I^{n-s} N$. Apply Nakayama.

(iii): If R is an integral domain, take $M = R$. If $N \neq 0$ then $rN = 0$, some $r \in 1+I$

This would give zero divisors. ✱.

(iv) If R is local then all ideals are in $J(R)$. So (ii) applies and $N=0$.

Topology Associated with Filtrations

Filtration: $M = M_0 \supseteq M_1 \supseteq \cdots$

Open sets: unions of sets of form $m + M_n$, for some $m \in M$, $n \in \mathbb{N} - \{0\}$.

Clearly, any union of these is open. Also, the intersection of $m_1 + M_{n_1}, \ldots, m_r + M_{n_r}$ is a union of sets of the form $m + M_n$, where $n = \max\{n_i\}$.

Thus an intersection of finitely many open sets is open.

If $\cap M_n = 0$ we can put a metric on M: $d(m_1, m_2) = p^{-k}$, where $k = \max_n (m_1 - m_2 \in M_n)$, and p is a rational prime.

This metric yields the same topology as above.

The choice of p is important in the special case $M = \mathbb{Z}$, $M_n = p^n\mathbb{Z}$.

Usually p is unimportant; we're just interested in the topology. Two filtrations determine the same topology if for each n there is $\begin{cases} s(n) \text{ such that } M_n \supseteq M'_{s(n)} \\ t(n) \text{ such that } M'_n \supseteq M_{t(n)}. \end{cases}$

The I-adic topology on M: one from filtration $(I^n M)$; in particular on R: the one from filtration (I^n). Observe that all stable I-filtrations yield the same topology:

Since $IM_n \subseteq M_{n+1}$ we have $I^n M \subseteq M_n$. Also, $IM_n = M_{n+1}$ for all $n \geq N$ and hence $M_{n+N} = I^n M_N \subseteq I^n M$.

Examples: (i) Take $I = (p)$ in $\mathbb{Z}$. p-adic topology. Two integers are close together if their difference is divisible by a large power of p.

(ii) Take $I = (f)$ in $k[X]$, f irreducible. Similarly.

Let (M_n) be a stable I-filtration, R Noetherian, M a finitely generated R-module. If $N \subseteq M$ then by (8.3), then $N \cap M_n$ is a stable I-filtration on N, and so the subspace topology on N induced from the I-adic topology on M is the same as the I-adic topology on N.

Definition: A Cauchy sequence (x_n) in M is a sequence such that for any open set U containing 0 there is $a(U) \in \mathbb{N}$ such that for $r, s \geq a(U)$, $x_r - x_s \in U$.

It is enough to look at open sets U of the form M_n. So a Cauchy sequence is one where for $r, s \geq a(M_n)$, $x_r \equiv x_s \pmod{M_n}$. Two Cauchy sequences $(x_n), (y_n)$ are equivalent if $x_n - y_n \to 0$. (ie. for any open U containing 0, there is $b(U)$ with $x_n - y_n \in U$ for $n \geq b(U)$).

Definition: The I-adic completion $\hat{M}$ of M is the set of equivalence classes.
$[x_n] + [y_n] = [x_n + y_n]$.
The I-adic completion $\hat{R}$ of R is the set of equivalence classes of Cauchy sequences with I-adic topology, $[r_n][s_n] = [r_n s_n]$, and addition as above.

Thus $\hat{R}$ is a ring, $\hat{M}$ is an $\hat{R}$-module: $[r_n][x_n] = [r_n x_n]$.
There is a ring homomorphism $R \to \hat{R}$
$r \longmapsto [r]$, equivalence class of the constant sequence with terms r. The kernel is $\cap I^n$.
Similarly, there is an additive group homomorphism $M \to \hat{M}$, with kernel $= \cap I^n M$.
$x \mapsto [x]$

Krull's Intersection Theorem (8.5) gives cases when these maps are injective.
For example, $R \to \hat{R}$, $M \to \hat{M}$ } injective if { R is integral domain, $I \subset J(R)$

Definition: R is complete if $R \to \tilde{R}$ is an isomorphism.

There is another way of defining things, via inverse limits, $\varprojlim (M/M_n)$ and $\varprojlim (R/I^n)$. [Take M_n stable I-filtration).
$\varprojlim (M/M_n) \subseteq \prod (M/M_n)$ - Cartesian product, allows infinitely many non-zero entries.
It equals $\{(\ldots, y_n + M_n, \ldots)$: if $r > s$ then under the canonical projection $M/M_r \to M/M_s$, have $y_r + M_r \mapsto y_s + M_s\}$

Have term-by-term addition. And multiplication in the case of $\varprojlim (R/I^n)$.
For each r we have a canonical projection $\varprojlim M/M_r \to M/M_r$
$\varprojlim R/I^r \to R/I^r$
We get map $\hat{M} \to \varprojlim (M/M_n)$: for $[x_n] \in \hat{M}$, set $y_n + M_n = x_{a(M_n)} + M_n$, where $a(M_n)$ is where the sequence stabilises, as in the definition of a Cauchy sequence.
Similarly $\hat{R} \to \varprojlim (R/I^n)$. These maps are injective: those sequences which eventually lie in M_n for each n are those equivalent to the zero sequence.
They are surjective: $[y_n] \to (\ldots, y_n + M_n, \ldots)$
Thus $\hat{M}$ can be identified with $\varprojlim (M/M_n)$. Inherit topology given by filtration.
$\hat{M}_n = \{(M_0, \ldots, M_n, \ldots)\}$
↑ zero elements in first $n+1$ positions.
$\hat{M}_n$ gives a filtration of $\hat{M} = \varprojlim (M/M_n)$.
Doing the same for $\hat{R} = \varprojlim (R/I^n)$, then get ideals of $\hat{R}$. In particular, $\hat{I}$ has elements with entry in R/I to be zero. $R/I \cong \hat{R}/\hat{I}$. More generally, $R/I^n \cong \hat{R}/\hat{I}^n$

Examples: $\mathbb{Z}_p$, p-adic integers, $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$

$k[[X_1,\dots,X_n]]$, power series, $\varprojlim k[X_1,\dots,X_n]/I^n$, where $I=(X_1,\dots,X_n)$.

- Here we identify a power series $1+x+x^2+\cdots$ with the sequence of partial sums $(0,\ 1+(x)^{\overset{=I}{},}\ 1+x+(x^2),\dots)$. (for $n=1$)

Note: if $\hat{r}\in\hat{I}$, then $\hat{1}+\hat{r}$ has multiplicative inverse $\hat{1}-\hat{r}+\hat{r}^2-\cdots$; this converges in $\hat{R}$, the I-adic completion. Thus if I is maximal in R and hence $R/I \cong \hat{R}/\hat{I}$ is a field, then any element of $\hat{R}$ not in $\hat{I}$ has an inverse; we can multiply by something to put it in the form $\hat{1}+\hat{r}$.

(8.7): If I is maximal in R then $\hat{R}$ is a local ring, with maximal ideal $\hat{I}$.

(8.8): Suppose R is Noetherian. If N is a submodule of a f.g. R-module M, then $\hat{N}$ is a submodule of $\hat{M}$, and $\widehat{M/N} \cong \hat{M}/\hat{N}$. Alternatively, if $0\to M_1\to M\to M_2\to 0$ is a short exact sequence of f.g. R-modules, then $0\to\hat{M}_1\to\hat{M}\to\hat{M}_2\to 0$ is exact.

Proof: By (8.3) the I-adic topology on N is the subspace topology induced from the I-adic topology on M. Two Cauchy sequences (x_n), (y_n) with all $x_n, y_n\in N$ are equivalent in M iff they are equivalent in N. Given open U in N it is of form $V\cap N$ for some open subset V of M. If $x_n-y_n\in U$ for large enough n, then $x_n-y_n\in V\cap N$. So $\hat{N}$ embeds in $\hat{M}$, $[x_n]_N\mapsto[x_n]_M$.

Viewing $\hat{M}$ as $\varprojlim (M/M_n)$, the image of this map is the set of elements of the form $(\dots, y_n+M_n,\dots)$, with $y_n+M_n\in (N+M_n)/M_n$

Now consider the map $\pi:\hat{M}\to\widehat{M/N}$, ie $\varprojlim M/M_n \to \varprojlim (M/(M_n+N))$

$$(\dots, y_n+M_n,\dots)\longmapsto(\dots, y_n+N+M_n,\dots)$$

The kernel is (the image of) $\hat{N}$.

Finally show that π is surjective. We need to see that we can find $z+M_{n+1}$ in the following diagram, given the rest of it: (Inductive step is pulling back an element of $\varprojlim M/N$)

$$\begin{array}{ccc} x+N+M_{n+1} & \longrightarrow & y+N+M_n \\ \uparrow & & \uparrow \\ z+M_{n+1} & \longrightarrow & y+M_n \end{array}$$

We want $z\in y+M_n$, $z\in x+N+M_{n+1}$. We know $x\in y+N+M_n$, and so $x+n\in y+M_n$ for some $n\in N$. Set $z=x+n$.

(8.9): Let R be Noetherian, I an ideal. Then $\hat{R}$, the I-adic completion, is Noetherian.

Proof: Since R is Noetherian, the ideal I is finitely generated, by $r_1,\dots,r_n$, say. Let J_1 be the ideal of $R[X_1,\dots,X_n]$ generated by $(X_1-r_1,\dots,X_n-r_n)$. This is the kernel of the map $R[X_1,\dots,X_n]\to R$.

$$X_i\longmapsto r_i.$$

Let $J_2=(X_1,\dots,X_n)$, ideal of $R[X_1,\dots,X_n]$. The J_2-adic topology on the $R[X_1,\dots,X_n]$-module $R[X_1,\dots,X_n]/J_1\cong R$ is the same as the I-adic topology on R, since $(J_2+J_1)/J_1 \leftrightarrow I$.

Forming the completion w.r.t J_2-adic topology, $\left(R[X_1,\dots,X_n]/J_1\right)^\wedge \cong (R[X_1,\dots,X_n])^\wedge/\hat{J}_1$, by previous lemma. But $(R[X_1,\dots,X_n])^\wedge \cong R[[X_1,\dots,X_n]]$, which is Noetherian by (11.11).

Thus the I-adic completion of R, which is isomorphic to LHS of $\otimes$ is an image of a Noetherian ring, and so is Noetherian.

(8.10): R Noetherian, M a f.g. R-module. $\hat{R} \otimes_R M \to \hat{M}$ is an isomorphism, via the composition $\hat{R} \otimes_R M \to \hat{R} \otimes_R \hat{M} \to \hat{R} \otimes_{\hat{R}} \hat{M} = \hat{M}$

↑ remember: $\hat{R} \times \hat{M} \to \hat{R} \otimes_{\hat{R}} \hat{M}$, universal $\hat{R}$-bilinear map, is R-bilinear, so get map indicated.

Proof: M is f.g., say by $x_1, \dots, x_n$. Define free R-module on n generators $y_1, \dots, y_n$
$F \to M$ - R-module map. So have: $0 \to N \to F \to M \to 0$.
$y_i \mapsto x_i$
By (4.5) and (8.8) we get:

$$\begin{array}{ccccccc} \hat{R} \otimes_R N & \to & \hat{R} \otimes_R F & \to & \hat{R} \otimes_R M & \to & 0 \quad \text{-exact} \\ \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\ 0 \to \hat{N} & \longrightarrow & \hat{F} & \xrightarrow{\delta} & \hat{M} & \longrightarrow & 0 \end{array}$$

where α, β, γ are of the type described in the statement.
β is an isomorphism, since F is free. Since δ is surjective, γ is surjective.
Thus we've proved that for any f.g. module M, the map $\hat{R} \otimes_R M \to \hat{M}$ is surjective, thus α is also surjective.
Must show γ is injective. Let $x \in \ker \gamma$. Exactness at $\hat{R} \otimes_R M$ shows that x is the image of $y \in \hat{R} \otimes_R F$, say. Consider $\beta(y) \in \ker \delta$.
Exactness at $\hat{F}$ gives that $\beta(y)$ is the image of an element of $\hat{N}$, which because α is surjective is the image of $z \in \hat{R} \otimes_R N$.
This z maps to $y_1 \in \hat{R} \otimes F$ with $y_1 - y \in \ker \beta$. But β is an isomorphism, so $y_1 = y$. Thus y is an image, and hence in the kernel of the map to $\hat{R} \otimes M$. So its image x is zero.
(β an isomorphism: $\hat{R} \otimes_R F = \hat{R} \otimes_R R^n \cong (\hat{R} \otimes_R R)^n \cong (\hat{R})^n = \hat{R^n} = \hat{F}$)

Associated Graded Rings

$R \supseteq I \supseteq I^2 \supseteq \cdots$, $M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$. Form $\operatorname{gr}_I R = \bigoplus_{n=0}^{\infty} I^n/I^{n+1}$, $\operatorname{gr} M = \bigoplus_{n=0}^{\infty} M_n/M_{n+1}$.
Multiplication in $\operatorname{gr} R$: $(x_m + I^{m+1})(x_n + I^{n+1}) = x_m x_n + I^{m+n+1}$
$\in I^m/I^{m+1}$ $\in I^n/I^{n+1}$ $\in I^{m+n}/I^{m+n+1}$

$\operatorname{gr} M$ is a graded $\operatorname{gr}_I R$-module if (M_n) is an I-filtration.

(8.11): (i) If R is Noetherian then $\operatorname{gr}_I R$ is Noetherian.
(ii) If M is a f.g. R-module and (M_n) is a stable I-filtration, then $\operatorname{gr} M$ is a f.g. graded $\operatorname{gr}_I R$-module.

Proof: (i) If R is Noetherian, the ideal I is f.g. by $x_1, \dots, x_s$, says, with $\bar{x}_i = x_i + I^2 \in I/I^2$. Then $\operatorname{gr}_I R = R/I[\bar{x}_1, \dots, \bar{x}_s]$, ring of finite type over R/I.
Corollary of Hilbert's Basis Theorem says that such a ring is Noetherian.
(ii) If (M_n) is a stable I-filtration, then for some N, $M_{N+r} = I^r M_N$, $\forall r \geq 0$.
Hence $\operatorname{gr} M$ is generated as a $\operatorname{gr} R$-module by $\bigoplus_{n \leq N} M_n/M_{n+1}$. But each M_n/M_{n+1} is a Noetherian R-module annihilated by I, hence is a f.g. R/I-module.
So $\bigoplus_{n \leq N} M_n/M_{n+1}$ is a f.g. R/I-module. So $\operatorname{gr} M$ is f.g. as a $\operatorname{gr} R$-module.

The particular case we are going to be interested in is where R is a Noetherian local ring with maximal ideal P. I is an ideal with $\sqrt{I} = P$ (so $P^n \leq I \leq P$, some n) $gr_P R$ is an affine R/P-algebra. Properties of R may be deduced from the theory of affine algebras.

Hilbert Functions.

Noetherian graded ring $T = \bigoplus_{n=0}^{\infty} T_n$, graded T-module $N = \oplus N_n$, T generated by T_0 and $x_1, \ldots, x_s$, homogeneous of degrees $k_1, \ldots, k_s$.

Poincaré series of N is the power series $P(N,t) = \sum_{n=0}^{\infty} \lambda(N_n) t^n \in \mathbb{Z}[[t]]$, where λ is an additive function on f.g. T_0-modules. ('Additive': $\lambda(U) + \lambda(V) = \lambda(W)$ if $\exists$ exact sequence $0 \to U \to W \to V \to 0$)

Example: If T_0 is a field then can take λ = vector space dimension.
More generally, if T_0 is Artinian, take λ = composition length.
(Ie, given f.g. T_0-module U, with $U = U_0 > U_1 > U_2 > \ldots > U_r = 0$ (each $U_0 > U_1$ maximal, each $U_1 > U_2$ maximal)

- composition series for U. $\lambda(U) = r$, the composition length.
Each U_j/U_{j+1} is a simple T_0-module. r is independent of choice of series).

(8.12) (Hilbert, Serre): $P(N,t)$ is a rational function in t, of the form $\frac{f(t)}{\prod_{i=1}^{s}(1-t^{k_i})}$, where $f(t) \in \mathbb{Z}[t]$, k_i the degree of generator x_i

Proof: By induction on the number of generators s of x_i.

$s=0$: $T = T_0$ and so N is a f.g. T_0-module. So $N_n = 0$ for large enough n.
Clearly $P(N,t)$ is a polynomial.

$s>0$: Assume true for $s-1$. Multiplication by x_s maps $N_n \to N_{n+k_s}$, and we get an exact sequence $0 \to K_n \to N_n \to N_{n+k_s} \to L_{n+k_s} \to 0$. - (*)
Let $K = \bigoplus_{n=0}^{\infty} K_n$, $L = \bigoplus_{n=0}^{\infty} L_n$. $K \leq M$, L is a quotient of M, so both are f.g. T-modules. Both K and L are annihilated by $x_s \in T$. ($K = \ker$, $L = N/x_s N$), and so they are $T_0[x_1, \ldots, x_{s-1}]$-modules.
Apply λ to (*) to get $\lambda(K_n) - \lambda(N_n) + \lambda(N_{n+k_s}) - \lambda(L_{n+k_s}) = 0$.
Multiply by t^{n+k_s} and sum wrt n: $t^{k_s} P(K,t) - t^{k_s} P(N,t) + P(N,t) - P(L,t) = g(t)$, g a polynomial.
Apply the induction hypothesis to $P(K,t)$ and $P(L,t)$.

(8.13): If each $k_i = 1$ then $\lambda(N_n)$ is a polynomial in n, with rational coefficients, of degree $d-1$, (for large enough n), where d = order of pole of $P(N,t)$ at $t=1$.

Proof: If each $k_i = 1$, $P(N,t) = \frac{f(t)}{(1-t)^d}$, for some d, with $f(t) \in \mathbb{Z}[t]$, $f(1) \neq 0$.
Now, $(1-t)^{-1} = 1 + t + t^2 + \cdots$, so repeated differentiation gives $(1-t)^{-d} = \sum \binom{d+n-1}{d-1} t^n$.
If $f(t) = a_0 + a_1 t + \cdots + a_s t^s$, then $\lambda(N_n) = a_0 \binom{d+n-1}{d-1} + a_1 \binom{d+n-2}{d-1} + \cdots + a_s \binom{d+n-s-1}{d-1}$ - $\oplus$.
RHS of $\oplus$ can be rearranged as a polynomial $\varphi(n)$ in n, with rational coefficients, if $d+n-s-1 \geq d-1$. $\varphi(x) = \frac{f(1)}{(d-1)!} x^{d-1}$ + lower order terms.
This polynomial is the Hilbert function.

Example: $T = k[X_1, \dots, X_n]$, k a field, λ = vector space dimension.

monomials of degree m = dimn of component of degree m = $\binom{n+m-1}{n-1}$ $\forall\, n \geq 0$.

$P(X) = \frac{1}{(n-1)!}(X+n-1)\cdots(X+1)$.

(8.14): Let R be a Noetherian local domain with maximal ideal P. Let I be such that $\sqrt{I} = P$. Let M be a f.g. R-module. Then, for sufficiently large n, the composition length of $M/I^{n+1}M$ is a polynomial of degree $\leq t$, where t = least number of generators of I.

Remark: Composition length, $\ell(M/I^{n+1}M) = \sum_{j=0}^{n} \ell(I^jM/I^{j+1}M)$

Proof: If $x_1, \dots, x_t$ generate I, the images in I/I^2 together with R/I generate the associated graded algebra $gr_I R$. By (8.13), $\ell(I^nM/I^{n+1}M) = f(n)$, with $f(n)$ a polynomial in n of degree $d-1$ (with d as in (8.13), $d \leq t$), for large enough n. But $f(n) = \ell(M/I^{n+1}M) - \ell(M/I^nM)$, and so $\ell(M/I^{n+1}M)$ is a polynomial of degree d ($\leq t$) for large enough n.

Justification: use ⊕ from (8.13): $\ell(I^nM/I^{n+1}M) = a_0\binom{d+n-1}{d-1} + \cdots + a_s\binom{d+n-s-1}{d-1}$.

This, together with $\binom{m}{n} = \binom{m-1}{n-1} + \binom{m-1}{n}$, yields $\sum_{v=0}^{n}\binom{d+v-1}{d-1} = \binom{d+n}{d}$.

We get: $\ell(M/I^{n+1}M) = a_0\binom{d+n}{d} + a_1\binom{d+n-1}{d} + \cdots + a_s\binom{d+n-s}{d}$; for $n \geq s$, this is a polynomial in n of degree d.

Remarks: If we set $M = R$, $\ell(M/M_n)$ is the Samuel Function.

If we have I with $\sqrt{I} = P$, J with $\sqrt{J} = P$, then $I^a \subseteq J$, $J^b \subseteq I$, some a, b, and hence the degree of the Samuel functions are the same for I and J.

This degree $d(M)$ can be regarded as a dimension of M.

If $0 \to M_1 \to M \to M_2 \to 0$, then $d(M) = \max\{d(M_1), d(M_2)\}$.

Theorem: If R a Noetherian local domain, then $d(R) = \dim R$ = least number of generators of some ideal I with $\sqrt{I} = P$.

Proof: Omitted.